Autorité de protection des données
Gegevensbeschermingsautoriteit

Litigation Chamber

Decision on the merits 61/2023 of 24 May 2023

This decision was annulled by the judgment 2023/AR/801[0] of 20 December 2023 of the Brussels Court of Appeal (Market Court), which refers the case back to the Litigation Chamber, otherwise composed, so that it can rule again on the merits, taking into account the considerations of the Market Court

File Number: DOS-2021-00068

Subject: Complaint concerning the transfer by the Federal Public Service (FPS) Finance of personal data to the US tax authorities under the FATCA agreement

The Litigation Chamber of the Data Protection Authority, formed by Mr Hielke Hijmans, President, and Mssrs Yves Poullet and Christophe Boeraeve, members;

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 *on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (General Data Protection Regulation), hereinafter GDPR;

Having regard to the Act of 3 December 2017 *establishing the Data Protection Authority* (hereinafter LCA);

Having regard to the Act of 30 July 2018 *on the protection of natural persons as regards the processing of personal data* (hereinafter LTD);

Having regard to the internal regulations as approved by the Chamber of Representatives on 20 December 2018 and published in the *Belgian Official Gazette* on 15 January 2019;

Having regard t

o the documents in the file;

has made the following decision regarding:

The plaintiffs: Mr **X**,

Hereinafter referred to as "the first plaintiff";

[0] By interlocutory judgment 2023/5139 of 28 June 2023, the Brussels Court of Appeal (Market Court) granted the request for suspension of the decision of the FPS Finances.

The non-profit association Accidental Americans Association of Belgium (AAAB), with registered offices at clos Albert Crommelynck, 4 bte 7, 1160 Brussels,

Hereinafter referred to as "the second plaintiff";

Hereinafter referred to jointly as "the plaintiffs";

Both having as their counsel Vincent Wellens, lawyer, with offices at Chaussée de la Hulpe, 120, 1000 Brussels.

The defendant:

The **Federal Public Service Finance (FPS Finance)**, with registered offices at Boulevard du Roi Albert II, 33, 1030 Brussels,

Hereinafter referred to as "the defendant";

Having as its counsel Jean-Marc Van Gyseghem, lawyer, with offices at Boulevard de Waterloo, 34, 1000 Brussels.

Contents

I. FACTS and BACKGROUND to the PROCEDURE

1. On 22 December 2020, the plaintiffs filed a complaint with the Data Protection Authority (DPA) against the defendant. The complaint denounced the unlawfulness of the transfer of personal data relating to the first plaintiff, as well as relating to accidental Americans in Belgium (whose interests are defended by the second plaintiff) by the defendant to the US tax authorities in the context of the intergovernmental FATCA agreement concluded between Belgium and the United States, as well as other infringements of the GDPR attributable to the defendant in this context.

2. The facts giving rise to the complaint are set out below in points 3 to 23, followed by the background to the procedure leading up to this decision (points 24 to 111).

I.A. The relevant facts

3. The first plaintiff resides in Belgium and holds dual Belgian and American nationality. With regard to the latter nationality, the first plaintiff describes himself as an *accidental* American, since he has American nationality only by virtue of having been born in the United States, at Stanford, without having subsequently retained any significant ties with that country. The plaintiff resides in Belgium.

4. The second plaintiff is a Belgian non-profit association (ASBL) whose purpose is to defend and represent the interests of individuals with Belgian-American nationality - such as the first plaintiff - who reside outside the United States. The purpose of the association is described as follows in article 4 of its articles of association dated 28 September 2019 (paraphrased):

> *"The purpose of the association is to defend the interests of natural persons of American nationality residing outside the United States, against the harmful effects of the extraterritorial nature of US legislation.*
>
> *The association pursues the realisation of its purpose by all means of action and in particular by:*
>
> - *representing the interests of members before the Belgian and American public authorities and before the European institutions*
> - *producing communication media*
> - *organising events*
> - *working with law professors to provide legal information for members' use*
> - *legal action to defend the interests of Belgian-American nationals*
>
> *The means listed above are indicative and not exhaustive".*

5. On account of his US nationality, the first plaintiff is considered to be subject to the control of the US tax authorities under US tax law. Indeed, this system is based on the principle of taxation based on *nationality*, and applies to accidental Americans as it does to any other taxpayer based on US territory or having activities in relation with this country; the fact that they do not reside in the United States is irrelevant. Only certain exceptions apply to non-residents on US territory.

6. In order to facilitate the collection of relevant information by the Internal Revenue Service (IRS) with a view to the possible taxation of Americans residing abroad (including accidental Americans such as the first plaintiff), the US government has entered into intergovernmental agreements with various states around the world. Under these agreements, domestic financial institutions (such as banks) are required to communicate data relating to these Americans who reside abroad, to the domestic tax authorities (such as the defendant), which are then required to transfer this data to the IRS.

7. This is the context of the "Agreement between the Government of the Kingdom of Belgium and the Government of the United States of America to improve International tax compliance and to implement Fatca", signed by representatives of the Governments of the Kingdom of Belgium and the United States of America on 23 April 2014. This agreement is commonly referred to as the "FATCA agreement".[1] It implements the US **F**oreign **A**ccount **T**ax **C**ompliance **A**ct, from which the acronym FATCA is derived. A comparable bilateral intergovernmental agreement has also been signed with various countries around the world, including the member states of the European Union (hereinafter EU).

8. For its part, the Belgian Act of 16 December 2015 *regulating the communication of information relating to financial accounts by Belgian financial institutions and the FPS Finance, in the context of an automatic exchange of information at the international level and for tax purposes* (hereinafter the Act of 16 December 2015) invoked by the defendants in several aspects, is part of the more *general* context of the exchange of tax data between countries, including but also - beyond the sole exchanges with the IRS pursuant to the above-mentioned FATCA agreement.

9. The purpose of this legislation, as defined in Article 1, is to regulate the obligations of Belgian financial institutions and the defendant with regard to the information which must be communicated to a competent authority of another jurisdiction in the context of an automatic exchange of information relating to financial accounts, organised in accordance with the commitments made by the Belgian State and resulting from the legal texts below:

    - Council Directive 2014/107/EU of 9 December 2014 *amending Directive 2011/16/EU as regards mandatory automatic exchange of information in the field of taxation*[2];

[1] This intergovernmental agreement, FATCA, which was signed with Belgium, was the subject of a law of assent on 22 December 2016.

[2] Council Directive 2014/107/EU of 9 December 2014 amending Directive 2011/16/EU as regards mandatory automatic exchange of information in the field of taxation, OJ 2014, L 359/1.

- The Joint OECD/Council of Europe Convention *on Mutual Administrative Assistance in Tax Matters of 25 January 1988 (the Multilateral Convention* or "the Convention");
- A bilateral agreement for the avoidance of double taxation on income;
- A bilateral treaty on the exchange of tax information (such as the FATCA agreement).

10. The Act of 16 December 2015 came into force on 10 January 2016 with regard to information intended for the United States (Article 20)[3].

11. On 22 April 2020, the first plaintiff received a letter from Bank Z, with which he has bank accounts. The subject of this letter was (freely translated): *"Confirmation of your status as a US Person in the context of Fatca and other regulatory purposes".* The plaintiff was requested to confirm that he is neither a US citizen nor resident in the United States, for the purposes of the obligations incumbent on Bank Z under the applicable regulations on the automatic exchange of information. The plaintiff was invited to complete a specific form issued by the US authorities for this purpose. The letter explains that the objectives of the US legislation are to identify all accounts held by US citizens and/or residents with non-US financial institutions, and to exercise greater control over the income and securities held by Americans. The letter specifies that if the signed and completed document is not returned, the law obliges the bank to consider the first plaintiff as a "US Person" by default: consequently, his contact details and information on his assets, income and gross proceeds will continue to be communicated to the relevant tax authorities. Finally, the letter specifies that if the first plaintiff is a US citizen or resident, he must report to the agency to complete the necessary formalities.

12. On 12 May 2020, the first plaintiff was informed by Bank Z that since he had several bank accounts in Belgium in 2019, these were subject to the obligation to make a declaration to the defendant, pursuant to the legal obligations incumbent on banking institutions with which tax residents of a country other than Belgium have one or more bank accounts, as is his case.

13. In this second letter, Bank Z informs the first plaintiff that it is obliged to declare the following data to the defendant: the name, address, jurisdiction where the person is a resident, tax identification number (TIN) or date of birth of each person subject to a declaration, account number(s), account balance or value as of 31 December (special case: if the account is closed, a zero amount is reported), interest, dividends, proceeds from the sale, redemption or repayment of financial audits and other income from financial assets held in the account.

14. Bank Z encloses with this letter the details of the first plaintiff, which will be communicated to the defendant in compliance with this reporting obligation.

[3] The Act of 16 December 2015 was published in the Belgian Official Gazette on 31 December 2015. Article 20 of the Act stipulates that it will come into force 10 days after its publication, as regards information destined for the United States.

15. This letter of 12 May 2020 makes *no reference to the FATCA agreement.* In addition to the list of details cited above and information on the principle of automatic exchange of financial information to which Bank Z risks being subject, the first plaintiff is referred to the defendant for any questions, as follows (freely translated): *"For further information on the automatic exchange of financial information, please consult the website of the FPS Finance or the OECD. You can also call us at XXX"*.

16. In a third letter dated 18 May 2020, Bank Z again contacted the first plaintiff and (a) this time explains in general terms the principle of the FATCA agreement, (b) lists the information to be communicated in this context and (c) indicates that as soon as the plaintiff had one or more accounts subject to the declaration obligation in 2019, it is obliged to communicate them to the competent tax authorities. Bank Z states that for further information on the FATCA agreement, the first plaintiff can call his bank at the telephone number indicated.

17. On 22 December 2020, the same day he filed a complaint with the DPA along with the second plaintiff (complaint no. 1 - point 1), the first plaintiff requested that the defendant delete the personal data it had obtained from the banks pursuant to the FATCA agreement, under Article 17(1)(d) of the GDPR. The first plaintiff also requested that the defendant take the necessary steps to obtain this erasure from the IRS or, failing that, the restriction of the processing thereof pursuant to Article 18(1)(b) of the GDPR. In any event, the first plaintiff is calling for the immediate cessation of the exchange of information between the defendant and the IRS that takes place every year pursuant to the FATCA Agreement: in his view, this transfer of personal data concerning him infringes various key principles of personal data protection law as applicable in Belgium and more generally within the EU. The second plaintiff is making the same claim in its own name, for the benefit of accidental Americans in Belgium, in accordance with its articles of association.

18. More specifically, the plaintiffs substantiate their claim on the following grounds: the unlawfulness of the transfer of personal data to the IRS under the FATCA agreement (in breach of Articles 45, 46 and 49 of the GDPR); non-compliance with the principles of purpose limitation (Article 5(1)(b) of the GDPR), proportionality and data minimisation (Article 5(1)(c) of the GDPR) and storage limitation (Article 5(1)(e) of the GDPR); failure to comply with the principle of transparency (Articles 12 to 14 of the GDPR) and a breach of the obligation to carry out a data protection impact assessment (DPIA - Article 35 of the GDPR). The letter details each of the alleged grievances. As these are also the basis of the complaint lodged with the DPA, they will be explained below when the Litigation Chamber discusses the respective viewpoints of the parties, including those of the plaintiffs (points 54 et seq.).

19. In its reply of 30 March 2021, the defendant refused to entertain the plaintiffs' request, arguing that there the allegations of unlawfulness were baseless. The defendant thus stated that the legal basis for the transfers it makes is stipulated in the FATCA agreement, as well as in the Act

of 16 December 2015. The defendant also invoked Article 96 of the GDPR, and concluded in support of it that, if the plaintiffs cannot demonstrate how the FATCA agreement infringed EU law prior to 24 May 2016, there is no basis for their claims. The defendant also refuted all the other allegations made against it.

20. To properly understand the decision, the Litigation Chamber cites Article 96 of the GDPR entitled "Relationship with previously concluded Agreements", which provides as follows:

> *"International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to 24 May 2016, and which comply with Union law as applicable prior to that date, shall remain in force until amended, replaced or revoked".*

21. Following this response from the defendant, only the first plaintiff renewed his demand on 9 July 2021 , emphasising the fact that the said data transfers from the defendant to the IRS were also unlawful under Directive 95/46/EC.[4]

22. In a decision dated 4 October 2021, the defendant refused to entertain the first plaintiff's demands, rejecting the arguments put forward by the latter with regard to the alleged infringements of both the GDPR and Directive 95/46/EC. For a proper understanding of the rest of its decision, the Litigation Chamber specifies that the defendant also considers under the terms of this decision (freely translated) *"that in the present case, the condition of a basis resting on important reasons of public interest - within the meaning of Article 49(1)(d) of the GDPR[5] or Article 26(1)(d)[6] of Directive 95/46/EC] - is indeed fulfilled since the basis for the lawfulness of the disputed processing rests on an international agreement [i.e. the FATCA agreement] and the Act of 16 December 2015".*

23. An action for annulment was brought before the Council of State (CoS) against the administrative decision of the defendant. In their conclusions and at the hearing before the Litigation Chamber, the parties indicated that this action was still pending. They specified that the defendant had argued that the CoS should await the outcome of the procedure with the DPA before making a decision. The plaintiff, for his part, requested that preliminary rulings be referred by the CoS to the Court of Justice of the European Union (hereinafter CJEU) as to the

---

[4] 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, OJ L 281/31.

[5] Article 49(1)(d) of the GDPR: *"In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions: [..] (d) the transfer is necessary for important reasons of public interest;"*

[6] Article 26(1)(d) (Derogations) of Directive 95/46/EC: *"By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that: [..] (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims".*

legal basis of the transfers made pursuant to the FATCA agreement, as to the admissibility of the application of Article 49(1)(d) of the GDPR or, where applicable, its equivalent in Directive 95/46/EC, if Article 96 of the GDPR is applied, as well as with regard to compliance with the principles of transparency, purpose limitation, data minimisation and storage limitation as enshrined in the relevant articles of the GDPR or their equivalents in Directive 95/46/EC if the application of Article 96 of the GDPR were to be accepted.

I.B. Background to the procedure

24. As mentioned in point 1 above, the plaintiffs filed a complaint with the DPA on 22 December 2020 (complaint no. 1**)**.

I.B.1. Admissibility of the complaint

25. On 22 March 2021, **complaint no. 1, as it was filed by the first plaintiff, was declared admissible** by the Front Line Service (FLS) of the DPA, pursuant to Articles 58 and 60 of the *Act of 3 December 2017 establishing the Data Protection Authority* (hereinafter LCA) and the complaint was forwarded to the Litigation Chamber pursuant to Article 62, § 1 of the LCA.

26. As regards complaint no. 1, as it was filed by the **second plaintiff, was declared inadmissible** on 12 February 2021 by the FLS of the DPA on the grounds that the second plaintiff did not meet the conditions set out in article 220.2. 3° and 4° of the Act of 30 July 2018 *on the protection of natural persons as regards the processing of personal data* (hereinafter LTD)[7].

27. The Litigation Chamber can confirm here that on **9 July 2021, the second plaintiff** filed a new complaint (complaint no. 2). This complaint consisted of a rewording of its complaint no. 1 of 22 December 2020. The second plaintiff was more explicit in this complaint about its interest in taking action. It therefore states that it is acting in its own name, in accordance with its articles of association, and not in the name and on behalf of one or more Belgian accidental Americans. The second plaintiff therefore stated that it was not getting involved as a representative within the meaning of Article 80(1) of the GDPR[8]. In its view, the conditions for applying this article as

[7] Article 220 of the LTD: § 1. (freely translated) The person concerned has the right to appoint a body, organisation or non-profit association to lodge a complaint on their behalf and to exercise on their behalf the administrative or jurisdictional remedies either with the competent supervisory authority or with the judiciary, as provided for by specific laws, the Judicial Code and the Code of Criminal Procedure.
§ 2. In the disputes referred to in paragraph 1, a body, organisation or non-profit association must:
- 1° be validly incorporated in accordance with Belgian law;
- 2° have legal personality;
- 3° have objectives in their articles of association in the public interest;
- 4° have been active in the field of protecting the rights and freedoms of data subjects in the context of personal data protection for at least three years.

§ 3. The body, organisation or non-profit association shall provide proof, by presenting its activity reports or any other document, that it has actually performed its activity for at least three years, that the activity corresponds to its corporate purpose and that this activity is related to the protection of personal data.

[8] Article 80(1) of the GDPR "Representation of data subjects": The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the

set out in article 220.2. 3° and 4° of the LTD, do not therefore have to be met. The second plaintiff, on the other hand, relies on article 58 of the LCA, which stipulates that (freely translated) "*any person may file a written, dated and signed complaint or request with the Data Protection Authority*". The second plaintiff considers itself entitled to lodge a complaint with the DPA on this basis, especially as the aim of its complaint is in line with its articles of association. It also argues that in its decision-making practice, the DPA, in support of decision 30/2020 of the Litigation Chamber for example, has recognised that there is broad interest in bringing an action, and that the possibility of lodging a complaint is not restricted to the natural data subjects, and that a complaint can be lodged by associations by virtue of their specific corporate purpose[9].

28. On 5 October 2021, this complaint n°2 was **declared admissible** by the FLS of the DPA on the basis of articles 58 and 60 of the LCA. This complaint was forwarded to the Litigation Chamber pursuant to article 62, § 1 of the LCA.

29. In view of the foregoing, the Litigation Chamber specifies that, for the purposes of this decision, the use of the term "the complaint" refers to the two complaints filed (no. 1 and no. 2), which were joined by the Litigation Chamber (see point 47).

I.B.2. The subject of the complaint

30. The main purpose of the complaint lodged by the plaintiffs is to obtain, pursuant to Article 58(2)(f) and (j) of the GDPR, the ban or even suspension of the transfer of data (the data of the first plaintiff and, beyond that, the data of all Belgian accidental Americans whose interests are defended by the second plaintiff) by the defendant to the IRS pursuant to the FATCA agreement.

31. Under the terms of their conclusions in reply (points 54 et seq. below), the plaintiffs added that, in the alternative, they were requesting that the Litigation Chamber order, pursuant to Article 58(2)(f) and (j) of the GDPR, that the transfer of data on account balances by the defendant to the IRS in the context of the FATCA agreement be banned, or even suspended, as regards both the first plaintiff and the Belgian accidental Americans whose interests are defended by the second plaintiff.

32. During the hearing held before the Litigation Chamber[10], the plaintiffs clarified that using the terms "ban or even suspension" is based on the exact wording of Article 58(2)(f) and (j) of the

rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.

[9] In this respect, the Litigation Chamber refers to the note it adopted on the position of the plaintiff (French only) https://www.autoriteprotectiondonnees.be/publications/note-relative-a-la-position-du-plaignant-dans-la-procedure-au-sein-de-la-chambre-contentieuse.pdf, in particular point B. (in fine) on page 2. It also refers to its decision 24/2022 and the references cited therein.

[10] See point B of the minutes of the hearing of 10 January 2023.

GDPR, and does not imply a request for a *temporary* suspension of transfers but rather their outright cessation going forward.

I.B.3. The investigation of the Inspection Service

33. On 20 April 2021, the Litigation Chamber commissioned the Inspection Service (hereinafter IS) to conduct an investigation, pursuant to articles 63, 2° and 94, 1° of the LCA. On the same date, in accordance with article 96, § 1 of the LCA, the Litigation Chamber's request to conduct an investigation was forwarded to the IS.

34. On 26 May 2021, the investigation of the IS was closed, the report was attached to the file and was sent by the Inspector General to the President of the Litigation Chamber (Article 91, § 1 and § 2, of the LCA).

35. Under the terms of this report, the IS concluded that there was (freely translated) "*no apparent breach of the GDPR*" (page 5 of the report).

36. The IS based its conclusion on the fact that the basis for the lawfulness of the transfers of bank details of US nationals (including the first plaintiff) was the FATCA agreement and the Act of 16 December 2015. The IS also highlighted the fact that the above-mentioned Article 96 of the GDPR (point 20) was applicable.

37. In its examination of whether the FATCA agreement was in compliance with the regulatory framework on data protection applicable prior to 24 May 2016, i.e. according to its terms, with Directive 95/46/EC as transposed under the terms of the Act of 8 December 1992 *on the protection of privacy with regard to the processing of personal data* (hereinafter LVP), the IS noted the following elements:

- On 17 December 2014, the Commission for the Protection of Privacy[11] (hereinafter CPP) issued a favourable opinion 61/2014 subject to strict suspensive conditions on the first draft of the future Act of 16 December 2015. In its opinion 28/2015 of 1 July 2015, the CPP then issued a favorable opinion on the second draft law, which implemented the remarks and conditions issued in its opinion 61/2014.
- Under the terms of its deliberation AF 52/2016 of 15 December 2016, the Sector Committee for the Federal Authority[12] (hereinafter SCFA) of the CPP authorised the defendant to transmit the financial information of declarable accounts of US taxpayers transmitted to it by financial institutions under the FATCA agreement, to the IRS. The

[11] The Commission for the Protection of Privacy (CPP) was the Belgian data protection authority within the meaning of Article 28 of Directive 95/46/EC. It was superseded on 25 May 2018 by the Data Protection Authority (DPA) in implementation of Article 3 of the LCA.

[12] Article 36bis of the LVP stipulated that any electronic transfer of personal data by a federal public service or by a public body with legal personality that falls under federal authority requires authorisation in principle from the SCFA, unless the transfer has already been authorised in principle by another sector committee set up within the CPP. The mission of the SCFA is to verify that the transfer complies with legal and regulatory provisions.

IS stressed that on this occasion, the SCFA assessed the admissibility of the tax purposes of the processing, as well as the proportionality of the data and the security of the processing. In keeping with the principle of transparency, the SCFA also ordered the defendant to inform the public, via accessible and comprehensible text on its website, of the circumstances in which their personal data (including financial data) may be transmitted to the IRS. The IS noted in this respect that a web page dedicated to FATCA was published on the defendant's website. Lastly, the IS points out that, in application of article 111 of the LCA[13], authorisations granted by the sector committees of the CPP (such as the SCFA) prior to the entry into force of this law, retain their legal validity in principle[14].

38. Finally, the IS ruled out the applicability of the Schrems II ruling[15] of the CJEU. It pointed out that this ruling invalidates the Privacy Shield, which concerned the transfer of personal data to the United States for *commercial* purposes (and not for tax purposes, including the fight against tax fraud and evasion, as in this case). The IS also referred to Article 17[16] of the Act of 16 December 2015, which refers both to the FATCA agreement and to the agreements to which the FATCA itself refers, i.e. the above-mentioned Convention of the OECD and the Council of Europe.

39. At the end of its investigation, the IS considered that, in view of these considerations and in accordance with Article 64.2 of the LCA, it is not appropriate to pursue its investigation further and that there is, as already mentioned (point 35), *no apparent infringement of the GDPR*.

---

[13] Article 111 of the LCA: (Freely translated) Without prejudice to the supervisory powers of the Data Protection Authority, authorisations granted by the sector committees of the Commission for the Protection of Privacy prior to the entry into force of this Act remain legally valid. Following the entry into force of this Act, adherence to a general authorisation granted by deliberation of a sector committee is only possible if the applicant sends a written and signed undertaking to the Data Protection Authority, in which they confirm that they adhere to the conditions of the deliberation in question, without prejudice to the supervisory powers that the Data Protection Authority may exercise after receipt of this undertaking. Unless otherwise stipulated by law, current authorisation requests submitted before the Act comes into force shall be processed by the data protection officer of the institutions involved in the data exchange.

[14] The Litigation Chamber will in general not give any ruling on the validity of these authorisations. It will examine the relevance of the recourse to that invoked by the defendant in the specific context of the complaint leading to the present decision.

[15] Judgment of the court of 16 July 2020, C-311/18, Facebook Ireland and Schrems (Schrems II), ECLI:EU:C:2020:559.

[16] Article 17 of the Act of 16 December 2015: § 1. (freely translated) Information transferred to a jurisdiction subject to declaration is subject to the confidentiality obligations and other protective measures provided for by the treaty on tax matters which permits the automatic exchange of information between Belgium and that jurisdiction and by the administrative agreement which organises this exchange, including the provisions limiting the use of the information exchanged. § 2. However, notwithstanding the provisions of a tax treaty, the competent Belgian authority : - may, as a general rule and subject to reciprocity, authorise a jurisdiction, to which the information is transferred, to use the information as evidence in criminal courts where the information contributes to the opening of criminal proceedings for tax fraud; - subject to the first indent, may not authorise a jurisdiction, to which the information is transferred, to use the information for any purpose other than the assessment or collection of, the enforcement or prosecution in respect of, the determination of appeals in relation to, or the oversight of the taxes referred to in the treaty; and - may not authorise a jurisdiction to which the information is transferred to communicate the information to a third jurisdiction.

I.B.4. The follow-up investigation of the Inspection Service

40. On 24 June 2021, the Litigation Chamber requested that the IS carry out a follow-up investigation pursuant to article 96.2. of the LCA.

41. On examining the report of 26 May 2021 (points 33 et seq.), the Litigation Chamber noted that there was a lack of information on certain points raised by the plaintiffs to substantiate their complaint, including:

- Are appropriate safeguards in place for transfers to the United States?
- Is there further processing, or not, for other purposes? And are there are any safeguards, where appropriate?
- How long will the data be kept, taking into account any further processing?
- Which data is communicated exactly, and what is the volume of this data per data subject, as well as the number of data subjects in Belgium?
- Is there a reciprocity clause, and if so, how is it implemented in practice?
- Has a DPIA within the meaning of Article 35 of the GDPR been carried out (or will one be carried out?), in what form and on what date?
- Has the first plaintiff lodged other claims with the same or similar object before other bodies (judicial, administrative) since lodging his complaint? And what was the outcome, if any?

42. On 9 July 2021, during the course of the investigation, the plaintiffs asked the IS to temporarily suspend the transfer of data in the context of FATCA reporting for the year 2020 to the IRS, as a *provisional measure* taken on the basis of the LCA and until the Litigation Chamber had made a final decision, and at least until 30 September 2021. The plaintiffs argue that the denounced transfers are likely to cause them serious, immediate and difficult-to-repair damage as soon as they are effectuated.

43. On 10 August 2021, the IS replied to the plaintiffs that taking provisional measures is one of the investigative powers conferred on the IS by the LCA, and that it is not an obligation but rather a possibility left to the sole discretion of the IS. The IS also highlighted the fact that, pursuant to article 64.2 of the LCA, it ensures that all useful and appropriate means are used for the purposes of the investigation. It added that it was not about to receive instructions from anyone as to which investigative measures had to be implemented, thereby rejecting the plaintiffs' request.

44. On 14 September 2021, the follow-up investigation of the IS was closed, the report was attached to the file and was sent by the Inspector General to the President of the Litigation Chamber (Article 91.1 and 91.2 of the LCA).

45. In its follow-up report, the IS noted that there was no evidence to suggest a lack of safeguards concerning the protection of transferred data or of non-reciprocity regarding the exchanges. The IS stated that it could only observe the fairly robust legal framework governing the transfer of US nationals' tax data by the defendant to the IRS. In this respect, it referred to the description of the safeguards surrounding the said transfers given by the defendant's Data Protection Officer (hereinafter DPO), to the parliamentary work of the law assenting to the FATCA agreement and to articles 3.7[17] and 3.8[18] of the said agreement. The IS also referred to the judgment of the French Council of State of 19 July 2019 referred to by the French sister organisation of the second plaintiff, a judgment in which the claim that Article 46 of the GDPR had been disregarded was rejected[19]. In its report, the IS also repeated the elements put forward by the defendant to justify the fact there is no DPIA (point 95).

I.B.5. Examination of the merits by the Litigation Chamber

46. On 20 January 2022, the Litigation Chamber decided, pursuant to article 95, § 1, 1° and article 98 of the LCA, that complaints n°1 and n°2 could be addressed on their merits.

47. On the same date, the parties were informed by registered mail of the provisions of article 95, § 2 and article 98 of the LCA. Under the terms of this letter, the Litigation Chamber decided to **join complaints no. 1 and no. 2**, which relate to the same processing of personal data (data relating to the same facts), both were lodged against the defendant, and both raise the same complaints against the latter. The Litigation Chamber therefore considers them to be so closely correlated that it has an interest in hearing and deciding on them simultaneously, to ensure that its decisions are consistent.

48. In the same letter, the Litigation Chamber granted the parties the following deadlines for concluding: 17 March and 16 May 2022 for the defendant and 15 April 2022 for the plaintiffs.

---

[17] Article 3.7. of the FATCA agreement: "All information exchanged shall be subject to the confidentiality and other protections provided for in the Convention, including the provisions limiting the use of the information exchanged". "Convention" refers to the Convention on Mutual Administrative Assistance in Tax matters of 25 January 1988.

[18] Article 3.8. of the FATCA agreement: Following the entry int force of this Agreement, each Competent Authority shall provide written notification to the other Competent Authority when it is satisfied that the jurisdiction of the other Competent Authority has in place (i) appropriate safeguards to ensure that the information received pursuant to this Agreement shall remain confidential and be used solely for tax purposes, and (ii) the infrastructure for an effective exchange relationship (including established processes for ensuring timely, accurate, and confidential information exchanges, effective and reliable communications and demonstrated capabilities to promptly resolve questions and concerns about exchanges or requests for exchanges and to administer the provisions of Article 5 of this Agreement). The Competent Authority shall endeavor in good faith to meet, prior to September 2015, to establish that each jurisdiction has such safeguards and infrastructure in place.

[19] The French Council of State was referred to by the French Association of Accidental Americans, with a petition to annul, on the grounds of abuse of authority, the decisions refusing its requests for the repeal of a decree and its ministerial order organising the collection and transfer of personal data to the American authorities. In its ruling, the French Council of State concluded that, in view of the specific safeguards applied by the FATCA agreement of 14 November 2013 (agreement concluded with France) to the disputed processing and the level of protection provided by the personal data legislation applicable in the United States through which the tax situation of taxpayers can be ascertained (the French CoS refers to the US Federal Privacy Act of 1974 and the Federal Tax Code), the action claiming infringement of Article 46 of the GDPR and Articles 7 and 8 of the EU Charter of Fundamental Rights must be rejected (points 23 et seq. of the ruling).

49. In support of the complaint and the reports of the IS, the Litigation Chamber also identified the grievances, regarding which it invited the parties to present their arguments:

    - The unlawfulness of the defendant's data transfers to the IRS under Articles 45 and 49 of the GDPR and the fact there is no legal basis;
    - Failure to comply with the principles of purpose limitation, proportionality and data minimisation (Article 5(1)(b) and (c) of the GDPR) as well as failure to comply with the principle of storage limitation (Article 5(1)(e) of the GDPR);
    - Failure to comply with the principle of transparency and the obligation to provide information (Articles 5(1)(a), 12 and 14 of the GDPR);
    - Failure to comply with Article 16 of the GDPR (right of rectification) in that the defendant's procedures do not provide for the possibility for data subjects to have their status corrected with regard to the FATCA legislation;
    - Failure to carry out a DPIA within the meaning of Article 35 of the GDPR;
    - Failure to comply with Articles 5(2) and 24 of the GDPR combined with the breaches detailed above;
    - Failure to comply with Article 20 of the Act of July 30, 2018 (LTD).

50. The Litigation Chamber also invited the parties to conclude on Article 96 of the GDPR invoked by the defendant in its letter of 4 October 2021 (point 22).

51. On 30 March 2022, the Litigation Chamber sent a supplementary request to the parties. Under the terms of this request, the Litigation Chamber stated that it had become aware, from the press, that the second plaintiff had lodged an appeal in December 2021 with the (Belgian) CoS with regard to the problem of transfers of the data of accidental Americans to the United States. Without prejudice to the respective competences of the CoS and the DPA, the Litigation Chamber requested the second plaintiff to clarify the subject of this appeal to the CoS and, if possible, the related timing, in its future reply or in a separate document, at the latter's discretion. The Litigation Chamber specified that this information was intended to enable it to assess whether (the outcome of) this appeal was likely to have an impact on the proceedings underway before the DPA and/or on its future decision. Under the terms of the complaint form, the plaintiff was asked to inform the DPA as to whether there were any complaint(s) lodged with other bodies. As this appeal to the CoS had not yet been lodged at the time the complaint was lodged with the DPA, the second plaintiff was asked to kindly clarify the matter to the Litigation Chamber. In this respect, the Litigation Chamber refers to the information provided in point 23 above.

52. On 31 January and 8 February 2022, the defendant requested a copy of the file (art. 95, §2, 3° LCA), which was sent to it on 9 February 2022.

I.B.6. The arguments of the parties

53. On 16 March 2022, the Litigation Chamber received the defendant's reply. As the defendant has also filed additional conclusions and summary conclusions at a later stage (hereinafter the summary conclusions), a summary of its full arguments will be set out in detail in paragraphs 79 et seq.

I.B.6.1. Position of the plaintiffs

54. On 15 April 2022, the Litigation Chamber received the plaintiffs' reply.

55. The plaintiffs' arguments, grievance by grievance, can be summarised as follows.

- *As regards Article 96 of the GDPR*

56. By way of introduction, the plaintiffs state that Article 96 of the GDPR is not applicable since the condition it lays down that the international agreement must, in order to continue to have effect, comply with EU law as applicable prior to 24 May 2016 is not satisfied. Indeed, the plaintiffs consider that the FATCA agreement is neither compliant with Directive 95/46/EC (applicable before 25 May 2016) nor, moreover, compliant with the GDPR. The plaintiffs also state that, in any event, aspects that are not regulated or imposed by or under the FATCA agreement, such as the obligation to inform data subjects (Title II.E.2) are subject to the GDPR without any interference from its Article 96.

- *As regards compliance with rules governing cross-border transfers*

57. As regards the transfer to the IRS, the plaintiffs note that prior to its reply conclusions of 16 March 2022 in which it stated that it relied on Article 46(2)(a) of the GDPR (point 82 et seq.), the defendant appeared, as evidenced by its administrative decision of 4 October 2021 (point 22), to rely on Article 49(1)(d) of the GDPR (or on Article 26(1)(d) of Directive 95/46/EC) or on the "important reasons of public interest", the basis for the lawfulness of the transfer resting, in its view, on the FATCA agreement and on the Act of 16 December 2015.

58. For the sake of completeness, the plaintiffs argue that the lack of equivalent reciprocity and the systematic nature of the alleged transfers are obstacles to the defendant's reliance on Article 49(1)(d) of the GDPR, even though it no longer relies on this provision since its reply conclusions.

- As regards the lack of reciprocity, the plaintiffs cite a number of letters from European authorities and other American positions that attest to this lack of reciprocity;
- As regards the systematic nature, the plaintiffs rely on Guidelines 02/2018 of the European Data Protection Board (hereinafter EDPB) on *derogations of Article 49 under*

Regulation EU 679/2016 [20], which state that recourse to Article 49(1)(d) of the GDPR cannot be invoked for recurrent, systematic transfers or transfers taking place on a large scale: derogations must be interpreted restrictively so that the exception *"does not become the rule in practice, but must be limited to specific situations (...)"*.

59. The plaintiffs further point out that Article 49(1)(d) of the GDPR provides one of the possible derogations to the ban on international transfers where, according to the cascade system set up by Chapter V of the GDPR and before it by Articles 25 and 26[21] of Directive 95/46/EC, no adequacy decision pursuant to Article 45(3) of the GDPR has been adopted for the country concerned or in the absence of appropriate safeguards pursuant to Article 46 of the GDPR. By using Article 26(1)(d) of Directive 95/46/EC as specified in Article 16(2) of the Act of 16 December 2015[22], the legislator was therefore, in the plaintiffs' view, acknowledging that there were no appropriate safeguards in place. It is therefore pointless for the defendant to rely on CPP opinions 61/2014 and 28/2015 to conclude that the FATCA agreement complied with EU law (including the rules on transfer) on 24 May 2016. These opinions related to the above-mentioned Belgian legislation and did not examine whether there were appropriate safeguards in the FATCA agreement itself.

60. The plaintiffs point out that these "appropriate safeguards" must be included in the FATCA agreement itself in order to bind the parties to it. These safeguards are those identified by the EDPB in its Guidelines 02/2020 *on Article 46(2)(a) and (3)(b) of the GDPR of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies* (hereinafter Guidelines 02/2020)[23]. The plaintiffs point out that the FATCA agreement does provide a scant reference to "confidentiality and other protections provided for in the Convention" (article 3.7. of the agreement). However, it contains nothing in terms of

[20] European Data Protection Board (EDPB), Guidelines *02/2018 on derogations of Article 49 under Regulation EU 679/2016 of 25 May 2018*: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf

[21] Article 26(1) of Directive 95/46/EC states that it applies by way of derogation from Article 25 (on the principle of adequacy) in cases where the third country does not ensure an adequate level of protection within the meaning of Article 25(2) of the Directive. Article 26(2) states that *"Without prejudice to paragraph 1, a Member State may authorise a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses*".

[22] Article 17 of the Act of 16 December 2015: *"§ 2. Insofar as these transfers form part of a reciprocal exchange of information for tax purposes and are conditional on Belgium obtaining comparable information allowing it to improve compliance with the tax obligations to which taxpayers subject to tax in Belgium are subject, these transfers are necessary to safeguard an important public interest in Belgium. To this extent, such transfers are carried out in compliance with article 22, § 1, paragraph 1, of the above-mentioned Act of 8 December 1992 when they are made to a jurisdiction outside the European Union which is not generally considered to ensure an adequate level of protection".* Underlined by the Litigation Chamber.

[23] European Data Protection Board (EDPB), *Guidelines 02/2020 on Article 46(2)(a) and (3)(b) of the GDPR of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies of 15 December 2020*: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22020-articles-46-2-and-46-3-b-regulation_en

"appropriate safeguards" apart from a few vague objectives and a list of data that does not respect the principles of necessity and data minimisation (see below).

61. More specifically, the plaintiffs believe that the defendant failed to assess the level of protection offered by the United States or at the very least failed to justify the "adequacy" of any safeguards and measures put in place on either side as it was incumbent upon it to do, pursuant to the Schrems II judgment of the CJEU and EDPB Guidelines 02/22020 in order to validly rely on Article 46(2)(a) of the GDPR, which it now invokes.

62. The plaintiffs point out that the following mandatory safeguards are lacking: (a) specification of the types of processing, (b) the principle of purpose limitation, (c) the principle of data minimisation, (d) the principle of storage limitation, (e) a list of security measures including a mutual notification mechanism for data breaches, (f) the rights of data subjects: (i) information and transparency, (ii) access, rectification, erasure, restriction and objection: the plaintiffs point out that while the US Privacy Act to which the FATCA agreement refers appears to provide for similar rights, these rights are not included in the agreement. Moreover, the IRS does not communicate on these rights that data subjects would have, (iii) Prohibition of automated decisions: according to the plaintiffs, it is not excluded that an automated decision takes place after the transfer to the IRS given the objective pursued by the U.S. authorities, as specified during the draft law that led to the Act of 16 December 2015, as follows (freely translated): "*This information will provide the other State with more resources to improve tax compliance by its residents (and citizens in the case of the US) and to make best use of the information provided via automatic cross-checking with domestic intelligence and automated data analysis*[24]."

63. In conclusion, the plaintiffs are of the opinion that, failing to comply with the prescriptions of Chapter V of the GDPR, the denounced data transfers carried out by the defendant to the IRS are unlawful.

- *As regards the principles of purpose, necessity and data minimisation*

64. *With regard to the principle of purpose*, the plaintiffs consider that the purposes pursued by the FATCA agreement are not sufficiently defined, in that they are too vaguely and broadly aimed at (a) improving compliance with international tax rules and (b) implementing the obligations arising from the US FATCA legislation aimed at tackling tax evasion by US nationals (see in particular the introductory recitals to the agreement). The plaintiffs further denounce the fact that the data exchanged may also, via other instruments, be used for non-tax purposes, including purposes such as combating the financing of terrorism where applicable under the conditions of Article 17 of the Act of 16 December 2015[25].

[24] Underlined by the Litigation Chamber.

[25] See note 16 above.

65. As regards the principles of necessity and data minimisation, the plaintiffs denounce the aggressive nature of the data processing implemented by the FATCA agreement, under the terms of which an *automatic* exchange of data takes place rather than a transfer of data following an *adhoc* request. In their view, this model raises important questions of necessity and data minimisation: the plaintiffs are of the opinion that the collection of data under the FATCA agreement is not necessary and does not respect the principle of data minimisation. In support of both the relevant work of the Article 29 Working Party (hereinafter Art. 29 WP) and the EDPB and the rulings of the CJEU (points 66 et seq. below), the plaintiffs are of the opinion that, in the absence of specific criteria justifying the processing operations, the collection and transfer of the data concerned to the IRS are disproportionate, contrary to the principle of data minimisation enshrined both in Article 5(1)(c) of the GDPR and in Article 6(1)(c) of Directive 95/46/EC already. They also recall Article 52 of the Charter of Fundamental Rights of the Union (hereinafter the Charter), which states that "*Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others (...)*".[26]

66. The plaintiffs take particular note of the CJEU's[27] ruling of 8 April 2014, which annulled Directive 2006/24/EC *on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks* in that this directive "*applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime*". They also cite the CJEU ruling of 24 February 2022[28], which prohibits the general and undifferentiated collection of personal data for the purpose of combating tax fraud. The plaintiffs believe that the collections and transfers under the FATCA agreement are carried out in the same general and undifferentiated manner, and should be prohibited under the case law cited. In the same vein, the plaintiffs also highlight DPA opinion 122/2020[29]. With regard to the specific situation of Belgian accidental Americans, the plaintiffs make it clear that they are not saying that before every exchange of information under the FATCA agreement, the defendant must carry out an *ex ante* check based on its own criteria to determine whether or not a particular account holder represents a low or high risk of tax evasion. They do however specify that, in view of the notion of tax evasion as defined in American law by 26 US Code, section

[26] Underlined by the Litigation Chamber.

[27] CJEU, judgment of 8 April 2014, joined cases C-293/12 and C-594/12 Digital Rights Ireland, ECLI: EU :C :2014 :238, point 58.

[28] CJEU, judgment of 24 February, 2022, case C-175/20, ECLI :EU :C :2022 :124, points 74 to 76.

[29] Data Protection Authority, Opinion 122/2020 on Chapter 5 of Title 2 of the draft programme law - articles 22 to 26 inclusive (French only): https://www.autoriteprotectiondonnees.be/publications/avis-n-122-2020.pdf See point 25.

7201, it is incomprehensible that the defendant should, for example, ignore the income threshold below which US citizens living abroad for 330 days (including accidental Americans) can ask the IRS to exclude income earned abroad, via the clause in Annex II of the agreement which allows other categories of accounts to be excluded from the FATCA declaration, even after the agreement has been signed.

- *As regards information and transparency*

67. The plaintiffs address this aspect both as a safeguard to be included in the FATCA agreement pursuant to Article 46(2)(a) of the GDPR (point 62) and as a stand-alone grievance (Title II.E.2).

68. They denounce that contrary to what is requested by the EDPB under its Guidelines 02/2020, neither the FATCA agreement nor the international conventions to which the agreement refers contain provisions on transparency and the provision of information as an "appropriate safeguard" pursuant to Article 46(2)(a) of the GDPR used by the defendant.

69. The plaintiffs also point out that the defendant does not even attempt to comment on the existence of and compliance with such an obligation of transparency on the part of the IRS, even though this is required by Article 16(3) of the Act of 16 December 2015[30]. At most, the IRS would be required to comply with the principle of transparency applicable to it under its domestic legislation, which does not translate into an obligation equivalent to what is required under Article 14 of the GDPR.

70. The plaintiffs add that point 2.4.1. of EDPB Guidelines 02/2020 clearly states that *"Individual information to data subjects should be made by the transferring public body in accordance with the notification requirements of Articles 13 and 14 GDPR"* and concludes that *"a general information notice on the website of the public body concerned will not suffice"*. In this respect, the plaintiffs consider that the defendant's website does not present the required information and that the reference to certain pages of this site does not constitute an active form of communication[31].

71. The plaintiffs further complain that since the defendant states that it relies on "appropriate safeguards" within the meaning of Article 46 of the GDPR, it was specifically obliged to comply with Article 14(1)(f) of the GDPR and to indicate *"reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available"*.

[30] Article 16.3 of the Act of 16 December 2015 (freely translated): *"Notwithstanding the other provisions of the law, the application of the law is postponed or suspended with regard to a jurisdiction which is not a member of the European Union if it is established that this jurisdiction has not put in place an infrastructure which guarantees that the financial institutions established on its territory and its tax administration sufficiently inform Belgian residents of the information concerning them which will be communicated by this jurisdiction within the framework of an automatic exchange of information relating to financial accounts. (...) "*.

[31] Article 29 Working Party, *Guidelines on transparency under Regulation* (EU) 679/2016 (WP 260): https://ec.europa.eu/newsroom/article29/items/622227 These guidelines were taken up by the EDPB at its inaugural meeting on 25 May 2018.

72. Finally, the plaintiffs consider that the defendant cannot[32] rely on Article 14(5)(c) of the GDPR since the appropriate measures required to be able to resort to this exception are not provided for by Belgian legislation.

➢ *As regards the absence of a DPIA*

73. The plaintiffs believe that the defendant was required to carry out a DPIA even before the GDPR came into force. In their view, this obligation derives implicitly from article 22.2. of the LVP and article 26(2) of Directive 95/46/EC, and more generally from article 16.4. of the LVP, which transposes article 17(1) of Directive 95/46/EC. The plaintiffs also cite the *Art. 29 WP Guidelines of 16 December 2015*, which already recommended that EU member states carry out a DPIA in the context of automatic data exchange for tax purposes[33].

74. Finally, the plaintiffs believe that, in any event, Article 35 of the GDPR introduces this obligation for processing operations with a *high risk*, which is, they believe, the case for the denounced processing operations. On the basis of several criteria drawn from the *EDPB Guidelines on data protection impact assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation (EU) 2016/679* (hereinafter the EDPB DPIA Guidelines)[34], the plaintiffs conclude that a DPIA was required in this case. The plaintiffs cite the following criteria: systematic monitoring, sensitive data or data of a highly personal nature, data processed on a large scale, cross-referencing or combination of data sets, data concerning vulnerable persons, and, to a certain extent, processing "which prevents the exercise of a right or the benefit of a service or contract".

75. By failing to carry out a DPIA within the meaning of Article 35 of the GDPR, the defendant has breached this provision, in the plaintiffs' view.

➢ *As regards accountability*

76. The plaintiffs point out that the principle of accountability requires the controller to comply with the GDPR but also to be able to demonstrate this compliance at any time. The plaintiffs believe that no EU member state is currently in a position to demonstrate this, including Belgium.

➢ *As regards article 20 of the LTD (obligation to conclude a protocol)*

77. Finally, under the terms of their complaint, the plaintiffs denounce a breach of Article 20 of the LTD, which provides that (freely translated) *"unless otherwise provided in specific laws,*

[32] The plaintiffs anticipate a possible argument from the defendant, which the latter will not raise.

[33] Article 29 Working Party, Guidelines for Member States on the criteria to ensure compliance with data protection requirements in the context of automatic exchanges of personal data for tax purposes, WP 234 of 16 December 2015: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp230_en.pdf

[34] Article 29 Working Party, *Guidelines on data protection impact assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation (EU) 2016/679* (WP 248): file:///C:/Users/win-verbvale/Downloads/20171013_wp248_rev_01_en_D7D5A266-FAE9-3CA1-65B7371E82EE1891_47711-1.pdf These Guidelines were taken up by the EDPB at its inaugural meeting on 25 May 2018.

pursuant to Article 6(2) of the Regulation [i.e. GDPR], the federal public authority that transfers personal data under Article 6(1)(c) and (e), of the Regulation [i.e. GDPR] to any other public authority or private organisation, shall formalise this transfer for each type of processing in a protocol between the initial controller and the controller receiving the data (§1)". Consequently, according to the plaintiffs, the defendant was obliged to enter into a protocol with the IRS, within the meaning of article 20 of the LTD.

78. In their conclusions in reply, however, the plaintiffs state that they have abandoned their argument that this provision has been breached.

I.B.6.2. Position of the defendant

79. On 16 May 2022, the Litigation Chamber received the defendant's summary conclusions.

80. The defendant's arguments, grievance by grievance, can be summarised as follows.

- *As regards compliance with rules governing cross-border transfers and as regards Article 96 of the GDPR*

81. The defendant does not deny that prior to its conclusions (in its decision of 4 October 2021 - point 22), it argued that Article 49(1)(d) of the GDPR allowed it to make the denounced data transfer to the IRS. It adds that, in reality, Article 49(1)(d) of the GDPR cannot be applied in this case since this transfer is not occasional.

82. As already mentioned, the defendant states that it relies on Article 46(2)(a) of the GDPR [35]since, in its view, the transfer of data to the IRS is based on a "*legally binding and enforceable instrument between public authorities or bodies that does not require any specific authorisation from the national supervisory authority*" within the meaning of that provision. In this regard, the defendant points out that the *binding and enforceable instrument* is, on the one hand, the FATCA agreement and, on the other hand, the Act of 16 December 2015, and that these are both national and international legally binding and enforceable instruments over which it has no control and which are, moreover, part of a global international framework recalled in point 9.

83. The defendant further invokes the above-mentioned Article 96 of the GDPR. It argues in support of its application that the FATCA agreement complied with EU law at the time it was concluded and that this is undoubtedly apparent, as the IS points out in its investigation elsewhere (points 37 et seq.):

[35] Article 46 of the GDPR: 1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. 2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by (a) a legally binding and enforceable instrument between public authorities or bodies [..]

- CPP opinions 61/2014 and 28/2015 on the draft Act of 16 December 2015;
- The deliberation 52/2016 of the SCFA of the CPP of 15 December 2016 authorising the defendant to transmit the financial information of declarable accounts of US taxpayers transmitted to it by financial institutions under the FATCA agreement, to the IRS, this deliberation is still in effect by virtue of article 111 of the LCA.
- The ruling of the Constitutional Court of 9 March 2017, which states that the Act of 16 December 2015 complies with the LVP through Article 22 of the Constitution and Article 8 of the European Convention on Human Rights (ECHR).

84. In conclusion, the defendant argues in support of these elements that the FATCA agreement was at the very least consistent with EU law applicable prior to 24 May 2016. As the conditions of Article 96 of the GDPR had been met, there was no reason for the defendant not to apply the Act of 16 December 2015. It adds that it cannot be blamed for not having carried out any other compliance assessment, since the legislator had done so itself, by seeking the opinion of the CPP and incorporating the latter's remarks.

85. The defendant adds that the fact the plaintiffs invoke the Schrems II judgment of the CJEU is irrelevant, and that they give this decision a scope that it does not have, since the judgment concerned the transfer of personal data for *commercial* purposes, which is not the case here, since it involves a transfer of data between public authorities for the purposes of taxation and combating tax fraud and evasion, with no commercial scope. Moreover, according to the defendant, there is clearly no large-scale collection of personal data within the meaning of this judgment.

86. As to whether there are appropriate safeguards within the meaning of Article 46(2)(a) of the GDPR, the defendant considers that the essential principles of the GDPR are in any event respected, regardless of Article 96 of the GDPR (see below). The defendant refers in this respect to the notification of the data protection measures and infrastructure required by article 3.8. of the FATCA agreement cited above[36], which attests that it has indeed carried out this analysis of whether there were adequate safeguards.

87. *As regards automated decisions*, the defendant maintains that there is no doubt that the processing it carries out under the FATCA agreement does not fall within the scope of Article 22 of the GDPR since it is "neither processing which produces legal effects concerning the data subject" nor "similarly significantly affects him or her". The defendant insists on its exclusively logistical role in this respect. Even supposing that the processing does fall within the scope of Article 22 of the GDPR, *quod non* according to the defendant, the latter considers itself to be in one of the cases of exception. More specifically, Article 22(2)(b) of the GDPR would find

[36] See note 18 above.

application in support of Recital 71, which explicitly mentions that *"decision-making based on such processing [referred to in Article 22.1.] (...) should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes (...)".*[37]

88. Finally, as to the retention period, the defendant states that the answer is given by Article 12(4) of the Act of 16 December 2015, which provides that (freely translated) *"reporting financial institutions shall keep the computerised databases that they have communicated to the Belgian competent authority for seven years from 1 January of the calendar year following the calendar year in which they communicated them to that authority. The databases are deleted on expiry of this period"*, as well as by article 15(3) of the same Act, which sets the same period of 7 years for the defendant to retain databases transferred to the competent authority of another jurisdiction, i.e. the IRS in this case. In this respect, the defendant rejects the plaintiffs' position, which artificially attempts to separate the FATCA agreement from the Act of 16 December 2015 (with regard to the principle of storage limitation discussed here in particular) and more generally from other rules on automatic exchanges of information in tax matters to which the defendant is *bound.*

- *As regards the principles of purpose, necessity and data minimisation*

89. *As regards purpose limitation*, the defendant refers to Article 3.8. of the FATCA agreement as well as Article 17 of the Act of 16 December 2015[38]. It also refers to the above-mentioned opinions and authorizations of the CPP (point 83).

90. *With regard to the principles of necessity and data minimisation*, the defendant highlights the following elements which, in its view, demonstrate compliance with the above-mentioned principles: (1) in compliance with the FATCA agreement, only data concerning US citizens subject to US tax legislation is transmitted to the IRS; (2) banks are not obliged to consider as declarable bank accounts whose balance or value does not exceed a certain amount (focus of the FATCA agreement on high-value balances); (3) only the data listed in article 2.2. of the FATCA agreement is transferred, and this data is necessary for the identification of taxpayers and the performance of its duties by the IRS pursuant to articles 4 and 22 of the Multilateral Convention of 1988. Here again, the defendant relies on the above-mentioned authorisation of the SCFA and the ruling of the Constitutional Court of 9 March 2017, which appears to have validated the *proportionality* of the data processed. The defendant also considers that the plaintiffs' reference to the ruling of the CJEU of 8 April 2014 is irrelevant, since in this case,

[37] Underlined by the Litigation Chamber.

[38] See note 16 above.

unlike the situation referred to in that ruling, there is no general and undifferentiated collection. The defendant points out that the data collection only involves a specific category of people (American nationals) and establishes a threshold below which the declaration is not required. There would therefore be precise criteria justifying collection.

➢ *As regards information and transparency*

91. The defendant states that its website provides comprehensive information combining more theoretical explanations, news, links to relevant documents and an FAQ.

92. It adds that under the terms of Article 14 of the Act of 16 December 2015 (freely translated) "*each reporting financial institution shall inform each natural person concerned that personal data concerning him or her will be transferred to the competent Belgian authority*" and that it is therefore in any event up to the banks to inform the data subjects, such as the first plaintiff and Belgian accidental Americans. This data is the following:

- The purposes of the transfer of personal data (a);
- The recipients or ultimate recipients of the personal data (b);
- The declarable accounts for which personal data are transferred (c);
- The existence of a right to obtain, on request, communication of the specific data that will be or has been transferred a declarable account and the procedures for exercising this right (d);
- The existence of a right to rectify personal data concerning the individual and how to exercise this right (e).

93. The defendant also states that this information was provided to the first plaintiff by its bank Z on 18 May 2020 (point 16). During the hearing, the defendant clarified that it could therefore rely on the information exemption provided for in Article 14(5)(a) of the GDPR.

➢ *As regards the fact there was no DPIA*

94. Referring to Article 35 of the GDPR, the defendant mentions that its DPO specified in a letter dated 30 June 2021 addressed to the Inspector General that (freely translated) "*according to the working methodology adopted by the FPS Finance [i.e. the defendant], and developed by the 'Service de Sécurité de l'information et de Protection de la Vie privée' (SSIPV), a pre-impact assessment had been carried out*".

95. On the basis of this pre-impact assessment, the defendant's DPO states that it was concluded that a DPIA was not necessary, since:

- The Act of 16 December 2015 had incorporated the remarks made by the CPP in its two opinions 61/2014 and 28/2015 cited above;

- The SCFA had issued a resolution authorising the transmission of data to the IRS and that the conditions of this resolution had been implemented;
- The processing complied with the requirements of the AEOI standard on confidentiality and data protection, as well as the defendant's information security policies based on the ISO 27001 standard;
- The US authorities are also required to provide the necessary security measures to ensure that the information remains confidential and is stored in a secure environment, as provided for in the FATCA *Data safeguard workbook*.

96. The defendant adds that the contents of this letter were reproduced *in extenso* in the follow-up investigation report of the IS (point 40).

97. The defendant also believes that the plaintiffs have not demonstrated any elements to justify a DPIA. It is of the opinion that the criteria set out in the EDPB DPIA Guidelines are not met in the context of the processing it carries out. It stresses that it does not analyse the data, but only prepares it for direct transfer to the IRS.

➢ *As regards accountability*

98. The defendant considers that, in view of the elements reported with regard to the above points, it sufficiently demonstrates that it complies with Article 5(1) of the GDPR.

➢ *As regards article 20 of the LTD (obligation to conclude a protocol)*

99. The defendant points out that although the plaintiffs claimed that this article had been breached in their complaint, they abandoned it in their conclusions in reply. The defendant, for its part, considers that it is clear from the preparatory work of the LTD that the obligation to conclude such a protocol is not applicable in the case of data transfers to or from third countries within the meaning of the GDPR. Since the transfer in question took place to the United States, the company cannot be accused of any breach.

I.B.6.3. Additional conclusions on the ruling of the Constitutional Court of 9 March 2017

100. On 17 August 2022, the Litigation Chamber exceptionally authorised the parties to make additional conclusions, on the reference to the ruling of the Constitutional Court of 9 March 2017 made by the defendant in its above-mentioned summary conclusions.

101. On 31 August 2022, the Litigation Chamber received the additional conclusions of the plaintiffs. In it, the plaintiffs insist above all on the fact that since the ruling dates back to 2017, the Constitutional Court was unable to take into account the evolution of case law relevant to assessing whether the FATCA agreement complies with data protection rules, in particular the lack of proportionality of the collection of the personal data of data subjects, and the subsequent transfer of this data. In 2017, the CJEU had already initiated its case law on the

principles to be taken into account when analysing the proportionality of a legislative measure under Article 8 of the ECHR and Articles 7, 8 and 52 of the Charter. According to the plaintiffs, judgment C-175/20 of 24 February (paragraph 66) leaves no doubt as to the unlawfulness of generalised data collection in the specific context of the fight against tax fraud. In this respect, the plaintiffs stress that in this judgment, the CJEU rejects the distinction suggested by the Advocate General between, on the one hand, ex-ante research and detection, for which the proportionality requirement could be assessed more flexibly in his view, and, on the other hand, *ex-post* verification in a specific case, to be assessed more strictly in his view[39]. According to the plaintiffs, the data listed in the agreement, as well as the thresholds[40] provided for in the agreement (below which the account is not declarable), do not constitute criteria within the meaning of the CJEU's case law; in fact, there is no analysis of the risk of tax evasion or fraud on the part of the persons whose data is processed. Finally, the plaintiffs point out that the Constitutional Court was unable to take into account the study of May 2018 commissioned by the European Parliament[41], which states that FATCA reporting obligations are not sufficiently limited with regard to the risk of tax evasion.

102. On 21 September 2022, the Litigation Chamber received the defendant's additional conclusions on the same judgment. The defendant's main demand is that the Litigation Chamber set aside those aspects of the plaintiffs' additional conclusions that go beyond the request made by the Litigation Chamber. According to the defendant, the plaintiffs are in fact going beyond the Litigation Chamber's invitation by once again putting forward arguments concerning the minimisation/proportionality of data.

103. For the remainder, the defendant also invokes Article 96 of the GDPR with regard to the claim that the principle of data minimisation has been breached, raised by the plaintiffs[42].

104. With regard to the ruling of the Constitutional Court itself, the defendant insists, as it did in its summary conclusions, that the ruling has the character of legal/constitutional truth. It adds that, after a precise and comprehensive analysis, the Constitutional Court considered that the Act of 16 December 2015 and, consequently, the FATCA agreement, were not inconsistent with either to Article 22 of the Constitution, or to the LVP, or to Directive 95/46/EC, including the condition of proportionality. There was therefore no reason for it to refuse to apply the Act of December 16, 2016.

[39] See CJEU, case C-175/20 - Opinion of Advocate General Michal Bobek delivered on 2 September 2021, paragraphs 70 et seq.

[40] In this respect, the plaintiffs cite CJEU judgment C-184/20, Vyriausioji tarnybinės etikos komisija, ECLI :EU :C :2022 :601.

[41] See https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604967/IPOL_STU(2018)604967_EN.pdf

[42] Indeed, the Litigation Chamber notes that in its summary conclusions, given the structuring of the titles used, the defendant appeared to invoke Article 96 of the GDPR only with regard to the appropriate safeguards that must accompany the transfer of data to the IRS.

105. Lastly, the defendant points out that if the Litigation Chamber were somehow to consider the case law of the CJEU cited by the plaintiffs - *quod non* - it would find that the plaintiffs had drawn erroneous conclusions from it. As such, the defendant argues that in the judgment C-175/20 of 24 February 2022 relied on by the plaintiffs, the CJEU asks the referring court to verify whether the Latvian administration would be able to target advertisements by means of specific criteria. In this respect, the defendant considers that, as the Belgian Constitutional Court has qualified the collection of data - listed by law - in implementation of the FATCA agreement and the Act of 16 December 2015 as proportionate, the CJEU's concern has been addressed.

I.B.7. The hearing of the parties

106. By e-mails dated 17 August and 8 September 2022, the parties were informed that the hearing would take place on 13 September 2022. This hearing was subsequently postponed to 7 November 2022 and then to 10 January 2023.

107. On 23 September 2022, the plaintiffs submitted 2 documents to the Litigation Chamber, which they described as "new documents" in the case. Specifically, these include an opinion of 23 August 2022 from the Slovak Data Protection Authority on the FATCA agreement and whether it was compliant with the GDPR (and its unofficial French translation), as well as the updated report of September 2022 "*FATCA legislation and its application at international and EU level - an update*" of the 2018 report commissioned by the European Parliament.

108. This led to an exchange of letters between the parties concerning the admissibility of these documents, which had been sent outside the deadlines set for the submission of their respective conclusions and documents.

109. On 3 October 2022, the Litigation Chamber informed the parties that it would give them the opportunity to comment on these documents at the start of the hearing.

110. On 10 January 2023, the parties were heard by the Litigation Chamber. At the hearing, and as reflected in the minutes, the Litigation Chamber indicated that it was authorised to inspect all relevant documents. No document is excluded from the proceedings, provided that it is possible to exercise the rights of defence with regard to them, either during the hearing or, if necessary, afterwards. The parties did not return to this point.

111. On 27 January 2023, the minutes of the hearing were submitted to the parties. The Litigation Chamber received no comments from the latter on these minutes.

*

II. JUSTIFICATION

II.A. As regards the competence of the Litigation Chamber of the DPA

112. Among other things, the GDPR has entrusted European data protection authorities ("supervisory authorities") with the task of handling complaints submitted to them (Article 57(1)(f) of the GDPR). These authorities must investigate such complaints with all due diligence[43].

113. In carrying out their duties, including handling complaints, data protection authorities must strive to consistently apply the GDPR throughout the EU. To this end, they cooperate with each other in accordance with Chapter VII of the GDPR (Article 51(2) of the GDPR).

114. In this case, the complaint submitted to the Litigation Chamber for examination concerns the transfer (i.e. processing within the meaning of Article 4(2) of the GDPR) of personal data (within the meaning of Article 4(1) of the GDPR) by a Belgian public authority (the defendant) to a foreign public authority (the IRS) pursuant to the FATCA agreement and the Belgian Act of 16 December 2015. **The single point of contact mechanism provided for in Article 56 of the GDPR does not find application in view of Article 55(2) of the GDPR, which provides that "*2. Where processing is carried out by public authorities or private bodies acting on the basis of point (c) or (e)[44] of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 56 does not apply.*** The DPA is nonetheless unquestionably competent to process it pursuant to Article 55 of the GDPR and Article 4 of the LCA.

115. As this transfer takes place in execution of an intergovernmental agreement, admittedly a bilateral one between Belgium and the United States, but similar in content to other bilateral agreements signed by the United States with other EU member states, whether the transfer of this data is compliant with the GDPR based on this agreement, even bilateral (and supplemented by national legislation), must be assessed with the same consistency in the various EU member states to the extent possible.

116. To this end, **the Litigation Chamber will take account in particular of the Guidelines relevant to this case issued by both the Art 29 WP[45] and the EDPB[46], as well as the relevant judgments of the CJEU**.

---

[43] Judgment of the court of 16 July 2020, C-311/18, Facebook Ireland and Schrems (Schrems II), ECLI:EU:C:2020:559, point 109.

[44] The defendant processes the data pursuant to an international agreement and Belgian legislation.

[45] Article 30(1)(a) of Directive 95/46/EC entrusted the Article 29 Working Party (Art. 29 WP) with the task of examining all questions relating to the implementation of national provisions adopted pursuant to this directive, with a view to striving toward the uniform application thereof. Under article 30(1)(b), Art. 29 WP was tasked with advising the European Commission on the level of protection in third countries.

[46] As set out in Recital 139 of the GDPR, the EDPB is set up for the purpose of promoting the consistent application of the GDPR in the EU through its various activities. It follows both from this Recital 139 and from the tasks entrusted to it under Article 70 of the GDPR that the EDPB has an essential role to play with regard to the consistent application of the rules laid down by the GDPR with regard to cross-border data flows. See in this respect, in addition to the reference to its task of

II.B. As regards the sovereign judgment of the Litigation Chamber

117. As set out in the background to the procedure, the defendant repeatedly stresses in its conclusions that the inspection reports did not find any failures on its part, and that the arguments it gave during the investigation are the basis for the conclusion reached in the reports of the IS.

118. As it had already done in its decision 81/2020, the Litigation Chamber specifies that recourse to the Inspection Service is not systematically required by the LCA. In fact, it is up to the Litigation Chamber to determine whether or not an investigation is necessary following the lodging of a complaint (article 63, 2° LCA - article 94, 1° LCA). The Litigation Chamber may therefore decide to deal with the complaint without referring it to the IS (art. 94, 3° LCA).

119. When a case is referred to the IS, its findings will undoubtedly enlighten the Litigation Chamber as to the facts of the complaint and how these facts should be qualified under data protection regulations. As such, they can be used to support one or other of the breaches ultimately upheld by the Litigation Chamber in its decision. Nevertheless, **the Litigation Chamber remains free to conclude, with reasons, that there are shortcomings in the case which the inspection report(s) would not have raised, based on all the documents produced during the proceedings, including the arguments developed during the adversarial debate following its decision to deal with the case on the merits (article 98 of the LCA).**

II.C. As regards the status of the defendant as controller

120. The Litigation Chamber notes that the defendant claims the status of controller[47] in support of article 13(2) of the Act of 16 December 2015, which explicitly qualifies it as such, both in its conclusions and at the hearing[48].

121. Article 13(2) stipulates that *(freely translated) "§ 2. For the purposes of the Act of 8 December 1992, each reporting financial institution and the FPS Finance [i.e. the defendant] are considered to be "controllers" of "personal data" as regards the information referred to in this law which relates to natural persons[49]".*

advising the European Commission on the level of protection in third countries, litera (c), (i), (j) and (s) of Article 70 as well as Article 64(e) and (f) of the GDPR, all of which specifically relate to the role of the EDPB with regard to such flows.

[47] See for example page 3 of the minutes of the hearing of 10 January 2023.

[48] As the Litigation Chamber points out in paragraph 208, the FATCA agreement does not provide for any qualification or definition in the area of data protection.

[49] Underlined by the Litigation Chamber.

122. The defendant is therefore expressly qualified as a controller under the terms of the Act of 16 December 2015. This Act obviously refers to the LVP repealed by the LTD (article 280 of the LTD). However, the definition of "controller" in Article 1.4. of the LVP and that used in Article 4(7) of the GDPR are identical.

123. Article 4(7) of the GDPR therefore states that the controller is "*any natural or legal person, public authority, service or other organisation which, alone or jointly with others, determines the purpose and methods of processing*". Article 4(7) adds that "*where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law*"[50]. This is the case for the defendant under Article 13(2) of the above-mentioned Act of 16 December 2015.

124. In its *Guidelines on the concepts of controller and processor in the GDPR*[51], the EDPB considers that where the controller has been specifically identified by law, this will be determinative for establishing who is acting as controller. This presupposes that the legislator has designated as controller the entity that has a genuine ability to exercise control.

125. On several occasions in its conclusions and at the hearing (see minutes of the hearing), the defendant also pointed out that it did not have access to the contents of the "bundle" of data it received from the financial institutions (in this case from Bank Z) for transfer to the IRS, *as an organisational measure to guarantee the security and integrity of the data*[52]. As already mentioned, the defendant does not deny that it is a controller (point 120).

126. Insofar as necessary, the Litigation Chamber wishes to point out that the fact that the defendant does not have access to the transferred data is irrelevant. Indeed, this element has no bearing on its status as controller, as the CJEU clarified in its Google Spain and Google judgment of 13 May 2014.[53]

---

[50] Underlined by the Litigation Chamber.

[51] European Data Protection Board (EDPB), Guidelines 07/2020 on the concepts of controller and processor in the GDPR, https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf (point 23).

[52] See the minutes of the hearing: the defendant's response to Mr. C. Boeraeve's question about the technical and organisational measures taken.

[53] CJEU judgment of 13 May 2014, C-131/12, Google Spain and Google, ECLI :EU :C :2014 :317, points 22 - 41, and especially points 22 and 34:

"22. According to Google Spain and Google Inc., the activity of search engines cannot be regarded as processing of the data which appear on third parties' web pages displayed in the list of search results, given that search engines process all the information available on the internet without effecting a selection between personal data and other information. Furthermore, even if that activity must be classified as 'data processing', the operator of a search engine cannot be regarded as a 'controller' in respect of that processing since it has no knowledge of those data and does not exercise control over the data".

"34. Furthermore, it would be contrary not only to the clear wording of that provision but also to its objective— which is to ensure, through a broad definition of the concept of 'controller', effective and complete protection of data subjects — to exclude the operator of a search engine from that definition on the ground that it does not exercise control over the personal data published on the web pages of third parties".

127. In conclusion, and in support of the combined reading of Article 4(7) of the GDPR and Article 13(2) of the Act of 16 December 2015, **the Litigation Chamber upholds the defendant's qualification as a controller with regard to the data processing challenged by the plaintiffs, namely the transfer of data to the IRS.**

128. As regards the financial institutions (in this case, Bank Z, with which the first plaintiff held bank accounts), they were deliberately not implicated by the plaintiffs[54]. They nonetheless play an important role in the chain of data processing that takes place in the context of the implementation of the FATCA agreement and the Act of 16 December 2015. In fact, they are the ones who first check the status of the account holders concerned by the obligation to provide data to the defendant. They are the ones who collect the data required under Article 2.2. of the FATCA agreement and Article 5 of the Act of 16 December 2015 and transfer it to the defendant who in turn performs the transfer to the IRS. As such, financial institutions are also qualified as controllers by the Belgian legislator for the purposes of the Act of 16 December 2015[55].

II.D. As regards Article 96 of the GDPR

129. As set out in paragraph 83, the defendant, relying on Article 96 of the GDPR, argues (taking into account favorable opinions from the CPP, a transfer authorisation from the SCFA of the CPP and the ruling of the Constitutional Court of 9 March 2017) that the FATCA agreement applied in combination with the Act of 16 December 2015 complies with EU law as applicable on 24 May 2016. The defendant therefore considers itself entitled to base the transfer of the first plaintiff's data in particular on these texts.

130. In view of this argument, the Litigation Chamber considers it necessary to **clarify the scope of Article 96 of the GDPR**. It sets out to do just that in the following paragraphs.

131. By opting for a regulation to replace Directive 95/46/EC, the European co-legislators chose to strengthen the harmonisation of personal data protection rules in the EU. The regulation is directly applicable in the domestic legal order of each Member State, and although it contains

See also CJEU judgment C-25/17, Jehovan Todistajat, EU:C:2018:551, paragraph 69 and CJEU judgment C-210/16, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388, paragraph 38, as well as the EDPB Guidelines 7/2020, cited above, on the concepts of controller and processor in the GDPR, paragraph 45.

[54] See the minutes of the hearing on this point.

[55] As mentioned in point 121, article 13(2) states that (freely translated) *"§ 2. For the purposes of the Act of 8 December 1992, each reporting financial institution and the FPS Finance [i.e. the defendant] are considered to be "controllers" of "personal data" as regards the information referred to in this law which relates to natural persons"*. Underlined by the Litigation Chamber.

In the context of this decision, the Litigation Chamber will not examine the question of whether or not the financial institutions and the defendant should be qualified as joint controllers within the meaning of Article 4(7) of the GDPR and, consequently, whether or not the conditions of Article 26 of the GDPR had to be complied with. In view of the grievances raised against the defendant, a possible qualification as joint controller is not likely to lead to a different decision by the Litigation Chamber.

a number of references to the national legislator, these do not call into question the objective of robust harmonisation.

132. By providing for the GDPR to apply two years after its entry into force, i.e. on 25 May 2018 (Article 99 of the GDPR), the European co-legislators not only granted a two-year compliance period for the new obligations of the GDPR, they also made it clear that on this same date of 25 May 2018, data processing already under way on 24 May 2016 had to comply with all of the GDPR's provisions.

133. In this regard, Recital 171 of the GDPR provides that "*Processing already under way on the date of application of this Regulation should be brought into conformity with this Regulation within the period of two years after which this Regulation enters into force*".

134. **This compliance is essential if the regulation's objective of robust harmonisation was to be achieved**. If processing which was under way before the GDPR came into force was not brought into line with it, two protection regimes would have coexisted. In essence, this would be contrary to the very nature of the regulation and, *a fortiori*, to that of a fundamental right enshrined in the Charter (article 8).

135. It is in the light of this *ratio legis* of the transitional provisions of the GDPR that Article 96 must be understood and applied, both in its material scope (rationae materiae) and in its temporal scope (rationae temporis).

136. Article 96 of the GDPR does not exempt controllers who perform data processing operations pursuant to international agreements concluded before 24 May 2016 either totally or indefinitely from both the material and temporal scope of the GDPR. Article 96, "*Relationship with previously concluded Agreements*" provides for a *transitional regime subject to conditions*, the objective pursued by Article 96 of the GDPR being "*to ensure comprehensive and consistent protection of personal data in the Union*" and to avoid any legal vacuum .[56]

II.D.1. As regards the material scope of Article 96 of the GDPR

137. **Only the content of the international agreement concluded by the Member State is covered by Article 96 of the GDPR, the wording of which unequivocally targets "*international agreements involving the transfer of personal data to third countries*".** The material scope of article 96 must be interpreted in strict compliance with this wording.

138. The Litigation Chamber notes here from the outset that Article 96 of the GDPR is invoked by the defendant only with regard to (1) the grievance alleging non-compliance with the

[56] This objective is expressly explained in Recital 95 of Directive 2016/680/EU, with regard to Article 61 of this Directive, which is identical to Article 96 of the GDPR. Recital 95 provides that "In order to ensure a comprehensive and consistent protection of personal data in the Union, international agreements which were concluded by Member States prior to the date of entry into force of this Directive and which comply with the relevant Union law applicable prior to that date should remain in force until amended, replaced or revoked. "(emphasis added by the Litigation Chamber).

framework for the transfer of data to the IRS[57] as well as with regard to (2) the grievance alleging breach of the principles of purpose, necessity and data minimisation. It does not appear to the Litigation Chamber that the defendant would invoke this Article 96 of the GDPR in light of all the data protection obligations incumbent on it. According to the Litigation Chamber's examination, Article 96 of the GDPR is therefore not invoked by the defendant with regard to the grievance based on a breach of the obligation to provide information, which is asserted against it by the plaintiffs, for example, nor is it invoked with regard to the applicability, where applicable, of Article 35 of the GDPR.

139. The Litigation Chamber shares this analysis. In fact, as the FATCA agreement does not contain any specific provisions concerning the obligation to provide information, for example, this is excluded from the scope of Article 96 of the GDPR. The application of Articles 12 and 14 of the GDPR by the defendant is therefore beyond doubt (see. Title II. E.2 below).

140. In addition, the new obligations arising from the GDPR will find full application: they are in fact non-existent in Directive 95/46/EC and therefore *a fortiori* not regulated in the FATCA agreement from 2014. To assert the contrary would be the same, for example, as admitting that a data breach on the part of the defendant does not have to be notified in compliance with the conditions laid down by Article 33 of the GDPR, or that the transfers denounced by the complaint do not have to be covered by the defendant's register of processing activities (Article 30 of the GDPR). This cannot be the case. **The application of Article 96 of the GDPR is circumscribed to the content of the agreement alone. The letter of Article 96 is clear on this point, and this reading is moreover consistent with the *ratio legis* of Article 96 which, as the Litigation Chamber will explain below (point 143), aims to safeguard the rights acquired by third countries under the terms of the said agreements.**

141. The Litigation Chamber will therefore assess whether or not the defendant was required to carry out a DPIA in the light of Article 35 of the GDPR without interference from Article 96 of the GDPR (see. Title II. E.3 below). The Litigation Chamber points out that the obligation of accountability also applies. Whether this was complied with by the defendant will be examined by the Litigation Chamber solely in the light of Articles 5(2) and 24 of the GDPR read together, without interference from Article 96 of the GDPR (see. Title II. E.4 below). Finally, the Litigation Chamber will assess whether the defendant is in compliance with article 20 of the LTD under the same conditions (see. Title II. E.5 below).

II.D.2. As regards the temporal scope of Article 96 of the GDPR

142. Article 96 of the GDPR provides for the continued application of international agreements involving transfers of personal data to third countries "*until amended, replaced or revoked*". Even if no specific deadline is set for such amendment, replacement or revocation, the fact they

[57] Point 6.2. of its summary conclusions and point 103 above.

are mentioned constitutes a time limit in itself. By these terms, **the co-legislators mean that keeping in place such international agreements is intrinsically limited in time. This reading is also the only one that, according to the Litigation Chamber, reconciles the GDPR's harmonisation objective (points 131 et seq. above), safeguarding the rights of third countries with which an international agreement has been concluded (point 143) and the principle of sincere cooperation of the Union's member states (point 144).**

143. Article **96 of the GDPR in fact aims to preserve the rights of third countries**. It is clear that negotiating an international agreement takes time, and that the rights acquired by a third country party to an international agreement cannot simply be annulled immediately as a result of new legislation coming into force, even though the agreement was in line with EU law at the time it was concluded.

144. **Without prejudice to the above, EU Member States are nonetheless obliged to comply with EU law**. This obligation derives from article 4(3) of the Treaty on European Union (TEU), which enshrines the principle of sincere cooperation between member states[58]. Article 4(3) of the TEU is binding on member states, including their independent data protection authorities entrusted with tasks based on applicable European law (Article 8(3) of the Charter and Articles 51 et seq. of the GDPR).[59]

145. In this respect, Article 96 of the GDPR is in line with Article 351 of the Treaty on the Functioning of the EU (TFEU)[60], with regard to which the CJEU has already ruled that:

- On the one hand, *"the rights and obligations arising from an agreement concluded before the date of accession of a Member State between it and a third country are not affected by the provisions of the Treaty. The purpose of that provision [i.e. Article 351 TFEU] is to make it clear, in accordance with the principles of international law, that application of the Treaty is not to affect the duty of the Member State concerned to respect the rights of third countries under a prior agreement and to perform its obligations thereunder[61]".*

[58] Article 4.3. TUE: Pursuant to the principle of sincere cooperation, the Union and the Member States shall, in full mutual respect, assist each other in carrying out tasks which flow from the Treaties. The Member States shall take any appropriate measure, general or particular, to ensure fulfilment of the obligations arising out of the Treaties or resulting from the acts of the institutions of the Union. The Member States shall facilitate the achievement of the Union's tasks and refrain from any measure which could jeopardise the attainment of the Union's objectives.

[59] See in this sense: Judgment of the CJEU of 15 June 2021, Facebook Ireland e.a. v. Gegevensbeschermingsautoriteit, C-645/19, ECLI:EU:C:2021:483, para 60.

[60] Article 351 of the TFUE: The rights and obligations arising from agreements concluded before 1 January 1958 or, for acceding States, before the date of their accession, between one or more Member States on the one hand, and one or more third countries on the other, shall not be affected by the provisions of the Treaties. To the extent that such agreements are not compatible with the Treaties, the Member State or States concerned shall take all appropriate steps to eliminate the incompatibilities established.

[61] CJEU, Judgment of 3 March 2009, C-205/06, ECLI:EU:C:2009:118, Commission v. Austria, para 33. This judgment relates to the second paragraph of Article 307 of the Treaty establishing the European Community (repealed by Article 351 TFEU). Article 307: "The rights and obligations arising from agreements concluded before 1 January 1958 or, for acceding States, before the date of their accession, between one or more Member States on the one hand, and one or more third

- On the other hand, practices must be brought into line with European law "*unless that practice is necessary in order for the Member State concerned to comply with obligations towards non-member States laid down in an agreement concluded prior to entry into force of the Treaty or to accession by that Member State*[62]*"*.

146. The Litigation Chamber therefore shares the view that it follows from this position of the CJEU that "*the meaning of the two paragraphs have been reconciled, and it is now safe to affirm that art. 351(1) TFEU provides temporary protection to allow the Member States not to incur international responsibility while the ultimate goal established by art. 351(2) TFEU (that is, the removal of all incompatibilities) is achieved in a sustainable (for the Member State involved) and lawful (from an international law perspective) manner*[63]*"*.

147. The Litigation Chamber cannot therefore subscribe to an interpretation according to which Article 96 of the GDPR would authorise, without any time limit, the continued application of international agreements concluded before 24 May 2016 - even if they complied with Directive 95/46/EC and EU law on that same date - without further compliance with the GDPR. Following such an interpretation, the co-legislators would have allowed, in defiance of the European case law cited above, for international agreements that complied with the state of Union law suspended on 24 May 2016 (including Directive 95/46/EC, which incidentally was repealed on 24 May 2018) to coexist without any time limit, on the one hand, and international agreements concluded after that date that were obligatorily compliant with the GDPR, on the other.

148. This reading of Article 96 of the GDPR would also imply that data protection authorities assess the compliance of these international agreements with regard to the state of the law on 24 May 2016 many years after that date, in particular in the light of a Directive 95/46/EC that has been repealed for a number of years that will only increase over time and without in any way taking into account developments in the case law of the CJEU with regard to key concepts of data protection that may be common to Directive 95/46/EC and the GDPR or with regard to the Charter.

149. **On the contrary, the Litigation Chamber is of the opinion that the fact that Article 96 of the GDPR does not provide for a** defined **time limit (with reference to a cut-off date or with reference to a number of years elapsed, for example) does not exempt EU**[64] **member states, controllers or data protection authorities from their respective obligations.**

countries on the other, shall not be affected by the provisions of this Treaty. To the extent that such agreements are not compatible with this Treaty, the Member State or States concerned shall take all appropriate steps to eliminate the incompatibilities established".

[62] CJEU, Judgment of 28 March 1995, C-324/93 The Queen / Secretary of State for the Home Department, ex parte Evans Medical and Macfarlan Smith, ECLI:EU:C:1995:84, p 33.

[63] Emphasis added by the Litigation Chamber: https://www.europeanpapers.eu/es/europeanforum/court-of-justice-finally-rules-on-analogical-application-art-351-tfeu

[64] Nor, more generally, states subject to the GDPR.

150. **As far as EU member states are concerned, Article 96 of the GDPR does not exempt them from (re)negotiating, in fulfillment of their duty of sincere cooperation, a GDPR-compliant agreement. The more time passes, the less acceptable the inertia of governments in this respect**. As early as 2021, data protection authorities - including the DPA - therefore invited EU member states to review their international agreements in light of the GDPR.[65]

151. The Litigation Chamber clarifies here that it is of the opinion that it is up to the Belgian State to negotiate a GDPR-compliant agreement, in fulfillment of its duty of sincere cooperation (Article 4(3) TEU - point 144). It points out that on the date of adoption of this decision, **7 years have passed since the GDPR came into force**. In this respect, the Litigation Chamber notes that no indication of the Belgian government's willingness to request a revision of the FATCA agreement has been brought to its attention in the context of this case.

152. The role of the Belgian State (like that of any other Member State that has signed a FATCA agreement comparable to the one signed by the Belgian State) does not, however, exempt the **controller** who, like the defendant, intends to rely on Article 96 of the GDPR, from examining whether the conditions for recourse to Article 96 are met. **Indeed, independently even of the accountability obligation (Title II.E.4), recourse to Article 96 of the GDPR intrinsically implies, by the condition it lays down (i.e. the compliance of the agreement with EU law as applicable on 24 May 2016), that the controller must carry out this assessment.**

153. **As regards the data protection authorities,** the Litigation Chamber is also of the opinion that the more time passes, the **less acceptable it is for them to be restricted in the exercise of the role entrusted to them by the GDPR** since 25 May 2018, a role which consists exactly as emphasised in points 113 et seq. in **contributing to the effective and uniform application of the GDPR**. In its Schrems II judgment cited above, the CJEU stresses in this regard the following with regard to the competence of supervisory authorities as enshrined in Articles 8(3) of the Charter and 57(1)(a) of the GDPR:

- *"(...) Each of those authorities is therefore vested with the power to check whether a transfer of personal data from its own Member State to a third country complies with the requirements laid down in that regulation (...) The exercise of that responsibility is of particular importance where personal data is transferred to a third country since, as is*

[65] Statement 04/2021 on international agreements including transfers of 13 April 2021: https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-042021-international-agreements-including_en
In it, the EDPB (EDPB) considers *"that, in order to ensure that the level of protection of natural persons guaranteed by the GDPR [..] is not undermined when personal data is transferred outside the Union, consideration should be given to the aim of bringing these agreements in line with the GDPR [..] for data transfers where this is not yet the case. The EDPB therefore invites the Member States to assess and, where necessary, review their international agreements that involve international transfers of personal data, such as those relating to taxation (e.g. to the automatic exchange of personal data for tax purposes), [..] which were concluded prior to 24 May 2016 (for the agreements relevant to the GDPR) [..] The EDPB recommends that Member States take into account for this review the GDPR [..], the relevant EDPB guidelines applicable to international transfers, as well as the case-law of the European Court of Justice, including the Schrems II judgment of 16 July 2020".*

clear from recital 116 of that regulation, 'when personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information" (points 107 and 108 of the judgment).

154. The Litigation Chamber will also pay particular attention to the following points:

- The CJEU imposes very strict conditions on *international agreements* that have an impact on the exercise of the rights to privacy and personal data protection enshrined in Articles 7 and 8 of the Charter. More specifically, it follows from Opinion 1/15 of the CJEU on the draft PNR agreement between Canada and the EU (as well as Judgment C-817/19 of 21 June 2022[66]) and the Schrems II judgment[67] that "*the communication of personal data to a third party, such as a public authority, constitutes an interference with the fundamental right enshrined in Article 7 of the Charter, whatever the subsequent use of the information communicated. The same is true of the retention of personal data and access to that data with a view to its use by public authorities. In this connection, it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference*" (point 124)[68].
- Any limitation on the fundamental rights enshrined in the Charter (including the fundamental right to data protection under Article 8) must satisfy the conditions of the above-mentioned Article 52(1) of the Charter, which states that "*Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others".*

155. **It follows from all of the above**, both (1) the ratio legis of Article 96 of the GDPR, and (2) the obligation of sincere cooperation which is imposed on Member States and, by extension, on supervisory authorities such as the DPA (of which the Litigation Chamber is the administrative litigation body), that (3) the necessary restrictive interpretation of Article 96 of the GDPR required by the CJEU since the effects of this article are such as to limit the exercise of fundamental rights, in particular the rights to privacy and data protection respectively enshrined in Articles 7 and 8 of the Charter**, that the "standstill" effect of Article 96 of the GDPR must be read and interpreted in a restrictive and proportionate manner.**

[66] CJEU, judgment C-817/19 of 21 June 2022, Ligue des droits humains, ECLI:EU:C:2022:491.

[67] See note 43 above.

[68] CJEU opinion of 26 July 2017 (EU-Canada PNR Agreement), ECLI:EU:C:2017:592, paras 123 and 124.

156. **The Litigation Chamber is therefore of the opinion that the text of Article 96 of the GDPR does not preclude the interpretation according to which its "standstill" effect diminishes over time and with the evolution of the interpretation of EU law, *a fortiori* with regard to principles already enshrined in Directive 95/46/EC and reprised as is in the GDPR. In its assessment of the use of Article 96 of the GDPR, the Litigation Chamber will therefore verify whether application thereof is necessary to safeguard the acquired rights of the United States with regard to the specific situation of the first plaintiff and the Belgian accidental Americans defended by the second plaintiff. In support of the obligation of sincere cooperation which weighs on it by extension, the Litigation Chamber will weigh the interests of the United States against the rights of the latter and could, if necessary, set aside Article 96 of the GDPR if its application were to have a disproportionate effect on those rights. In this weighing exercise, the Litigation Chamber will take the liberty, if need be, of taking into account case law developments since 24 May 2016.**

II.E. As regards the grievances reported

157. Pursuant to Article 44 of the GDPR, a party exporting data who, like the defendant, transfers personal data to a third country must, in addition to complying with Chapter V of the GDPR, also meet the requirements of the other provisions of the GDPR. All processing must comply with the GDPR in its entirety.

158. The Litigation Chamber will therefore first examine the conformity of the data transfer to the IRS (Title II.E.1).

159. This examination will involve analysing compliance with the principles of purpose, necessity and proportionality of the transfer by the defendant to the IRS from the perspective of the principles of purpose, necessity and proportionality/data minimisation enshrined both in Article 6(1)(b) and (c) of Directive 95/46/EC given the highlighted applicability of Article 96 on these aspects and in Article 5(1)(b) and (c) of the GDPR (Title II.E.1.1).

160. This examination will also involve analysing compliance with the specific framework for transfer to the United States as a third country required by Chapter V of the GDPR (and its equivalent under Directive 95/46/EC applied in combination with Article 96 of the GDPR as well) (Title II.E.1.2).

161. Finally, the Litigation Chamber will examine the defendant's obligations to provide information (Title II.E.2), to carry out a DPIA (Title II.E.3) and to ensure accountability (Title II.E.4), before concluding its analysis by examining compliance with article 20 of the LTD (Title II.E.5).

II.E.1. As regards the conformity of the transfer of data to the IRS

II.E.1.1. As regards the infringements of the principles of purpose, necessity and minimisation

II.E.1.1.1. As regards the principle of purpose limitation

162. The principle of purpose as enshrined in Article 5(1)(b) of the GDPR - as it was in Article 6(1)(b) of Directive 95/46/EC - requires that data be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Whether or not the data processed is actually necessary to achieve the purpose depends on whether the purpose is sufficiently specific. Objectives that are too broadly defined leave too much latitude to the controller, and do not allow effective application of the principle of purpose, an essential principle of data protection regulations.

163. With regard to the principle of purpose, the plaintiffs consider that the purposes pursued by the FATCA agreement are not sufficiently defined in that they are too vaguely and broadly aimed at (a) improving compliance with international tax rules and (b) implementing the obligations arising from the US FATCA legislation aimed at combating tax evasion by US nationals (see in particular the introductory recitals to the agreement).[69]

164. As early as 2015, the Article 29 Working Party specified in its WP 234 document specifically devoted to data protection requirements in the context of automatic data exchange that *"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"*. The CJEU upheld this requirement in its above-mentioned Opinion 1/15 (EU-Canada PNR), in which it ruled that an international agreement must be worded very precisely[70].

165. In the light of the foregoing**, the Litigation Chamber is of the opinion that the purposes stated in the FATCA agreement are not sufficiently specified** in that they do not make it possible to assess in what way the data processed are necessary to achieve the stated purposes. The wording means that neither data subjects nor the DPA can identify the exact purpose and, above all, the data processing that may result, even if the data processed has itself been listed (Article 2.2. of the FATCA agreement and 5 of the Act of 16 December 2015).

II.E.1.1.2. As regards the principles of necessity and data minimisation/proportionality

[69] See the following recitals: *"Whereas the government of the Kingdom of Belgium and the Government of the United States of America (...) desire to conclude an agreement to improve international tax compliance through mutual assistance in tax matters based on an effective infrastructure for the automatic exchange of information"* and *'Whereas, the Parties desire to conclude an agreement to improve tax compliance and provide for the implementation of FATCA based on domestic reporting and reciprocal automatic exchange pursuant to the Convention [read the Convention on mutual administrative assistance in tax matters done in Strasbourg on January, 25, 1988](...)".*

[70] See H. Hijmans, PNR Agreement EU-Canada Scrutinised: CJEU Gives Very Precise Guidance to Negotiators, European Data Protection Law Review, 2017/3.

166. As the plaintiffs point out, the transfer of data to the IRS in the context of the FATCA agreement is a system whereby data is automatically transferred every year, on the basis of the criterion of US nationality and declarable bank accounts (Articles 2 of the FATCA agreement and 5 of the Act of 16 December 2015) without any indication that any tax law has been violated, so it is not therefore a system where data is transferred on an *ad hoc* basis at the request of the US authorities, since there are indications that the data transfer must take place, given the stated purposes.

167. In this respect, the Litigation Chamber recalls the principle of proportionality (according to the terminology used in article 6(1)(c) of Directive 95/46/EC) or, another term, the principle of data minimisation (according to the terminology used in article 5(1)(c) of the GDPR) in application of which the data processing must be **strictly necessary to achieve the purpose.**

168. As early as 2015, the data protection authorities of the Article 29 Working Party insisted on the need to respect this principle in the FATCA context, in the following terms: "*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*".[71]

169. This position taken by the Art. 29 WP in its WP 234 followed the annulment of Directive 2006/24/EC by the CJEU under the terms of a judgment of 8 April 2014 on the grounds of failing to comply with the principle of proportionality. The court had therefore ruled that retaining data generated or processed in connection with the provision of publicly available communications services or of public communications networks was disproportionate in that this obligation applies (...) *"eeven to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime"*[72].

170. The Litigation Chamber agrees with the view stated by the Art. 29 WP at the time that there is no reason to limit this consideration to measures adopted in the fight against terrorism. Other public policy measures intended to pursue a specific purpose in particular through the collection of personal data are also subject to the same respect for the principle of proportionality of Article 6(1)(c) of Directive 95/46/EC then applicable and today in Article

[71] Art. 29 WP, *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*, WP 234 of 16 December 2015. Underlined by the Litigation Chamber.

[72] CJEU, judgment of 8 April 2014 C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and others, ECLI:EU:C:2014:238, pt 58.

5(1)(c) of the GDPR. This is the case for data collection imposed under agreements governing the automatic exchange of tax data, such as the FATCA agreement. For this reason, the analogy with the positions taken by the Art. 29 WP, the EDPB and, above all, the CJEU is particularly relevant.

171. The Art. 29 WP also stated, back in 2015, that *"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"*.

172. In 2017, the EDPS echoed these sentiments when it insisted in its guide to Assessing the necessity of measures that limit the fundamental right to the protection of personal data that *"Not everything that 'might prove to be useful" for a certain purpose is 'desirable or can be considered as a necessary measure in a democratic society. Mere convenience or cost effectiveness55 is not sufficient"*.

173. The EDPS also pointed out that the fact that the data transfers under FATCA took place every year in itself demonstrated that the transfers were not based on indications of fraud, but occurred systematically.

174. Finally, in 2018, a study commissioned by the European Parliament stated that the declaration requirements set out in the FATCA agreement were not sufficiently limited with regard to the risk of tax evasion. The study in question stated that *"In conclusion, FATCA restrictions operating within the EU through IGAs [intergovernmental agreements] at the current stage and under certain circumstances appear to be neither proportionate, nor necessary in so far they fail to narrow down the reporting obligations to individuals suspected of tax evasion. By contrast, these FATCA restrictions would constitute 'necessary and proportionate measures" upon the condition that the U.S. provided, on a case-by-case basis, specific evidence that U.S. expatriates are using the EU financial system to engage in offshore tax evasion. Lacking such evidence FATCA restrictions appear to go beyond what is strictly necessary to achieve the goal of fighting against offshore tax evasion"*. The updated version of this study comes to the same conclusion[73].

175. All these elements therefore already existed on 24 May 2016. They had to be taken into account from 2014 on, well before the GDPR came into force. They were repeated and reinforced in the years that followed, including after 24 May 2016, and the defendant could not have been totally unaware of this.

[73] See https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/734765/IPOL_IDA(2022)734765_EN.pdf

176. More recently,[74] on 24 February 2022, the CJEU issued a judgment in which it expressly stated that the general and undifferentiated collection of personal data for the purpose of combating tax fraud by a tax authority was not authorised. The administration concerned must refrain from collecting data that is not strictly necessary for the purposes of the processing operation (point 74 of the judgment). The administration must also consider whether its requests can be more targeted on the basis of more specific criteria. The CJEU made these considerations in the light of a request made by the Latvian tax authorities to an economic operator to provide it each month with the data relating to listings for passenger cars published on its website the previous month. According to the CJEU, even in the exercise of the public interest mission with which it has been entrusted, the controller cannot collect data in a general and undifferentiated manner, and must consider the possibility of further targeting, in this case targeting certain advertisements by means of specific criteria.

177. It follows from this judgment that the recipient of the data request is obliged to examine the merits of the request and to verify whether it is legally authorised to respond. Otherwise, the recipient of the request risks violating its own obligations under the GDPR.

178. In this respect, the Litigation Chamber is of the opinion that the mere nationality of the first plaintiff and, more generally, of the Belgian accidental Americans defended by the second plaintiff is an insufficient criterion in view of the purpose pursued. The fact that a list of data concerning them has been drawn up does not constitute a relevant and sufficient targeting criterion. The communication of personal data relating to all Belgian accidental Americans - of course excluding those whose account balances are below the declarable threshold - without any other indication of tax evasion or avoidance is disproportionate, a fortiori with regard to those who would not be subject to taxation in the United States, taking into account any exemptions authorised by American law, as pointed out by the plaintiffs[75].

II.E.1.1.3. Conclusion as regards the infringements of the principles of purpose limitation, necessity and data minimisation

179. **The case law cited with regard to the principles of necessity and data minimisation admittedly partly came after 24 May 2016[76]. However, it confirms the position adopted by**

[74] CJEU, Judgment of 24 February 2022, C-175/20, Valsts ieņēmumu dienests (Processing of personal data for tax purposes), ECLI:EU:C:2022:124. See also judgment C-817/19, Ligue des droits humains (PNR), cited above, of 21 June 2022: *"115. As regards observance of the principle of proportionality, the protection of the fundamental right to respect for private life at EU level requires, in accordance with settled case-law of the Court, that derogations from and limitations on the protection of personal data should apply only in so far as is strictly necessary. In addition, an objective of general interest may not be pursued without having regard to the fact that it must be reconciled with the fundamental rights affected by the measure, by properly balancing the objective of general interest against the rights at issue".*

[75] It should be noted in this context that the plaintiff's bank had specified in its letter of 22 April 2020 that the aim of the US legislation was to identify ALL accounts held by US citizens or residents, which at the very least attests to the difficulty in understanding the (overly broad, see below) purpose of the agreement.

[76] By citing this judgment in support of its reasoning, the Litigation Chamber neither grants nor rejects the plaintiffs' argument as requested by the defendant in its additional conclusions relating to the ruling of the Constitutional Court of 9

the CJEU from 2014 on, and on which, as has just been recalled, data protection authorities alerted as early as 2015 and have continued to do so ever since. In view of the diminishing standstill effect of Article 96 of the GDPR, the defendant could not fail to take this into account in its assessment of the use of Article 96 of the GDPR and the continuation of processing on this basis. In the opinion of the Litigation Chamber, the argument of a possible compromise of the rights acquired by the United States could not be invoked here, since prior to 24 May 2016, compliance with the principles of necessity and data minimisation/proportionality of the FATCA agreement had already been vitiated. Admittedly, the CJEU had not ruled on the FATCA agreement as such, but the interpretation it had given to the principles of necessity and data minimisation in a comparable context was therefore imperative with regard to both the FATCA agreement and the Act of 15 December 2016. This is all the more so in the wake of recent CJEU rulings in the same vein. The same conclusion applies with regard to the failure to comply with the principle of purpose limitation, a key principle of data protection since before the GDPR that has not been complied with (see above).

180. **In support of the above, the Litigation Chamber therefore notes that from 24 May 2016 on, the compliance of the data transfers provided for by the FATCA agreement and the Act of 16 December 2015 with the principles of purpose, necessity and proportionality/data minimisation could be seriously doubted. If doubts about this compliance were to remain in the eyes of some, *quod non* according to the Litigation Chamber, these doubts are completely dispelled in 2023 given the evolution of the CJEU's case law[77].**

181. In conclusion, the Litigation Chamber is of the opinion that **neither the FATCA agreement nor the Act of 16 December 2015 comply with the principles of purpose, necessity and data minimisation/proportionality. The Litigation Chamber concludes that the defendant can neither rely on Article 6(1)(e) nor 6(1)(c) of the GDPR, which stipulate this condition of necessity, which is not met, to perform the denounced transfers.**

II.E.1.2. As regards compliance with the rules governing transfers to the IRS

II.E.1.2.1. Reminder of the principles

182. Chapter V of the GDPR covers the transfer of personal data to third countries or international organisations. A third country is any country that is not a member of the European Economic

March 2017 (point 102). The Litigation Chamber is free to invoke this and any other case law it deems relevant in the exercise of its decision-making competence.

[77] Here again, the Litigation Chamber refers to the CJEU's ruling of 6 October 2020, which emphasises that limitations on the exercise of the rights enshrined in Articles 7 and 8 of the Charter are permissible only "provided that those limitations are provided for by law, that they respect the essence of those rights and that, in compliance with the principle of proportionality, they are necessary and genuinely meet objectives of general interest recognised by the Union [...]. Judgment of the CJEU, Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and others, ECLI :EU :C :2020 :791, pts 120 and 121.

Area (EEA). The transfer of the first plaintiff's personal data by the defendant to the IRS is a transfer to a third country within the meaning of the GDPR.

183. As the parties point out in their respective conclusions (points 53 et seq.), Chapter V of the GDPR organises a cascade system between different instruments that can be applied by a controller or processor to transfer personal data to a third country.[78] This system is in line with the data transfer regime set out in Directive 95/46.[79] Therefore, in the absence of an adequacy decision within the meaning of Article 45 of the GDPR, the controller or processor may transfer personal data to a third country only if it has provided appropriate safeguards and on condition that the data subjects have enforceable rights and effective legal remedies within the meaning of Article 46 of the GDPR. These appropriate safeguards can take various forms such as a legally binding instrument, binding corporate rules (or BCRs), standard data protection clauses or even a code of conduct or a certification mechanism under the conditions set out in Articles 46 and 47 (in the case of BCRs) of the GDPR. Finally, in the absence of an adequacy decision and appropriate safeguards, a transfer of data to a third country may only take place if one of the derogations listed in Article 49 of the GDPR applies.

184. If the requirements of Articles 45 to 49 of the GDPR are not met, the transfer of personal data to a country outside the EEA is prohibited.

185. It is not disputed **that there is no adequacy decision** covering the transfer of data from the first plaintiff (and more broadly from the accidental Belgian Americans whose interests the second plaintiff is defending) to the IRS in the United States, since the "Privacy Shield" decision[80] - moreover invalidated by the CJEU in the above-mentioned "Schrems II" judgment - does not apply to this type of transfer.

186. **In other words, the transfer of data *by an authority* in the EU, such as the defendant to, as in this case, an authority in a third country that does not provide adequate protection, can only take place if the controller, i.e. the defendant, has envisaged *appropriate safeguards* and on condition that data subjects have enforceable rights and effective remedies** either through "a legally binding and enforceable instrument between public authorities or bodies" (Article 46(2)(a) of the GDPR); or by "*provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights*" within the meaning of Article 46(3)(b) of the GDPR.

[78] See Kuner, in Kuner a.o. The EU General Data Protection Regulation: A Commentary, OUP 2020, p. 846.

[79] For a comparison between Directive 95/46/EC and the GDPR, Kuner, in Kuner a.o. The EU General Data Protection Regulation: A Commentary, OUP 2020, p. 758.

[80] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016, pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ 2016, L 207/1.

187. **It has already been mentioned that the defendant relies in this case on Article 46(2)(a) GDPR, in combination with Article 96 GDPR as well as autonomously (paragraphs 82 et seq.).**

188. It is clear from the very text of Article 46(2)(a) of the GDPR (as it is from Article 46(3)(b) moreover) that *appropriate safeguards must be included in* the legally binding instrument (or in the relevant administrative arrangement).[81] Article 46(2)(a) reads as follows: "*appropriate safeguards (...) may be provided for (...) by a legally binding and enforceable instrument between public authorities or bodies*"[82].

189. Recital 102 of the GDPR, which relates to Article 96 of the GDPR, states in the same vein that "*This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects*".[83]

190. While the French wording of this recital is not the clearest, reading the English[84] and Dutch[85] versions clarifies that these agreements must contain appropriate safeguards for the benefit of data subjects. Indeed, whereas the French version uses the wording "les accords (...) y compris les garanties appropriées", the English and Dutch versions explicitly link said agreements to safeguards, stipulating that the latter must be included in said agreements. The English version therefore states *"agreements (...)* ***including*** *appropriate safeguards for data subjects",* while the Dutch version, the most explicit, mentions *"internationale overeenkomsten waarin [**in** which] passende waarborgen zijn opgenomen [appropriate safeguards are included]".*

191. **In other words, pursuant to Article 46(2)(a) of the GDPR, whether or not applied in combination with Article 96 of the GDPR as interpreted and applied as the Litigation Chamber set out in points 129 et seq. these safeguards must be included *in* the international agreement itself.**

192. Why is this so important? As the international agreement constitutes the legal basis for the data transfers it provides for, it must contain the appropriate safeguards as regards data protection. Only if these safeguards are included IN the agreement will they be enforceable against the non-EU country with which the agreement is concluded. As mentioned above, the Litigation Chamber points out that there is no adequacy decision in favor of the third country. Compliance

[81] See also EDPB Guidelines 02/2020, p.21 ff.

[82] Underlined by the Litigation Chamber.

[83] Underlined by the Litigation Chamber.

[84] Recital 102 (English version): This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects.

[85] Recital 102 (Dutch version): Deze verordening doet geen afbreuk aan internationale overeenkomsten die de Unie en derde landen met elkaar hebben gesloten om de doorgifte van persoonsgegevens te regelen en waarin passende waarborgen voor de betrokkenen zijn opgenomen.

with the European data protection rules to which EU member states are bound therefore requires, when the decision is made to conclude an international agreement, as in this case, that this agreement complies with these rules. This compliance involves inserting safeguards in the agreement which, as will be explained below, reflect the minimum European data protection requirements that will be applied to transferred data. If they are not included in the agreement (by or by virtue of the agreement), these safeguards will not be enforceable against the third country. In its Guidelines 02/2020, the EDPB stresses that "*International agreements shall contain specific wording requiring that the core data protection principles are ensured by both parties*" (point 17). Consequently, moreover, the fact that these safeguards would result, as the defendant points out with regard to some of the said safeguards (see below), from the Belgian Act of 16 December 2015 is insufficient in this respect since this legislation is not binding on the third state.

193. In view of the fact that the defendant is invoking Article 96 of the GDPR with regard to the complaint alleging the unlawfulness of the transfer to the United States, the Litigation Chamber points out that in its document WP 234 of 16 December 2015, the Art. 29 WP listed the safeguards which, without prejudice to additional *adhoc* safeguards, must always be present in the legal basis (whether legislation or international agreement) in the context of the automatic exchange of data for tax purposes.

194. In its Guidelines 02/2020, the EDPB also lists, in support of Article 44 of the GDPR and the case law of the CJEU, in particular the Schrems II judgment cited above, the minimum safeguards that must be found in the binding legal instrument, to use only the case of Article 46(2)(a) of the GDPR invoked by the defendant in the present case. These reinforce those already set out by the Art. 29 WP in its above-mentioned WP 234 document. **Rather than recommendations, these are minimum safeguards that *must* be included in the international agreement**. The purpose of these safeguards is indeed, as just recalled, to ensure that the level of protection afforded to natural persons under the GDPR is not compromised when their personal data is transferred outside the EEA and that data subjects benefit from a level of protection substantially equivalent to that guaranteed within the EU.

195. These minimum safeguards include the following requirements, which are found both in the above-mentioned Art. 29 WP document WP 234 - albeit implicitly - and in the most recent EDPB Guidelines 02/2020.

- As regards the key concepts of data protection:

196. International agreements should contain definitions of the basic personal data concepts and rights in line with the GDPR relevant to the agreement in question. EDPB Guidelines 02/2020[86] state that if they refer to these concepts, international agreements should, if referenced,

[86] Point 16 of the EDPB Guidelines 02/2020.

include the following important definitions: “personal data”, “processing of personal data”, “controller”, “data processor", “recipient” and “sensitive data”

197. The Litigation Chamber points out that although the Art. 29 WP's WP 234 document did not explicitly mention this, it is nonetheless essential, whether under Directive 95/46/EC or the GDPR, that the parties to an international agreement agree on the definition of the key concepts of the data processing operations provided for by the agreement - *a fortiori* when the purpose of the agreement is based on these processing operations as in the present case - and that these concepts are defined therein. Otherwise, the effectiveness of any other data protection safeguards mentioned could be compromised. The said definitions are, with limited exceptions[87], otherwise identical in Directive 95/46/EC and in the GDPR.

- As regards the principles of data protection:

198. *Purpose limitation principle*[88]: International agreements need to specify the purposes for which personal data is to be transferred and processed including compatible purposes for further processing, as well as to ensure that the data will not be further processed for incompatible purposes.

199. Principle *of data minimisation*[89]: The international agreement must specify that the data transferred and further processed must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are transmitted and further processed.

200. *Principle of storage limitation*[90]: the international agreement must contain a clause on data storage. In particular, this clause must specify that personal data is only kept in a form that allows identification of the data subjects for as long as is necessary for the purposes for which it was transferred and subsequently processed. Where a maximum retention period is not set in national legislation, a maximum period should be set in the text of the agreement.

- As regards the rights of data subjects:[91]

201. The international agreement must ensure enforceable and effective data subject rights as specified in article 46 (1) and recital 108 of the GDPR. The rights available to the data subjects, including the specific commitments taken by the parties to provide for such rights, should be listed in the agreement. T To be effective, the international agreement must provide for

[87] The notion of processing in the GDPR (article 4(7)) is completed by a reference to structuring, and the list of sensitive data in article 9 includes new data.

[88] See page 6 of the WP 234 and point 18 of EDPB Guidelines 02/2020.

[89] See page 6 of the WP 234 and points 21 et seq. of EDPB Guidelines 02/2020.

[90] See pages 6 and 7 of the WP 234 and point 18 of EDPB Guidelines 02/2020.

[91] See page 7 of the WP 234 and title 2.4. (points 27 et seq.) of EDPB Guidelines 02/2020.

mechanisms that ensure their application in practice. Moreover, any breach of data subject rights must carry an appropriate remedy.

202. As such:

- Parties must ensure that the international agreement contains clear wording describing the transparency obligations of the parties.
- The agreement must guarantee the data subject the right to obtain information on and access to all personal data being processed.
- In principle, the agreement will have to include a clause stating that the receiving public body will not take a decision based solely on automated individual decision-making, including profiling, producing legal effects concerning the data subject in question or similarly affecting this data subject, within the meaning of Article 22 of the GDPR. Where the purpose of the transfer includes the possibility for the receiving public body to make such decisions, the conditions for such decision-making will have to be defined in the agreement and comply with Article 22(2)-(4) of the GDPR.

➢ As regards redress mechanisms:

203. In order to guarantee enforceable and effective data subjects rights, the international agreement must provide for a system that enables data subjects to continue to benefit from redress mechanisms after their data has been transferred to a non EEA country. These redress mechanisms must provide recourse for data subjects whose rights have been infringed to lodge complaints regarding such non-compliance and to have these complaints resolved.

204. The Litigation Chamber has not reproduced here the complete list of minimum safeguards pursuant to Article 46(2)(a) of the GDPR. It has limited itself to listing those it will examine. **Indeed, the absence of one or other safeguard in the agreement is sufficient to conclude that any transfers carried out on the basis of the agreement are unlawful, whether or not Article 46(2)(a) of the GDPR is applied in combination with Article 96 of the GDPR, since these guarantees were required both before 24 May 2016 and after that date.**

205. In the absence of appropriate safeguards within the meaning of Article 46 of the GDPR, the only possibility is to rely on Article 49 of the GDPR. In its *Guidelines 2/2018 on derogations of Article 49 under Regulation (EU) 2016/679*[92] the EDPB clarified that Article 49 of the GDPR cannot be relied upon for repetitive and/or structural processing. Article 49 of the GDPR is therefore excluded in this case (which the defendant admits) since the transfer of data by the defendant to the IRS is automatic and takes place annually.

[92] European Data Protection Board, *Guidelines 02/2018 on derogations under Article 49 of Regulation EU 2016/679* : https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf, p. 5.

II.E.1.2.2. In this case

206. **The Litigation Chamber considers, like the parties (points 57-59 and 81), that Article 49(1)(d) of the above-mentioned GDPR cannot be invoked. As mentioned above, this exception cannot be invoked in the case of recurrent and systematic transfers, as is the case with the data transfers in question**.

207. On the other hand, the Chamber will examine below whether the FATCA agreement offers the appropriate safeguards required by article 46(2)(a) of the GDPR - applied both in combination with article 96 of the GDPR invoked by the defendant but also autonomously since the defendant defends the view that in any event, even supposing that the Litigation Chamber does not retain article 96 of the GDPR, the appropriate safeguards required are in place.

- As regards the key concepts of data protection:

208. With regard to the definitions of such essential data protection concepts as "personal data", "processing" and "controller", the Litigation Chamber notes that the FATCA agreement contains no definitions. While Article 1 of the agreement is devoted exclusively to definitions (1 litera a) to z) + litera aa) to mm), **none of these deal with data protection concepts, despite the fact that the very principle of the agreement is based on a chain of personal data processing operations**.

- Principle of storage limitation:

209. The Litigation Chamber notes that the FATCA agreement contains no commitment as to the limited storage of data processed and transferred under the agreement. Admittedly, as the defendant points out (paragraph 88) , the Act of 16 December 2015 provides for a retention period of 7 years for its part. This time limit under national law is only binding on the defendant. It **does not demonstrate that the IRS would also be bound by a limited storage period for the transferred data**.

- Rights of data subjects:

210. With regard to the rights of the data subjects, the Litigation Chamber notes that the FATCA agreement does not contain any mention of the rights of data subjects, some of which are referred to in point 201 above. The defendant argues in this respect that it informs the data subjects via its website in a section dedicated to the FATCA agreement. Even supposing that this information is provided in the correct manner, *quod non* (see. Title II.E.2 below), **such information is not equivalent to the enshrining of the rights of data subjects (which include many rights other than the right to transparency and information) required in the agreement itself. As the rights of data subjects are not covered by the FATCA agreement - nor by the legal texts to which the agreement refers (as the rights enshrined in the Privacy Act are limited and not equivalent to those provided by the GDPR - this safeguard is lacking**. With specific regard to the reference to Article 22 of the GDPR, the defendant argues that it does

not operate any processing operations falling under this provision. This circumstance, if verified (see Title II.E.4 on DPIA), is irrelevant. In fact, what is required as a safeguard in the agreement is an undertaking by the parties, including the recipient of the data (i.e. the IRS), not to carry out this type of processing in particular. This safeguard is not provided by or under the agreement.

211. The Litigation Chamber notes that here too the **defendant has failed to demonstrate that this appropriate safeguard enshrining the "rights of data subjects" is binding on the parties to the agreement.**

- As regards redress mechanisms:

212. On this point, the Litigation Chamber can only observe that **the defendant has not demonstrated that such a redress mechanism exists for the benefit of the first plaintiff and, more generally, for the benefit of the data subjects by the denounced processing operations, once the data has been transferred, including that of the accidental Belgian Americans.**

213. In support of the foregoing, the **Litigation Chamber concludes, as the Slovak Data Protection Authority did before it**[93]**, that the defendant fails to demonstrate that the appropriate safeguards required by Article 46(2)(a) of the GDPR that it invokes, applied where applicable in combination with Article 96 of the GDPR, are provided by or pursuant to the FATCA agreement. Consequently, the Litigation Chamber finds a violation of Article 46(2)(a) of the GDPR (and more broadly of Chapter V of the GDPR) combined with Articles 5(1) and 24 of the GDPR (accountability - see infra Title II. E.4) on the part of the defendant.**

II.E.1.3. Conclusion as regards the conformity of the transfer of data to the IRS

214. As **already explained (paragraphs 129 et seq.), the defendant could only rely on Article 96 of the GDPR if it had assessed the compliance of the FATCA agreement and concluded that it complied with the useful reading of Article 96.** This assessment obligation results from the very text of Article 96 of the GDPR and especially from the defendant's accountability obligation from 24 May 2018 on, which moreover required the defendant to carry out this assessment on an ongoing basis (Title II.E.4 below).

215. To attest to both its assessment and compliance, the defendant states that it relies on documents issued by the CPP, which was succeeded by the DPA. Two of these documents

[93] Notice of the Office for Personal Data Protection of the Slovak Republic of 23 August 2022 addressed to the Ministry of Finance of the Slovak Republic. This opinion follows the request for an assessment of the compliance of international agreements on the exchange of tax information with the GDPR, formulated by the EDPB in its statement 04/2021. The Slovak DPA concludes in this regard that, as regards the transfer to the US authorities, the conditions of Chapter V of the GDPR are not met. Appropriate safeguards as set out by the EDPB in its Guidelines 02/2020 are not provided for in the FATCA agreement as required by Article 46(2)(a) of the GDPR.

consist, as already mentioned, of opinions (61/2014 and 28/2015) issued by the CPP on successive versions of the draft law that led to the Act of 15 December 2016 (point 83).

216. The Litigation Chamber points out that it is not disputed that these opinions relate to the draft law that led to the future Act of 16 December 2015 and not to the content of the FATCA agreement as such, which the CPP regrets in its opinion. The same applies to deliberation 56/2015 of the SCFA. Furthermore, since this legislation was based on the equivalent of Article 49(1)(d) of the GDPR, the existence of appropriate safeguards within the meaning of Article 46(1)(a) of the GDPR was not examined.

217. As regards the ruling of the Constitutional Court of 9 March 2017, also invoked by the defendant, the Litigation Chamber considers that on the grounds of the application of the cited case law of the CJEU with regard to the principles of necessity and data minimisation, its conclusions on proportionality/ data minimisation in particular, could not form the basis of the defendant's belief that the FATCA agreement was in compliance.

218. **In conclusion, in view of the foregoing and in support of its conclusions in subheadings II.E.1.1. and II.E.1.2. the Litigation Chamber is of the opinion that the arguments put forward by the defendant in support of the compliance of the agreement with Directive 95/46/EC and Union law from 24 May 2016 on did not permit it to conclude that it could continue to transfer the data to the IRS by relying on Article 96 of the GDPR. It also follows from these same conclusions that the FATCA agreement is no more compliant with the GDPR currently than it was with EU law prior to 24 May 2016.**

II.E.2. As regards the reported breach of the obligation to provide information

219. In its capacity as controller, the defendant is bound by Articles 13 and 14, combined with the requirements of Article 12 of the GDPR with regard to the data processing operations it carries out.

220. In this case, the first plaintiff therefore had to be informed by the defendant about the transfer of his personal data to the IRS. As this involved the processing of data that it had not obtained directly from the first plaintiff (the data having been transferred to it in this case by Bank Z), the defendant had to comply with Article 14 of the GDPR, combined with the requirements of Article 12 of the GDPR.

221. Article 14 of the GDPR requires that where personal data has not been collected from the data subject, as in this case, the controller must provide the data subject with all the information listed below. The data protection authorities have agreed that *all* the information in Article 14

of the GDPR, whether required by (1) or (2), must be communicated to the data subject[94]. This information is the following:

- The identity and the contact details of the controller and, where applicable, of the controller's representative (Article 14(1)(a));
- Where applicable, the contact details of the data protection officer (DPO) (Article 14(1)(b));
- The purposes of the processing for which the personal data are intended as well as the legal basis for the processing (Article 14(1)(c));
- The categories of personal data concerned (Article 14(1)(d));
- The recipients or categories of recipients of the personal data, if any (Article 14(1)(e));
- Where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the [European] Commission, or *in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards* and the means to obtain a copy of them or where they have been made available (Article 14(1)(f)).
- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period (Article 14(2)(a));
- Where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party (Article 14(2)(b));
- The existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability (Article 14(2)(c));
- Where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal (Article 14(2)(d));
- The right to lodge a complaint with a supervisory authority (Article 14(2)(e));
- From which source the personal data originate, and if applicable, whether it came from publicly accessible sources (Article 14(2)(f);
- The existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic

[94] Art. 29 WP, *Guidelines on Transparency under Regulation EU 2016/679*, WP 260 (point 23): https://ec.europa.eu/newsroom/article29/items/622227 These Guidelines were taken up by the European Data Protection Board at its inaugural meeting on 25 May 2018.

involved, as well as the significance and the envisaged consequences of such processing for the data subject (Article 14(2)(g)).

222. The defendant does not contest the applicability of Article 14 of the GDPR (as already pointed out, it does not invoke Article 96 of the GDPR with regard to this information obligation - point 138) but defends that it can rely on the exception of Article 14(5)(a) of the GDPR (point 93) which provides that the information items of Article 14(1)-(2) do not have to be provided to the data subject "*where and insofar as the data subject already has the information*".

223. The Litigation Chamber recalls that the defendant considered in its conclusions and at the hearing that it was the responsibility of the banks to inform the first plaintiff, and that bank Z would have informed the latter. The defendant thus invokes Article 14(1) of the *Act of 16 December 2015*, which requires reporting financial institutions (i.e. banks) to inform the data subjects (freely translated) "*that the information referred to in the law will be communicated to the competent Belgian authority*".[95] The Litigation Chamber points out from the outset that this obligation to inform is intended to inform the data subject that data will be communicated to the defendant and not to the IRS.

224. In the opinion of the Litigation Chamber, the banks' duty to inform leaves intact the defendant's duty to inform with regard to the processing it carries out in its capacity as controller, in particular the transfer of data to the IRS. Even though it was legally obliged to inform the first plaintiff, Bank Z (and the reporting financial institutions in general) did not have to provide all the information that the defendant, for its part, had to provide in view of its own processing. There is no perfect identity of information with regard to the processing operations of one and the other, as each controller is required to provide information with regard to the processing they carry out. The defendant's argument that it was up to the banks to inform the plaintiff (albeit in compliance with the law) cannot therefore be accepted. In this respect, the fact that the defendant did not have access to the transferred data is irrelevant. Indeed, this element has no bearing on its status as controller, as the Litigation Chamber already specified (point 126). This element - apart from the fact that it results from the defendant's decision not to access the contents of the bundle for organisational reasons, as it explained at the hearing[96] - is in any case not such as to prevent the communication of at least some of the information listed above specific to "its" processing, such as, for example, the safeguards governing the flow to the United States (article 14(1)(f)), the rights of the data subjects or the storage period, to name but a few.

[95] Underlined by the Litigation Chamber.

[96] See footnote 52 referring to the minutes of the hearing.

225. The exemption to providing information in Article 14(5)(a) of the GDPR must moreover be applied within the strict limits of the text. It may therefore cover only some of the items of information listed above. This is clear from the unequivocal use of the words *"insofar as"* [97] ..

226. In this regard, the Litigation Chamber first notes that Article 14(1) of the Act of 16 December 2015 does not in any event provide for all the elements required by Article 14(1)-(2) of the GDPR. Furthermore, it goes without saying that Article 14(5)(a) of the GDPR can only be invoked if the information has already been provided in relation to the processing concerned.

227. On the basis of the documents submitted, the Litigation Chamber established that certain information had indeed been provided to the plaintiff (points 11-16). However, in order to be rely, as it believes it can, on Article 14(5)(a) of the GDPR, the defendant had to examine whether all the information elements of Article 14(1)-(2) of the GDPR recalled above had been communicated by Bank Z with regard to the processing which is teh defendant's own responsibility (and not that of Bank Z), i.e. the transfer to the IRS. This was not the case. Indeed, it does not follow from the documents communicated by the parties that the first plaintiff would have been informed by Bank Z of all the items of information required by Articles 14(1) and 14(2) of the GDPR with regard to the processing carried out by the defendant (points 11-16) but only some of them as required by the Act of 16 December 2015 (point 226).

228. Article 14(5)(c) of the GDPR (the applicability of which the plaintiffs reject without it being invoked by the defendant) also provides that the items of information listed in paragraphs 1 and 2 do not have to be provided to the data subject where *"obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests".*

229. The Litigation Chamber notes a language difference between the French version and, for example, the Dutch version of this provision. While the French version of article 14(5)(c) mentions "lorsque et dans la mesure où l'obtention ou la communication des informations[98] sont expressément prévues par le droit de l'Union ou de l'Etat membre", the Dutch version of the text uses the following terms: *"wanneer en voor zover het verkrijgen of verstrekken van de gegevens[99] uitdrukkelijk is voorgeschreven bij Unierecht of lidstaatelijk recht".*

230. The Litigation Chamber is of the opinion that it is the obtaining and the communication *of data* that must be provided for by national law (and not that of the information listed in article 14(1)-(2)), notwithstanding the terms of the French version of article 14(5)(c) of the GDPR.

---

[97] Art. 29 WP, *Guidelines on Transparency under Regulation EU 2016/679*, WP 260 (point 56): https://ec.europa.eu/newsroom/article29/items/622227 These Guidelines were taken up by the European Data Protection Board at its inaugural meeting on 25 May 2018.

[98] Underlined by the Litigation Chamber.

[99] Underlined by the Litigation Chamber.

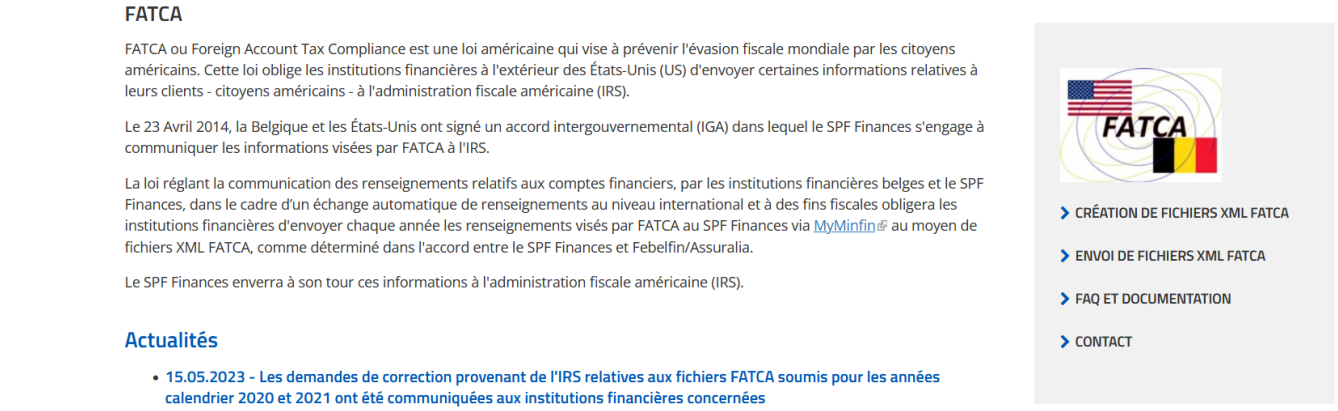
231. **The Litigation Chamber is of the opinion that Article 14(5)(c) of the GDPR is not applicable in the present case, as the conditions for its application have not been met**, be it the processing provided for by the FATCA agreement and the Act of 16 December 2015. This exception can only be invoked *if appropriate measures* to protect the legitimate interests of the data subjects are provided for in the above-mentioned regulations, which the defendant has not demonstrated.

232. As no exemption from providing information applies, the **Litigation Chamber will examine the extent to which the defendant is fully discharging its obligation to provide the information referred to above (Article 14(1)-(2) of the GDPR), as it otherwise claims.** The Litigation Chamber adds that in accordance with Article 12(1) of the GDPR, this information must be in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

233. The Litigation Chamber notes that the defendant does indeed provide information to the data subjects on its website via, as it states in its conclusions, "*more theoretical explanations, news, links to relevant documents and an FAQ" (point 91)*.

234. The Litigation Chamber thus noted the following:

235. https://finances.belgium.be/fr/E-services/fatca[100]: this is a general page which describes the principle of the FATCA agreement in general terms as below, and also includes a number of news items of a technical nature:



236. https://financien.belgium.be/fr/E-services/fatca/creation_de_fichiers_xml_fatca[101]: this is the "Fatca XML file creation" page, which details how FATCA XML files must be formatted in accordance with the XSD schema defined by the US tax authorities (IRS). The page is therefore aimed at financial institutions (banks) and links to the various user guides and IRS pages in English only. Only the note on the correction process and the note on use exist in French, for example.

[100] Consultation of the website by the Litigation Chamber on 23 May 2023.
[101] *Idem*

CRÉATION DE FICHIERS XML FATCA

Les fichiers XML FATCA doivent être formatés conformément au schéma XSD défini par l'administration fiscale américaine (IRS) et décrit dans le User Guide FATCA XML et en tenant compte des Business rules établies de commun accord entre le SPF Finances et Febelfin / Assuralia. Après l'envoi d'un fichier XML FATCA, le SPF Finances, au moyen d'une série de règles de validation, déterminera si le fichier XML FATCA satisfait aux conditions reprises ci-dessus.

Schéma XSD et documentation

- Schéma XSD FATCA
- Schema XSD FATCA (v2.0) < à partir de janvier 2017>
- FATCA XML User Guide (V1.1.)
- FATCA XML User Guide (v2.0) < à partir de janvier 2017>
- Business Rules convenues d'un commun accord entre Febelfin/Assuralia et le SPF Finances (**NEW - 06.12.2021**)
- Processus de correction (PDF, 225 Ko)

Application web EOI XML Tool

- Accès à l'application
- Note d'utilisation (PDF, 273.6 Ko)

FATCA

CRÉATION DE FICHIERS XML FATCA

ENVOI DE FICHIERS XML FATCA

FAQ ET DOCUMENTATION

CONTACT

237. https://financien.belgium.be/fr/E-services/fatca/envoi_de_fichiers_fatca_xml[102]: this page describes the process for sending files to the defendant, and is therefore also aimed at financial institutions.

ENVOI DE FICHIERS XML FATCA

En tant qu'institution financière belge, vous devez communiquer chaque année au SPF Finances les renseignements visés par la loi FATCA en envoyant un fichier XML FATCA valide via MyMinfin.

Pour être autorisé à envoyer un fichier XML FATCA, vous devez au préalable :

- enregistrer d'abord votre institution financière auprès de la Sécurité sociale (si ce n'est pas déjà fait). Cela vous permettra d'accéder aux services en ligne sécurisés et de désigner ensuite un gestionnaire d'accès principal ;
- vous attribuer ou attribuer à vos collaborateurs le rôle « FATCA » via l'application Ma gestion des rôles eGov.

Une fois le rôle attribué, connectez vous à MyMinfin en choisissant « au nom d'une entreprise ».

Sélectionnez le numéro d'entreprise pour lequel vous voulez charger le fichier XML FATCA.

Sous « Mes outils professionnels » :

- cliquez sur « Fichiers FATCA » puis,
- chargez le fichier XML FATCA que vous avez créé.

Vous recevrez un accusé de réception après transmission et validation du fichier par le SPF Finances.

Si votre fichier n'est pas valide, vous recevrez alors un rapport d'erreur.

Plus d'information concernant l'attribution d'un rôle via l'application « Ma gestion des rôles eGov »

Envoi de fichiers XML FATCA

Accès au portail :

FATCA

CRÉATION DE FICHIERS XML FATCA

ENVOI DE FICHIERS XML FATCA

FAQ ET DOCUMENTATION

CONTACT

238. https://financien.belgium.be/fr/E-services/fatca/faq_et_documentation[103]: the "FAQ and documentation" section contains a list of numerous links to various documents relevant in the context of transfer or taxation by foreign tax authorities, many of which are in English.

[102] *Idem*
[103] *Idem*

FAQ ET DOCUMENTATION - FATCA

FAQ

- FAQs IRS
- Généralités
- Création de fichiers
- Envoi de fichiers
- Test
- Renseignements à fournir dans le cadre des échanges internationaux de renseignements fiscaux (CRS et FATCA)

Documentation pratique

- GIIN (Global Intermediary Identification Number)
- GIIN Registration
- Belgian Guidance notes (PDF, 2.4 Mo)
- IRS Notice 2017-46: Revised Guidance Related to Obtaining and Reporting Taxpayer Identification Numbers and Dates of Birth by Financial Institutions
  - Note (PDF, 673.12 Ko) aux institutions financières concernant l'obligation de communiquer le TIN et la date de naissance pour les personnes rapportables
  - Note (PDF, 230.87 Ko) aux institutions financières concernant les valeurs autorisées pour déclarer l'élément TIN US
  - Notice 2023-11 et notes (PDF, 192.59 Ko) aux institutions financières à propos des procédures d'allègement temporaires concernant l'obligation de communiquer le TIN

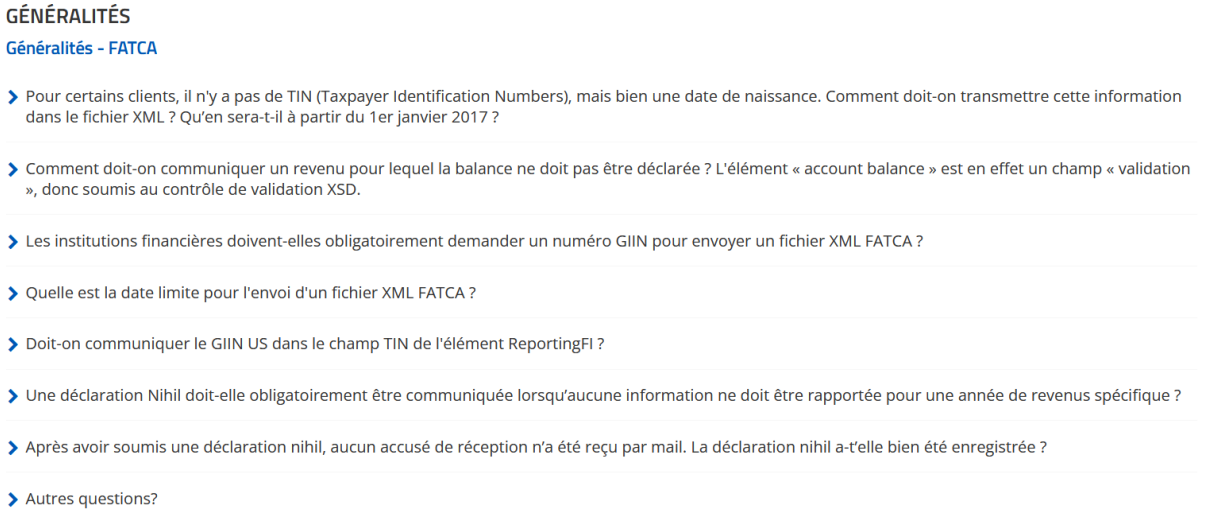
Bases légales et accords administratifs

- Foreign Account Tax Compliance Act (FATCA 18/03/2010)
- Intergouvernmental Agreement Between US and BE (IGA 23/04/2014)
  - Supplemental Agreement to the IGA (from 29/09/2015) (PDF, 277.38 Ko)

FATCA

- CRÉATION DE FICHIERS XML FATCA
- ENVOI DE FICHIERS XML FATCA
- FAQ ET DOCUMENTATION
- CONTACT

239. https://financien.belgium.be/fr/E-services/fatca/faq_et_documentation/faq/generalites[104]: By way of example, the General FAQ refers to a number of questions (cited in the defendant's conclusions as proof that it fulfilled its obligation to provide information).



GÉNÉRALITÉS

Généralités - FATCA

- Pour certains clients, il n'y a pas de TIN (Taxpayer Identification Numbers), mais bien une date de naissance. Comment doit-on transmettre cette information dans le fichier XML ? Qu'en sera-t-il à partir du 1er janvier 2017 ?
- Comment doit-on communiquer un revenu pour lequel la balance ne doit pas être déclarée ? L'élément « account balance » est en effet un champ « validation », donc soumis au contrôle de validation XSD.
- Les institutions financières doivent-elles obligatoirement demander un numéro GIIN pour envoyer un fichier XML FATCA ?
- Quelle est la date limite pour l'envoi d'un fichier XML FATCA ?
- Doit-on communiquer le GIIN US dans le champ TIN de l'élément ReportingFI ?
- Une déclaration Nihil doit-elle obligatoirement être communiquée lorsqu'aucune information ne doit être rapportée pour une année de revenus spécifique ?
- Après avoir soumis une déclaration nihil, aucun accusé de réception n'a été reçu par mail. La déclaration nihil a-t'elle bien été enregistrée ?
- Autres questions?

240. In view of the foregoing, the Litigation Chamber notes that the elements of the defendant's website clearly provide information on the FATCA agreement, on the obligations incumbent on Belgian banks and on the manner in which the latter have to provide the data to the defendant, which will in turn transmit it to the IRS. This information is both general and technical, and is aimed in large part at financial institutions and not directly at potentially involved citizens. Many documents are only available in English.

241. **In view of the preceding paragraphs, the Litigation Chamber notes that this information does not, however, correspond to the information that must be actively provided to data subjects under the terms of Article 14(1)-(2) of the GDPR.**

[104] Idem

242. **Furthermore, the various pieces of information, whether contained in one document or another, *quod non*, are neither easily accessible or intelligible to data subjects as required by Article 12(1) of the GDPR.**

243. These findings of the Litigation Chamber are in line with those of the SCFA in its deliberation 52/2016 which, already in 2016, expressed the following:

> 60. Le Comité constate qu'en dépit de quelques éléments d'information de politique générale, l'information fournie sur le site n'est pas en mesure de rencontrer les attentes des personnes concernées[6]. Les informations « vulgarisées » sont principalement à destination des Institutions financières et outre le texte de la Loi du 16 décembre 2015, la documentation qu'on y trouve n'est que rarement si pas du tout traduite dans les langues nationales belges.
>
> 61. Le Comité constate dès lors que l'analyse et la compréhension cet accord n'est pas à la portée de tous et ne suffit pas à l'information claire et transparente pour les personnes concernées.

244. In view of the foregoing, the Litigation Chamber **finds a breach of Article 14(1) and 14(2) combined with Article 12(1) of the GDPR on the part of the defendant**.

II.E.3. As regards the reported breach of the obligation to perform a DPIA

245. The Litigation Chamber recalls that Article 35(1) of the GDPR states the following: "*Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks*". This obligation for the controller to carry out a DPIA in certain situations must be understood in the context of its general obligation to appropriately manage the risks presented by the processing of personal data.

246. The Litigation Chamber also points out that if the controller performs one of the processing operations listed in Article 35(3) of the GDPR[105], it is obliged to carry out this DPIA. The same applies when the envisaged processing is included in the list of processing operations requiring

[105] Article 35(3) of the GDPR provides that a DPIA is required in the following 3 cases: (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person, (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or (c) a systematic monitoring of a publicly accessible area on a large scale.

a DPIA adopted by the DPA pursuant to Article 35(4) of the GDPR[106]. The processing covered by the complaint are not covered by these provisions.

247. As it has already made clear (paragraph 141), the Litigation Chamber is of the opinion that the obligation to carry out a DPIA is not covered by the scope of Article 96 of the GDPR

248. As regards the application of the obligation to carry out a DPIA over time, the data protection authorities (including the DPA) have agreed that a DPIA is not necessary in particular where the processing was authorised before 24 May 2018 by a supervisory authority in accordance with Article 20 of Directive 95/46/EC[107] and the implementation of that processing has not changed since that prior checking.

249. Irrespective of whether or not the SCFA's decision qualifies as an "authorisation" within the meaning of Article 20 of Directive 95/46/EC, **the Litigation Chamber considers that the SCFA's authorisation cannot, in any event, serve as a basis for enjoying an exemption from the obligation to carry out a DPIA. Indeed, the SCFA's analysis did not focus on the existence or otherwise of appropriate safeguards within the meaning of Article 46(2)(a) of the GDPR or its equivalent under Directive 95/46/EC. The Litigation Chamber also considers that it cannot be considered that the implementation of the processing (transfer) has not changed since this authorisation dated 15 December 2016. Analysis of the evolution of risks likely to call into question the exemption necessarily includes the evolution of the context - including the legal context - in which this processing is performed. In this respect, as already mentioned in Title II.E.1 above, several conditions for transfers that must be examined in the context of the DPIA (see Article 35(7) of the GDPR which lists the required elements[108]) such as data minimisation (proportionality) have been strengthened since the GDPR came into force, under the terms of CJEU case law in particular.**

250. Consequently, the Litigation Chamber considers that the defendant was not in a situation in which it could invoke a possible "rationae temporis" exception to its obligation. It therefore had to consider, in the context of its accountability obligation, whether the transfer to the IRS

[106] The list of processing operations which, according to the DPA, require a DPIA pursuant to Article 35(4) of the GDPR can be found here (French only): https://www.autoriteprotectiondonnees.be/publications/decision-n-01-2019-du-16-janvier-2019.pdf

[107] Article 20(1) of Directive 95/46/EC: Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.

[108] Article 35(7) of the GDPR requires the DPIA to contain at least: (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller, (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes, (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph1, and, (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

required it to carry out a DPIA or not, and to do so from 25 May 2018 and thereafter on an ongoing basis.

251. The Litigation Chamber stated that in its defence, the defendant specified that when questioned as to this by the IS on 30 June 2021, its DPO replied that on the basis of a pre-impact assessment, it had been concluded that an impact assessment was not necessary in view of the fact (point 46):

- That the law had incorporated the remarks made by the CPP in the two opinions issued on the draft law;
- That the SCFA had issued a resolution authorising the transmission of data to the IRS and that the conditions of this resolution had been implemented;
- That the processing complies with the requirements of the AEOI standard on confidentiality and data protection, as well as the defendant's information security policies based on the ISO27001 standard: the transmission of information is doubly protected, at the level of the encrypted and signed files and at the level of the channel through which the information is communicated (MyMinfin secure platform for data transmission by Belgian banks and IDES secure platform for transmission to the IRS);
- That the US authorities are also required to provide the necessary security measures to ensure that the information remains confidential and is stored in a secure environment, as provided for in the FATCA Data safeguard workbook.

252. The Litigation Chamber notes that the defendant's DPO does not specify the date on which this pre-assessment was carried out. While the IS explicitly asked for this assessment to be communicated to it, the defendant declined. This pre-assessment is not included in the file.

253. The Litigation Chamber also submits that the defendant's argument cannot be entertained for the following reasons.

254. The Litigation Chamber recalls Article 35(10) of the GDPR here: *"Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities"*.

255. Article 23 of the Belgian Data Protection Act states that even if an impact assessment has been carried out as part of the adoption of the legal basis on which the processing is lawful (Article 6(1)(c) or Article 6(1)(e) of the GDPR), the controller is not exempt from carrying out a DPIA within the meaning of Article 35(1) of the GDPR when the conditions for its application are met.

256. **Thus, even supposing they were relevant, *quod non* as the Litigation Chamber demonstrated above, the opinions issued by the CPP could not exempt the defendant from carrying out a DPIA. These positions could not form the basis for the defendant's conclusion that a DPIA was unnecessary.**

257. Indeed, while the Belgian legislator has taken the trouble to provide that the DPIA carried out in the context of parliamentary work does not exempt the controller from carrying out a DPIA within the meaning of Article 35 of the GDPR prior to the implementation of the processing operations concerned, it would be contrary to this option to admit that a pre-assessment could rely on the existence of such opinions to conclude that the controller is not required to carry out a DPIA.

258. The defendant's DPO also argues that the pre-assessment was based on other standards. However, as will be shown below, these standards alone were not sufficient to exempt the defendant.

259. **The Litigation Chamber is in fact of the opinion that the transfer of data to the IRS is processing which is likely to result in a high risk to the rights and freedoms of natural persons within the meaning of Article 35(1) of the GDPR.**

260. **Several criteria** cited under Recital 75 of the GDPR as well as in the EDPB's DPIA Guidelines [109]are indeed **present in this case.**

261. As such, the Litigation Chamber held:

- "Systematic monitoring" [110]in that the data concerned are, with some exceptions linked to the "declarable" threshold of bank accounts, systematically transferred to the IRS on an annual basis, whether or not there is any indication of fraud or tax evasion (see Title II.E.1.1.);
- The data communicated are financial data which fall into the category of "data of a highly personal nature"[111] within the meaning of the above-mentioned Guidelines;

[109] Article 29 Working Party, *Guidelines on data protection impact assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation (EU) 2016/679*, WP 248: https://ec.europa.eu/newsroom/article29/items/611236. The European Data Protection Board (EDPB) endorsed these guidelines on 25 May 2018 under the terms of the decision you can find here: https://edpb.europa.eu/sites/default/files/files/news/endorsement_of_wp29_documents.pdf

[110] In its *Guidelines on data protection impact assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation (EU) 2016/679*, WP 248, the Art. 29 WP/EDPB defines as falling within the scope of surveillance data processing used to observe, monitor or control data subjects, including the collection of data via networks, for example. "Monitoring" is therefore not limited to camera surveillance, for example. "Systematic" also means any monitoring that meets one or more of the following criteria: surveillance is carried out according to a system; it is prepared, organized or methodical; it is carried out as part of a general collection plan; it is carried out as part of a strategy.

[111] In its *Guidelines on data protection impact assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation (EU) 2016/679*, WP 248, the Art. 29 WP/EDPB clarifies that beyond Articles 9 and 10 of the GDPR, certain categories of data may be considered as increasing the possible risk to individuals' rights and freedoms. They are considered "sensitive" in the common sense of the term. This includes financial data, all the more so when its disclosure is intended to combat offences that could be attributed to the data subjects.

- The data is processed on a "large scale" [112]in that it concerns, a priori and with limited exceptions, the data of all US nationals with bank accounts in Belgium. The scope of the obligation and its recurrence, even on an annual basis, play a role here in assessing the "large-scale" nature of the processing, alongside the number of data subjects and the volume of data transferred;
- The data subjects can be described as "vulnerable" (recital 75) if an imbalance in their relationship with the defendant can be identified, and even more so with the IRS. This imbalance results not only from the fact that the transfer is imposed on the data subjects without their being able to oppose it, but above all from the complexity of the legal framework, including the existence of any means of redress for the exercise of their rights (see below the finding regarding the absence of this safeguard - point 212).
- the purpose pursued and the subsequent processing likely to be carried out in the United States entails, according to the Litigation Chamber, a potential "matching or combining of data sets", another criterion of the guidelines already cited as mentioned in the preparatory work of the Act of 16 December 2015 cited by the plaintiff (point 62).

262. Finally, although this is not one of the 9 criteria listed by the EDPB, the transfer takes place to a non-EEA country whose level of data protection is not considered adequate and has been the subject of ongoing controversy for many years. The defendant could not have been unaware of this, and in the Litigation Chamber's view, the situation required particularly rigorous attention and risk assessment.

263. The Litigation Chamber recalls that the EDPB is of the opinion that in most cases, the controller may consider that a processing operation that meets 2 of the 9 criteria listed in its Guidelines requires a DPIA. Generally speaking, the EDPB considers that the more criteria a processing operation "meets", the more likely it is to represent a high risk to the rights and freedoms of data subjects, and therefore to require a DPIA, whatever measures the controller intends to adopt.

264. **Combined, the fact there are 5 criteria identified in point 261 - the respective weightings of which may vary - indicates a high level of risk for the denounced transfer to the IRS. In the Litigation Chamber's view, this high level of risk justified a DPIA, within the meaning of article 35(1), being carried out by the defendant. By the latter's own admission, this assessment was not carried out, for reasons that the Litigation Chamber rejected in the preceding paragraphs.**

[112] To determine whether a processing operation is "large-scale", the Art. 29 WP/EDPB recommends, in the DPIA guidelines cited in note 110 above, that the following factors in particular be taken into account: the number of data subjects, the volume of data and/or the range of different data elements processed; the duration or permanence of the processing activity; the geographical extent of the processing activity.

265. **Consequently, the Litigation Chamber finds a breach of Article 35(1) of the GDPR on the part of the defendant.**

II.E.4. As regards the reported breach of accountability

266. In accordance with the principle of accountability, the defendant was under an obligation (paragraph 141), taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, to implement appropriate technical and organisational measures, to simultaneously ensure that processing is performed in accordance with the GDPR, and be able to demonstrate it.

267. As such, any breach, for example one-off or resulting from human error, does not necessarily imply a breach of Articles 5(2) and 24 of the GDPR. However, that is not the situation in this case.

268. Here, the nature of the processing, its scope and its purpose, i.e. in this case (1) a transfer of personal data to a country outside the EEA for which there is no adequacy decision, (2) carried out for the purposes of possible taxation and combating tax evasion and fraud - i.e. for the purposes of determining whether a foreign law has been infringed, (3) even though the data subjects have no connection with the state in question other than having nationality from there, and (4) no evidence of an offence has been established, **clearly presented risks for the rights and freedoms of the data subjects (as the Litigation Chamber demonstrated in Title II.E.3 above).**

269. Admittedly, in the context of the complaint which has culminated in the present decision, the defendant argues that it relied on favorable opinions and authorisations from the CPP prior to the entry into force of the GDPR in particular, invoking Article 96 of the GDPR, the scope and exact consequences of which are, admittedly, not self-evident upon the first reading.

270. At the same time, the defendant could not ignore the repeated calls (some of which came after these opinions and authorisations) in particular from the data protection authorities made within the Art. 29 WP and then the EDPB (including the DPA) to assess an international agreement such as the FATCA agreement against the GDPR. **While some of these political appeals were aimed directly at the Belgian State, others, more technical, in the form of the Guidelines cited in this decision, for example, were addressed directly to controllers such as the defendant.**

271. **The Litigation Chamber further demonstrated that the above-mentioned opinions and authorisation from the CPP did not in fact exempt the defendant from carrying out this assessment in view of both (1) its accountability obligation, (2) its obligation to carry out a DPIA within the meaning of Article 35 of the GDPR and (3) Article 96 of the GDPR. As**

already noted, Article 96 intrinsically requires that this assessment be carried out in order to produce its effects, taking account in particular the reinforcement of the CJEU's case law on the principles of necessity and data minimisation/proportionality, compliance with which had already been called into question under Directive 95/46/EC with regard to comparable data processing operations.

272. **The Litigation Chamber ruled that the defendant had not accurately assessed the risks to the rights and freedoms of the first plaintiff and the Belgian accidental Americans, whose interests were being defended by the second plaintiff, nor had it adopted the appropriate measures to deal with these risks. As is clear from the findings of the Litigation Chamber with regard to the various breaches identified (Titles II.E.1, II.E.2. and II.E.3), the defendant still cannot demonstrate that it has put in place the appropriate measures to guarantee compliance with the GDPR in their regard.**

273. Without prejudice to the foregoing, the Litigation Chamber is aware that the defendant intended to implement an international agreement and Belgian legislation over which it argued that it had little or no control, and that these texts were part of a broader international context.

274. However, this circumstance is not such as to rule out any breach on his part, given its capacity as controller. Indeed, the aim of the accountability principle is to make controllers - whether they are authorities, public bodies or private companies - accountable, and to enable supervisory authorities such as the DPA (and through it, the IS and the Litigation Chamber) to verify the effectiveness of the measures taken to implement it. This principle would be largely undermined, or even made devoid of substance, if it were sufficient for a controller to invoke, once faced with a complaint brought before the supervisory authority, the fact that a legal obligation or the exercise of a public interest mission would mean that it could not comply with the GDPR.

275. Pursuant to its duty of accountability, the defendant could at the very least have alerted the relevant authorities to the untenable situation in which it found itself with the FATCA agreement, in relation to its obligations under data protection law. In this respect, the Litigation Chamber cannot entirely reject the idea that if the defendant had carried out the DPIA referred to in Title II.E.3, it would have quickly realised that notwithstanding the measures it could have taken, admittedly limited in the legal context in which this transfer takes place, it still had a high residual risk. Prior consultation with the DPA within the meaning of Article 36 of the GDPR might therefore have been required.

276. In view of all the foregoing, the **Litigation Chamber concludes that the defendant has violated Articles 5(2) and 24 of the GDPR.**

II.E.5. As regards the reported breach of Article 20 of the LTD

277. As the Litigation Chamber explained in paragraph 77, the plaintiffs state in their reply that they are not invoking a violation of article 20 of the LTD on the part the defendant.

278. Nevertheless, the Litigation Chamber is competent to examine whether this provision should have been complied with in this case, and if so, whether that was the case.

279. Indeed, **once it has received a complaint, the Litigation Chamber is competent to independently monitor compliance with the GDPR and its national implementing laws such as the LTD, and ensure their effective application notwithstanding, as in this case, the fact that one or other grievance initially raised is waived during the procedure**.

280. This **abandonment of grievance does not mean that any previous breach on the part of the defendant is now eliminated, nor does it mean that the Litigation Chamber, as a matter of principle, cannot exercise of its powers with regard to the defendant**. The actual monitoring that the DPA must perform in this case pursuant to Articles 51 et seq. of the GDPR and Article 4(1) of the LCA, unquestionably precludes this. In view of the subject of the complaint, the Litigation Chamber intends to examine any potential infringements[113].

281. This monitoring must nevertheless be exercised **with due respect for the rights of the defence**. In this respect, the Litigation Chamber notes that the defendant refuted the claim that it had breached article 20 of the LTD in its reply of 16 March 2022[114], before the plaintiffs indicated that they would waive this claim in their subsequent reply of 15 April 2022, as well as in its summary conclusions.

282. As already mentioned, Article 20 of the LTD provides that (freely translated) "*unless otherwise provided in specific laws, in execution of Article 6(2) of the Regulation [i.e. GDPR], the federal public authority that transfers personal data on the basis of Article 6(1)(c) and (e), of the Regulation [i.e. GDPR] to any other public authority or private organisation, shall formalise this transfer for each type of processing by a protocol between the initial controller and the controller receiving the data (1)*".

283. The preparatory work[115] for this article indicates that the obligation to conclude a protocol to formalise data transfers from federal public authorities cannot be imposed for flows to foreign countries.

284. The preparatory work justifies this exclusion by referring to Article 1 of the GDPR, which states that: "*The free movement of personal data within the Union shall be neither restricted nor*

[113] See also decision 41/2020 of the Litigation Chamber. In its policy note on the closure of complaints with no further action, the Litigation Chamber states in the same vein that if a complaint is withdrawn, it will be dismissed with no further action, unless there are specific circumstances (French only) https://www.autoriteprotectiondonnees.be/publications/politique-de-classement-sans-suite-de-la-chambre-contentieuse.pdf

[114] Title 6.2. points 16-17. See also the defendant's summary conclusions of 16 May 2022 (title 6.3, points 23-24).

[115] Draft law on the protection of natural persons as regards the processing of personal data, Doc., Ch. 54K3126, p. 44.

prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data".

285. In its recommendation[116] on this obligation, the DPA states on this basis[117] that data transfers to EEA countries cannot be made conditional on the conclusion of a protocol between the initial controller and the data recipients. Nonetheless, the recommendation concludes, controllers involved in a transfer of personal data must ensure that this transfer complies with all the regulations in force, in particular the GDPR.

286. With regard to data flows outside the EEA, as in this case, the recommendation states that Chapter V of the GDPR must be complied with, and that if Article 46 of the GDPR is applied - as invoked in this case by the defendant - the federal public authorities must provide appropriate safeguards to supervise these flows. This supervision is discussed in Title II.E.1. above.

287. In line with this interpretation, the DPA has devised a model protocol from which it is clear that the transfer of data covered by the obligation to conclude a protocol within the meaning of Article 20 of the LTD takes place between a federal public authority on the one hand and a recipient "resident" in Belgium on the other[118].

288. **In view of the foregoing, the Litigation Chamber concludes that the obligation to conclude a protocol within the meaning of Article 20 of the LTD applies only to transfers between federal public authorities and does not find application for data transfers to or from third countries within the meaning of the GDPR. This obligation of protocol therefore does not apply to the defendant in relation to the transfer of the data referred to in the complaint to the IRS, and it cannot therefore be accused of any breach in this respect.**

II.F. Corrective measures and sanctions

289. Under article 100 of the LCA, the Litigation Chamber has the power:

1. to close the complaint without further action;
2. to order the dismissal of the case;
3. to order a suspended sentence;
4. to propose a transaction;

[116] https://www.autoriteprotectiondonnees.be/publications/recommandation-n-02-2020.pdf

[117] The Litigation Chamber agrees with the legislator's analysis in view of the provisions on applicable transborder data flows set out in Chapter V of the GDPR and the fact that the LTD consists of a law implementing the GDPR at least as far as Article 20 is concerned. The Litigation Chamber is nevertheless of the opinion that mentioning this derogation in the text of the LTD itself would have been clearer and more predictable.

[118] See https://www.autoriteprotectiondonnees.be/professionnel/premiere-aide/toolbox, which provides a model protocol for the transfer of data pursuant to article 20 of the LTD.

5° to issue warnings or reprimands;

6° to order compliance with the data subject's requests to exercise his rights;

7. to order that the person in question be informed of the security problem;

8. to order the suspension, restriction or temporary or definitive prohibition of processing;

9. to order that the processing to be brought into compliance;

10. to order the rectification, restriction or deletion of data and the notification thereof to the data recipients;

11. to order the withdrawal of the approval from certification bodies;

12. to issue a penalty payment;

13. to impose administrative fines;

14° order the suspension of transborder data flows to another State or international organisation;

15. to forward the file to the Brussels Public Prosecutor's Office, which will provide information on the action taken with regard to the file;

16. to decide on a case-by-case basis to publish its decisions on the Data Protection Authority's website.

290. On the basis of the documents in the file and at the end of its analysis, the Litigation Chamber concludes, as mentioned in the conclusion of Title II.E.1., that the processing of the first plaintiff's personal data by the defendant, including the transfer thereof to the IRS, is unlawful, since such processing takes place in violation of the principles of purpose, necessity and data minimisation/proportionality and the rules of Chapter V of the GDPR. The Litigation Chamber has shown that this unlawfulness affects not only the processing of the plaintiff's personal data, but also, more generally, that of the personal data of Belgian accidental Americans.

291. In view of this unlawfulness, the **Litigation Chamber has decided to order the prohibition of the data processing of the first plaintiff and the Belgian accidental Americans performed in execution of the FATCA agreement and the Act of 16 December 2015 and this, pursuant to both article 100.8 of the LCA and article 58(2)(f) and (j) of the GDPR**. The Litigation Chamber considers that this corrective measure is the **only one capable of putting an end to the identified breaches**, each category of breach taken in isolation (whether the breach of the principles of purpose and data minimisation on the one hand (Title II.E.1.1.) or the breach of the rules of Chapter V of the GDPR on the other (Title II.E.1.2.) justifying this prohibition. This prohibition means that the flow of said data to the IRS must be suspended, pursuant to article 100.14 of the LCA.

292. **In accordance with the above-mentioned Schrems II ruling of the CJEU of 16 July 2020, the Litigation Chamber adds that it is also obliged to issue such a prohibition**. The operative part of this judgment in fact states that "*Article 58(2)(f) and (j) of the GDPR must be interpreted as meaning that, unless there is a valid Commission adequacy decision, the competent supervisory authority is required to suspend or prohibit a transfer of data to a third country pursuant to standard data protection clauses adopted by the Commission, if, in the view of that supervisory authority and in the light of all the circumstances of that transfer, those clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law, in particular by Articles 45 and 46 of the GDPR and by the Charter, cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer.*" (point 121 of the judgment[119]).

293. The fact that the CJEU's ruling requires standard contractual clauses to be set aside is not such as to preclude the Litigation Chamber's obligation to prohibit data transfers carried out under an international agreement, such as the FATCA agreement.

294. Indeed, the operative part and points 119-121 of the judgment enshrine more generally what is expected of data protection authorities in terms of exercising their powers with regard to cross-border data flows that take place in breach of the GDPR, in particular in breach of Articles 45 and 46, as in the present case.

295. In the light of all the circumstances surrounding the denounced transfers and the infringements identified by the Litigation Chamber, **the protection of the transferred data required by EU law can only be ensured by the prohibition ordered by the Litigation Chamber, since the defendant refused, in its decision of 4 October 2021, to suspend the transfer of such data and defended in the present proceedings that it was entitled to continue doing so.**

296. The Litigation Chamber finds that the defendant is also guilty of a **violation of Article 14(1)-(2) combined with Article 12(1) of the GDPR** in that the defendant did not sufficiently inform the first plaintiff and does not sufficiently inform the Belgian accidental Americans and more generally the data subjects of the data processing carried out in execution of the FATCA agreement (Title II. E.2).

297. For this breach**,** the Litigation Chamber has issued a reprimand to the defendant **on the basis of article 100, 5° of the LCA, together with a compliance order** on the basis of article 100, 9°

[119] The Litigation Chamber also refers to paragraphs 111 and 112 of the judgment, which state that:
"111. If a supervisory authority takes the view, following an investigation, that a data subject whose personal data have been transferred to a third country is not afforded an adequate level of protection in that country, it is required, under EU law, to take appropriate action in order to remedy any findings of inadequacy, irrespective of the reason for, or nature of, that inadequacy. To that effect, Article 58(2) of that regulation lists the various corrective powers which the supervisory authority may adopt. 112. Although the supervisory authority must determine which action is appropriate and necessary and take into consideration all the circumstances of the transfer of personal data in question in that determination, the supervisory authority is nevertheless required to execute its responsibility for ensuring that the GDPR is fully enforced with all due diligence."

of the LCA to **provide full, clear and accessible information regarding the transfer of data to the IRS, on its website.**

298. The Litigation Chamber finds that the defendant is also guilty of a **breach of Article 35(1) of the GDPR** in that the defendant failed to carry out a DPIA (Title II.E.3).

299. For this breach**,** the Litigation Chamber issued a **reprimand to the defendant under Article 100.5° of the LCA, together with a compliance order under Article 100.9° of the LCA to carry out a data protection impact assessment** in accordance with Article 35 of the GDPR. The Litigation Chamber is of the opinion that, notwithstanding the issued prohibition on processing, it is still useful to carry out such an assessment. A rigorous DPIA should help create a framework which is GDPR-compliant in the future.

300. Finally, the Litigation Chamber finds that the defendant is also guilty of a **breach of Articles 5(2) and 24 of the GDPR** in that the defendant failed to comply with its obligation of accountability (Title II.E.4).

301. For this breach, the Litigation Chamber has issued a **reprimand to the defendant on the basis of article 100. 5° of the LCA, together with a compliance order consisting of alerting the competent legislator** to the breaches found under the terms of the present decision and the issued prohibition on processing.

III. PUBLICATION AND TRANSPARENCY

302. In view of the importance of transparency regarding the decision-making process and the decisions of the Litigation Chamber, this decision will be published on the website of the DPA. Up to now, the Litigation Chamber has generally decided to publish its decisions by redacting information which could directly identify the plaintiff(s) and other persons cited, whether natural persons or legal entities, as well as the identities of the defendant(s).

303. In the present case, the Litigation Chamber has decided to publish the present decision with identification of the parties, with the exception of the first plaintiff.

304. The Litigation Chamber points out that this publication, which identifies both the second plaintiff and the defendant, pursues several objectives.

305. As regards the defendant, it pursues an objective of general interest, because the present decision addresses the question of the liability of a federal public service (the defendant) subject to obligations arising from an international agreement (FATCA) concluded with a country outside the EU, obligations which are deemed contrary to the GDPR under the terms of the present decision.

306. Identifying the defendant is also necessary for a proper understanding of the decision, and thus to achieve the objective of transparency pursued by the Litigation Chamber's policy of publishing its decisions.

307. With regard to the second plaintiff, a useful reading of the decision also requires that its identity be disclosed since it defends a category of persons affected by the data processing which is deemed contrary to the GDPR, and the examination of the parties' grievances and defences is based in particular on the specific situation of this category of persons.

308. Furthermore, without this being an overriding argument, the Litigation Chamber is aware that the complaint lodged by the second plaintiff against the defendant was reported on by the press, on the initiative of the plaintiff's counsel, and therefore made public.

309. Finally, publishing the identity of the second plaintiff and the defendant also contributes to the objective of consistency and harmonised application of the GDPR. As explained in point 114, the complaint was not intended to be addressed under the single point of contact mechanism, but the FATCA issue is being felt well beyond Belgium's borders, and it cannot be ruled out that other EU data protection authorities may have to address similar complaints in the future, for the examination of which this decision may be useful, since each supervisory authority exercises its powers in complete independence.

FOR THESE REASONS,

the Litigation Chamber of the Data Protection Authority decides, after deliberation:

- Pursuant to Article 100.8. of the LCA, to prohibit the processing by the defendant of the data of the first plaintiff and the Belgian accidental Americans under the FATCA agreement and the Act of 16 December 2015 *regulating the communication of information relating to financial accounts by Belgian financial institutions and the FPS Finance, in the context of an automatic exchange of information at the international level and for tax purposes.*
- Pursuant to Article 100.5. of the LCA, to issue a reprimand against the defendant regarding the violation of Article 14(1)-(2) combined with Article 12(1) of the GDPR accompanied by a compliance order on the basis of Article 100.9. of the LCA, which involves providing GDPR-compliant information on its website;
- Pursuant to Article 100.5. of the LCA, to issue a reprimand to the defendant regarding the violation of Article 35(1) of the GDPR together with an order for compliance on the basis of Article 100.9. of the LCA, which involves carrying out a DPIA within the meaning of Article 35 of the GDPR.
- Supporting documents attesting to the compliance measures ordered must be sent to the Litigation Chamber at litigationchamber@apd-gba.be within 3 months of notification of this decision;
- Pursuant to Article 100.5. of the LCA, to issue a reprimand against the defendant regarding the violation of Articles 5(2) and 24 of the GDPR.

In accordance with Article 108 § 1 of the LCA, an appeal against this decision may be submitted within thirty days of its notification, to the Contract Court (Court of Appeal in Brussels), with the Data Protection Authority as defendant.

Such an appeal may be filed by means of an interlocutory motion, which must contain the information listed in Article 1034ter of the Judicial Code120. The interlocutory motion must be filed

[120] On pain of nullity, the request must contain:
1° the indication of the day, month and year;
2° the full name and address of the applicant and, where applicable, their capacities and national register number or company number;
3° the full name, address and, where applicable, the capacity of the person to be summoned;
4° the subject and a summary of the grounds for the application;
5° the indication of the judge referred to for the application;
6° the signature of the applicant or their lawyer.

with the clerk's office of the Contract Court in accordance with Article 1034quinquies of the Judicial Code[121], or via the e-Deposit information system of the Ministry of Justice (Article 32ter of the Judicial Code).

(Sé). Hielke Hijmans

President of the Litigation Chamber

[121] The request, together with its annex, must be sent in as many copies as there are parties involved, by registered letter to the clerk of the jurisdiction or submitted at the court registry.