FATCA/CRS & Data Protection

DSB and ICO decisions (May 2019)

Serious questions for the EDPB

19 June 2020

Mishcon de Reya

Mishcon de Reya

TABLE OF CONTENTS

***

Mishcon de Reya

Our Ref: 5999/FXN/60052.1/fxn

Africa House
70 Kingsway
London WC2B 6AHgsway

www.mishcon.com

Sent via email
European Data Protection Board (EDPB)

CC: - European Parliament, Petitions Committee (PETI)
- Council of Europe's T-PD

19 June 2020

Dear All

FATCA & CRS | Implications of Austrian and UK decisions for the EDPB

I refer to my letter dated 16 June 2020 in which we discussed the implications of the recent negative decisions from the Austrian Data Protection Authority (**'DSB'**) and the UK Information Commissioner's Office (**'ICO'**) for the EDPB and its Chair

1. **Today's email from the ICO**

1.1 I received an email from the ICO saying that "*we have been asked by colleagues in other EU DPAs to share a* redacted *version of the decision*".

1.2 I am glad that other EU data protection authorities are taking an interest in this matter and I therefore attach a copy of the decision dated 29 May 2020 in the case of a US-born British citizen known as Jenny.

2. **Refusal to discuss case law from the EU Courts**

2.1 As you will see, the ICO has *not spent a single word* on the various decisions from the European Court of Justice (**CJEU**) and the European General Court (**EGC**) in the area of data protection, the transfer of data to the US and the principles of necessity and proportionality (*Digital Rights Ireland*, *Schrems*, *Tele 2*, *MEP expenses* and *PNR Agreement with Canada*).

2.2 This is the very same approach adopted by the Austrian Data Protection Authority in its decision dated 18 May 2020 currently under judicial review.[1]

3. **Refusal to discuss existing concerns raised by EU experts**

3.1 Similarly, the ICO refused to even discuss any of the opinions issued by the EDPB's predecessor (the WP29), as well as the EDPS, the AEFI Group and the European Parliament. In particular, the WP29 issued consistent warnings concerning the compatibility of AEOI systems with individuals' fundamental rights in opinions issued on 21 June 2012, 4 February 2015, and 16 December 2015, and lastly with a 'frank' letter dated 12 December 2016 directly from the Chair to the European Commission and the OECD. As you know, our investigation has also shown the existence of 'worrying' concerns raised by the European Commission.

[1] As discussed at paragraph 4.4. of my letter dated 16 June 2020.

3.2 Again, this is the very same approach adopted by the Austrian Data Protection Authority, which is led by the EDPB's Chair.[2]

4. Refusal to examine of compatibility of FATCA with fundamental rights

4.1 You will recall from my letter dated 16 June 2020 that the Austrian Data Protection Authority claimed that (my translation from German):

> *"Whether and to what extent the Austrian CRS law (GMSG) and the DAC2 directive are compatible with the fundamental right to privacy and data protection enshrined in § 1 of the Austrian Data Protection law, Article 8 ECHR and/or Articles 7 and 8 of the EU Charter of Fundamental Rights is beyond the powers of the Data Protection Authority.*
>
> *Such a task falls exclusively in the province of the Constitutional Court and, absent a statutory basis, not in that of the Data Protection Authority. Therefore, the data protection complaint is rejected."*

4.2 The ICO took an identical approach, whilst carefully avoiding any express statement relating to the extent of the powers available to national data protection authorities. However, the outcome is the same:

> *"Is the FATCA Legal Framework itself in breach of the European Convention on Human Rights (**ECHR**) or the Charter of Fundamental Rights of the European Union (the **Charter**)?*
>
> *This [question] falls outside the scope this complaint response."*

4.3 Fewer words, same substance. In other words, like its Austrian counterpart, the ICO has decided to ignore the principle enunciated in the CJEU's *Schrems* judgment:

> *"Where a national authority or the person who has brought the matter before the national authority considers that a… decision is invalid, that authority or person must be able to bring proceedings before the national courts so that they may refer the case to the Court of Justice if they too have doubts as to the validity of the… decision."*

4.4 The idea of national data protection authorities ignoring leading case law from the CJEU sets a dangerous precedent and raises worrying concerns for the Rule of Law. The fact that two national data protection authorities do this within the space of one month from each other requires a direct intervention from the EDPB in accordance with its powers under the GDPR.

5. Disregard/selective regard for national case law

5.1 English case law disregarded

(a) The ICO conveniently disregarded the most recent judgment by the UK Supreme Court in a case concerning the exchange of data with the US. It did so on a technicality:

[2] As discussed at paragraphs 4.3 and 4.4 of my letter dated 16 June 2020.

"[That case] was brought in relation to the Law Enforcement Directive. It is therefore not applicable to this complaint under the GDPR."

(b) This *escamotage* enabled the ICO to disregard the warnings from the land's highest judges in relation to the issues of necessity and proportionality, which underpin the entire EU legal framework for data protection – from Art. 8 ECHR, via Art. 52 Charter all the way to Art. 5.1(d) GDPR:

"8 … The data controller cannot transfer personal data unless three conditions are met.

9. Condition 1 is that the transfer is necessary for any of the law enforcement purposes (section 73(2))… The test of necessity is a strict one, requiring any interference with the subject's rights to be proportionate to the gravity of the threat to the public interest…

"12. A transfer to a third country or international organisation is based on special circumstances if it is necessary for any of the five purposes listed in section 76(1). Only two could be relevant here: "(d) in individual cases for any of the law enforcement purposes; or (e) in individual cases for a legal purpose". Once again, the test of necessity is a strict one, requiring the controller to address his mind to the proportionality of the transfer. Crucially, however, section 76(2) provides: "But Page 5 subsection (1)(d) and (e) do not apply if the controller determines that fundamental rights and freedoms of the data subject override the public interest in the transfer." Once again, this obviously requires the controller to address his mind to the fundamental rights and freedoms of the data subject and to whether they override the public interest in the transfer."

5.2 Selective regard for French case law

(a) On the other hand, in a remarkable instance of *entente cordiale*, the ICO felt drawn by a recent decision by the French Administrative Court (*Conseil d'Etat*) in the case brought by the French Association of Accidental Americans.

(b) By contrast, the ICO conveniently disregarded a previous decision by the French Constitutional Court (*Conseil Constitutionnel*) concerning another transparency measure, notably the introduction of public register of trusts.[3] In that decision, France's constitutional court, which unlike its administrative counterpart deals exclusively with constitutional issues, held what follows:

"The freedoms proclaimed by Art. 2 of the French Declaration of the Rights of Man and of the Citizen of 1789, entail a right to respect for private life. Accordingly, the collection, registration, retention, consultation and communication of personal data must be justified on the basis of a public interest and must be carried out in a manner that is adequate and proportionate to the achievement of such objective."

(c) In the light of the conflicting case law in France, the overwhelming body of opinion from the European data protection authorities, and the growing case law from the CJEU and the EGC in relation to the necessity and proportionality principles, one

[3] Decision no. 2016-591 QPC of 21 October 2016

should have expected the ICO to involve the Courts, not least because the ICO acknowledged that 'FATCA does not rise to the gold standard' of data protection:

6. **'FATCA not the gold standard of data protection – *but that's okay with us*'**

6.1 In what would appear as a *prima facie* acknowledgement of the concerns raised by Jenny, the ICO accepted that:

> "*the FATCA Legal Framework does not rise to the gold standard set out in the EDPB Guidelines.*"

6.2 Nevertheless, the ICO did not see anything wrong with this. In the opinion of the ICO:

> "*FATCA falls on the spectrum of compliance provided by the EDPB guidelines. When the US-UK IGA is next reviewed, we recommend that the parties take into account at an early stage any applicable guidelines on Art. 46.2(a) GDPR.*"

6.3 There are two problems with this.

(a) Firstly, the ICO has not shown *how* the US-UK IGA complies with the EDPB Guidelines, as the ICO's decision does not contain any reasoned comparison between the provisions of the US-UK IGA and the EDPB Guidelines. We, by contrast, carried out a careful analysis in our letter dated 6 March 2020 of which we provided you a copy.

(b) Secondly, whilst the GDPR was introduced with the stated objective to "*give citizens back control over their data and create a high level of data protection*", the decision from the ICO seems to suggest that there are two standard of data protection: a high (gold) standard for private companies, and a lower (silver or bronze) standard for public authorities.

7. **'HMRC might have breached its obligations - *but that's okay with us*'**

7.1 The existence, seemingly, of two weights and two measures (one for the private sector and one for tax authorities) seems to be confirmed by the last point covered by the attached decision from the ICO. Thus, the ICO's decision dated 29 May 2020 states that:

> "*On the basis of the information we have considered, our view is that HMRC has complied with its data protection obligations in transferring of your client's personal data to the IRS, with one exception. We consider that HMRC may not have fully complied with its Art 14 transparency obligations.*"

7.2 Interestingly, the Austrian Data Protection Authority seems to have found a similar issue. Thus, in its decision dated 18 May 2020, the body led by the EDPB's Chair held as follows (my translation from German):

> "*The question of whether the Austrian authorities violated their transparency obligations under Art. 14 GDPR is not covered by this decision. This question will be dealt with separately.*"

7.3 Back to the UK and the ICO, the decision deals with the breach of the transparency obligations in the following way:

> *"Although HMRC may not have complied with all of its data protection obligations, having taken into account the circumstances of this case, we do not consider that it is necessary and proportionate to take any further regulatory action."*

7.4 Interestingly, the ICO's website says this about transparency:

> *"The right to be informed covers some of the key transparency requirements of the GDPR. It is about providing individuals with clear and concise information about what you do with their personal data.*
>
> *Getting this wrong can leave you open to fines and lead to reputational damage."*

8. Two weights, two measures?

8.1 Today's decision from the French *Conseil d'Etat* to uphold a €50m fine against Google for breaching its transparency obligations towards consumers compounds the sense of national data protection authorities applying two weights and two measures: one for commercial companies and another one for public authorities.

8.2 However, Art. 8 ECHR was introduced shortly after the Holocaust and at the height of Stalinism to protect individuals from the potential of abuse from public authorities - see Art. 8(2) ECHR (*'there shall no interference by a public authority with the right to private life*.). In turn, the EU Charter was adopted in 2000 shortly before the enlargement of the EU eastward in 2004, where a number of countries are under notice from the EU for issues relating to the Rule of Law.

8.3 By shielding tax authorities against legitimate claims from compliant citizens, the UK Information Commissioner's Office and the Austrian Data Protection Authority are turning the most basic data protection principles that underpin the democratic development of post-war Europe on their head.

8.4 In terms of numbers, in 2018 the CRS involved some 47m accounts for an aggregate value of over Eur 4.9 trillion, which is a huge number (it exceeds the GDP of most major economies, as explained in my letter dated 16 June 2020). It is difficult to see how the violation of basic GDPR obligations by national tax authorities could be seen as smaller than the violations attributed to Google in the French case.

9. Conclusions

9.1 Based on the above, it would appear that:

(a) The EDPB is now aware of two decisions by national data protection authorities that have failed to adequately consider the scope of their powers under the *Schrems* principle.

(b) The two decisions – which were published within 10 days of each other – appear to be highly coordinated. They adopt the identical approach in dealing with certain issues (e.g. transparency obligations) and avoiding others (compatibility with

fundamental rights, ignoring case law from the CJEU and the EGC, and ignoring the consistent opinions from the WP29, the EDPS, the AEFI Group and even the Parliament).

(c) The two decisions are imbued with a desire to spare the tax authorities from any criticism. To this extent, they appear to be supported by political motivations.

(1) Indeed, on 20 May 2020 the ICO sent me the attached email which states *inter alia*:

> *"Dear Mr Noseda*
>
> *As you are aware, this matter has received attention from our legal team, who are now seeking a policy view in order to finalise our response to you and HMRC."*

(2) However, in *Elgizouli* (the UK Supreme Court judgment that the ICO decided to ignore), the UK's highest judges declared that a transfer of data to the US was illegal because:

> *"227. It is apparent that the decision was based on political expediency, rather than strict necessity under the statutory criteria. There was no consideration as to whether transfer of 'personal data' as such was required."*

(3) It should clear by now to national data protection authorities that their role is to stand up for individuals' fundamental data protection rights, and act independently. After all, the motto of the ICO (according to its website) is: *"The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals."*

(d) In both cases, the national data protection authorities are shifting the responsibility (and costs) of having the legal framework of FATCA and the CRS tested before the courts to the individual. This reflects the approach taken by the EDPB, which has led the European Parliament to conclude that the debate about FATCA is 'Kafkaesque'.

9.2 For all these reasons, I would reiterate the requests contained in our letters dated 3 June 2020 and 16 June 2020 that the EDPB take up its duties under the GDPR, by advising the European Commission and providing national data protection authorities with guidance about their role in implementing the GDPR.

9.3 As I said in my letter dated 16 June 2020, in the absence of any action, the responsibility for another hacking involving CRS or FATCA data would lie squarely with the EDPB.

Best regards,

Filippo Noseda
Partner

Direct Tel: +44 20 3321 7980
Direct Fax: +44 20 3761 1846
E-mail: filippo.noseda@mishcon.com