Irish Council for Civil Liberties

1st Floor 34 Usher's Quay
Dublin 8, Ireland
T: +353 1 912 1640
E: info@iccl.ie
W: www.iccl.ie

Executive Vice-President Vestager
Commissioner Didier Reynders
Commissioner Thierry Breton
Rue de la Loi 200
1049 Brussels
Belgium

cc
Michel Barnier, Head of the Task Force for Relations with the UK
Jeppe Tranholm-Mikkelsen, Secretary General of the Council
David McAllister MEP, Chair of the Parliament's EU-UK Coordination Group
Dr Andrea Jelinek, Chair of the European Data Protection Board

12 October 2020

The Commission's obligation to refuse an "adequacy decision" to the United Kingdom due to inadequacy of enforcement of personal data protection in that jurisdiction

Dear Executive Vice President Vestager,
Commissioner Reynders, and
Commissioner Breton,

I write on behalf of the Irish Council for Civil Liberties (ICCL), Ireland's oldest independent human rights monitoring organisation. We monitor, educate and campaign for all human rights, for everyone. I write to draw your attention to a deficit in the protection of personal data in the United Kingdom, which must make an "adequacy decision" for the transfer of personal data from the EU to the UK impossible at the present time.

Under the terms of Article 45(2)b of the GDPR, an adequacy decision is impossible because the UK's data protection supervisory authority, the Information Commissioner's Office (ICO), does not met the test of an "effectively functioning" supervisory authority.

Failure to act against the largest GDPR infringement in the UK
The ICO has shown itself to be incapable of discharging the tasks required of a supervisory authority under Article 57 of the GDPR and section 115 of the UK Data Protection Act, with respect to the largest data breach of all time:[1] Real-Time Bidding (RTB).

The RTB system operates behind-the-scenes on virtually every website and app, and constantly broadcasts the private things that people do and watch online, and where they are in the real world, to countless companies. There is no way of limiting what then happens to these data.

[1] See RTB scale in 2018-19 at https://www.iccl.ie/wp-content/uploads/2020/09/Scale-billions-of-bid-requests-per-day-RAN2019061811075588.pdf.

The RTB data free-for-all infringes Article 5(1)f of the GDPR. Many RTB companies that process the personal data of data subjects in the Union are established in the UK.

In January 2018, I blew the whistle about RTB infringements to the ICO. I was then an executive at company in the RTB industry.[2] Then, in September 2018, the Executive Director of the Open Rights Group and an academic at the University of London filed a formal GDPR complaint to the ICO about RTB. This complaint was a duplicate of the complaint that I filed with the Irish Data Protection Commission on the same day.[3] Ten months after receiving the complaint, the ICO published a report validating our evidence of the enormous scale and severity of the RTB infringement.[4]

Even so, despite the fact that the enormity of the data protection infringements were publicly acknowledged by the ICO in its report, it did not take action to end the infringements. Instead, it accepted gestures from the infringers that did not limit or correct the infringements.[5] As a result, infringements of the GDPR by RTB companies established in the UK have increased in the years since the ICO was notified.[6]

The consequences of this should be of utmost concern to the European Commission, endangering the right to protection of personal data and going so far as to interfere in elections within the Union. For example, profile data leaked by the RTB system were used to profile LGBTQ+ people in Poland in order to influence the 2019 Parliamentary Election.[7]

The ICO has failed over the last two years to take any substantive action against the largest data breach that the UK and EU have ever experienced. It would be unreasonable to anticipate that it will perform any better after Brexit is complete.

The UK Government's "explanatory framework"

In March 2020, the UK Government published "explanatory framework" documents that it claims "provide the information necessary for the Commission to plan and conduct its assessment"[8] for an adequacy decision.

---

[2] See chronology of ICO failure in "Surveillance on UK council websites", Brave, 4 February 2020 (URL: https://brave.com/ukcouncilsreport/), p. 8.

[3] "Grounds of complaint to the Data Protection Commissioner", Ravi Naik acting for Johnny Ryan, 12 September 2018 (URL: https://www.iccl.ie/wp-content/uploads/2020/09/DPC-Complaint-Grounds-12-Sept-2018-RAN2018091217315865-1.pdf).

[4] "Update report into adtech and real time bidding", ICO, 20 June 2019 (URL: https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf), p. 20-23.

[5] "Adtech – the reform of real time bidding has started and will continue", ICO, 17 January 2020 (URL: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/01/blog-adtech-the-reform-of-real-time-bidding-has-started/).

[6] For example, "IndexExchange", a large RTB company that has an establishment in London, today sends 120 billion broadcasts about people's online behaviour per day, whereas at the time of the complaint in 2018 it sent 50 billion such broadcasts. See source in footnote 2.

[7] "New data on the RTB privacy crisis: people with AIDS profiled in Ireland, and Polish elections influenced", Irish Council for Civil Liberties, 21 September 2020 (URL: https://www.iccl.ie/human-rights/info-privacy/rtb-data-breach-2-years-on/).

[8] "Explanatory Framework for Adequacy Discussions", section A, UK Government Department for Digital, Culture, Media & Sport, 13 March 2020 (URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872228/A_-_Cover_Note.pdf), p. 1.

The claims about the ICO in these documents merit further examination:

First, the UK Government suggests that the ICO is "capable of handling complex cases and imposing tough sanctions where necessary", and points to the issuing of 13 monetary penalties since the application of the GDPR on 25 May 2020.[9] However, by September 2020 the ICO had actually issued only a single fine under the UK Data Protection Act that implements the GDPR,[10] though it had issued fines on matters outstanding under previous legislation. Indeed, the ICO has found itself unable to proceed with the major fines that it had announced under the GDPR.[11]

Second, the UK Government claims that the ICO is among the "three most active data protection authorities in recent years in terms of individual fining decisions".[12] However, the citation on which this claim relies refers to a conference paper from 2017 that predates the GDPR, and which does not appear to substantiate the claim.[13]

Third, the UK Government writes that the ICO has a staff of approximately 750, a budget of €55.65 mil, and "world-leading expertise in niche areas such as the impact of new technologies and privacy rights".[14] It further asserts that "almost all" of the ICO's budget "supports data protection compliance".[15] However, documents obtained under freedom of information show that the ICO had 680 full time equivalent staff, of which only 21 are specialist tech investigators. Moreover, only 8 people work in the ICO's "Cyber incident response & investigation unit".[16]

In other words, the ICO may be the biggest and most expensive supervisory authority to operate, but it is not configured to monitor and enforce data protection in the digital age. Indeed, only 1 per cent of its staff is devoted to this purpose.

An adequacy decision for the UK

The document in which the UK Government presents the ICO as an asset in its case for an adequacy decision is almost entirely devoted to describing the legal framework that provides the ICO's investigative and enforcement powers. There is very little space given to discussing the ICO's actual performance.[17] Irrespective of the fact that the UK has integrated the EU acquis into its national law, the mere fact that a supervisory authority exists in name does not mean that the rights of data subjects in the Union will be protected in practice. As Article 45(2) observes, both the "the existence and effective functioning" of a third country's supervisory should be considered when evaluating that country's adequacy.

---

[9] "Explanatory Framework for Adequacy Discussions", section A, p. 2.

[10] "Penalty Notice to Doorstep Dispensaree Ltd.", ICO, 20 December 2019 (URL: https://ico.org.uk/media/action-weve-taken/mpns/2616742/doorstop-mpn-20191217.pdf).

[11] See "Intention to fine British Airways £183.39m under GDPR for data breach", ICO, 8 July 2019; and "Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach", ICO, 9 July 2019 (URL: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/).

[12] "Explanatory Framework for Adequacy Discussions", section A, pp 2-3, and section G, p. 3.

[13] "Fines under the GDPR", CPDP 2017 Conference Book (URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3270535).

[14] "Explanatory Framework for Adequacy Discussions", section A, p. 3; and section G, p. 1.

[15] ibid., p. 1.

[16] See detail in "Europe's governments are failing the GDPR: 2020 report on the enforcement capacity of data protection authorities", Brave, April 2020 (URL: https://brave.com/wp-content/uploads/2020/04/Brave-2020-DPA-Report.pdf).

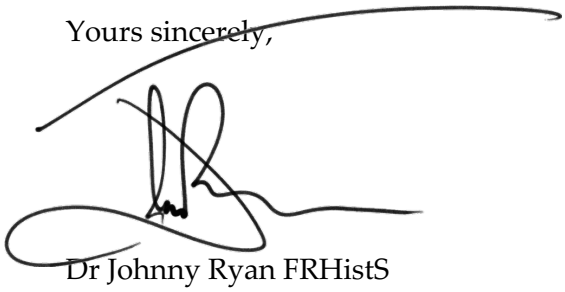
[17] "Explanatory Framework", section G.

Failure to secure an adequacy decision from the European Commission would introduce friction and uncertainty to EU-UK data transfers that could jeopardise 13% of the UK's global exports. The UK Government reports that UK exports of "personal data-enabled services" to the EU accounted for £85bn in 2018.[18] The UK's total global exports in the same year were £655.5bn.[19] For perspective, the entire UK fishing industry had a GDP of only £0.75 bn last year.[20] The stakes are therefore very high for the UK.

However, both the UK and the EU recognised in their Political Declaration that it would be impossible for the European Commission to adopt an adequacy decision unless "the applicable conditions are met".[21] EU data protection law is clear about what these conditions are. Article 45(2) of the GDPR provides that "the Commission shall, in particular, take account of … the existence and effective functioning of one or more independent supervisory authorities" when determining whether a third country should be the subject of an adequacy decision.

The UK lacks an effective independent supervisory authority that is capable of enforcing compliance with data protection law and vindicating data subjects' rights. As a consequence, the personal data of data subjects in the Union do not at present have an adequate level of protection in the UK. Therefore, we suggest to you that the inescapable conclusion is that the UK must be unable to benefit from an adequacy decision at the present time.

Yours sincerely,



Dr Johnny Ryan FRHistS
Senior Fellow of the Irish Council for Civil Liberties
Senior Fellow of the Open Markets Institute

[18] "Explanatory Framework", section A, p. 1.
[19] "Statistics on UK-EU trade", Briefing Paper No. 7851, House of Commons, 17 June 2020 (URL: http://researchbriefings.files.parliament.uk/documents/CBP-7851/CBP-7851.pdf).
[20] "UK Sea Fisheries Statistics 2019", UK Marine Management Organisation, (URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/920679/UK_Sea_Fisheries_Statistics_2019_-_access_checked-002.pdf), p. 55.
[21] "Political Declaration setting out the framework for the future relationship between the European Union and the United Kingdom", 17 October 2019, paragraph 9.