Written evidence on the

Data Protection and Digital Information (No.2) Bill ("DPDI2")

submitted by Tim Bell, Managing Director of Data Protection Representative (UK) Limited (trading as DataRep UK)

Specifically relating to Section 13 of DPDI2, which proposes to remove the obligation that companies outside the UK should appoint a Representative within the UK.

Data Protection Representative (UK) Limited (trading as DataRep UK) is a company incorporated in the UK with registered number 12953008. DataRep UK provides the UK GDPR Representative service to its clients outside the UK. Details about DataRep UK and its services can be found on its website here: www.datarep.uk.

Tim Bell is available to attend the committee considering DPDI2, should they wish to hear evidence in person.

This evidence is without prejudice to the observations of other commentators relating to other sections of DPDI2; this submission is limited to the proposals in Section 13, as that is the area of specialisation of the author.

Executive Summary:

- The benefit of removing the obligation to appoint a UK Data Protection Representative – as proposed in Section 13 of DPDI2 – is minimal, and far outweighed by the benefits of retaining this obligation.
- Specifically:
    - The UK Representative aids UK citizens' access to data protection rights;
    - The ICO would find cross-border enforcement significantly harder without the existence of a UK Representative;
    - The only benefit of removing the Representative obligation (removing a barrier to trade) has been significantly overstated;
    - The current lack of evidence for the benefit of a Representative is the result of the brief period of enforceability of the current regime, not its overall effectiveness or usefulness; and
    - Removing the Representative obligation may be viewed negatively by the EU when considering the UK's GDPR adequacy status.

Background:

1. The current UK legislation (specifically UK GDPR Article 27) obliges companies outside the UK, which are selling to the UK or monitoring people here, to appoint a UK-based Data Protection Representative. This obligation was proposed to be removed by the previous DPDI Bill – despite that proposal not being mentioned in the consultation which preceded it, so that this evidence could be provided prior to the reading of that first Bill – and that proposal remains in DPDI2.

2. Summarised, the roles of the UK Data Protection Representative are primarily (a) to facilitate communications between UK-based data subjects / the Information Commissioner's Office ("ICO") and those companies outside the UK which are processing UK personal data, and (b) to ensure that the ICO and UK-based individuals are able to enforce their data protection rights against companies which cannot be reached in the UK (e.g. social media, marketing and software-as-a-service (SaaS) companies based outside the UK delivering their services via the cloud)[1].

Evidence

3. The UK Representative aids UK citizens' access to data protection rights

4. The UK Representative gives UK-based individuals a route to access their data protection rights – e.g. to view, correct or erase their personal data – with businesses outside the UK.

5. There are a huge number of these businesses already in existence, and more being created daily, with ever-expanding ways of exploiting the personal data which they obtain. Because the business case for having a UK office simultaneously diminishes when those businesses can deliver their services online via the cloud, this locally-based route to accessing the rights which have been granted to UK citizens is increasingly essential if those individuals are to be able to obtain a useful, rather than theoretical, benefit from the data protection rights granted to them.

6. If the obligation to appoint such a Representative is removed, it is likely those individuals' ability to access and effect their rights would be significantly reduced. The businesses which are processing that personal data, being otherwise out of reach of those individuals, would find it increasingly easy to ignore, delay or otherwise frustrate the efforts of those individuals to access their rights if there was no reliable location at which, and no reliable organisation with whom, they could be raised.

7. The difficulty in accessing those data protection rights can be identified already where data subjects have not been able to obtain responses to their requests, or

[1] See ICO website here for more information on the current obligation: https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/the-uk-gdpr/uk-representatives/

even to find a point of contact at which to raise such requests. Removing this route to access rights is likely to increase the large proportion of the data protection complaints received by the ICO which relate to ignored / delayed responses to data requests, or inadequate responses to them.

8. In the most-recently reported set of data issued by the ICO setting out the data protection complaints received in Q3 2022/23, 59.4% (5,786 of the 9,748) of complaints related to issues under Articles 15-21 of UK GDPR, the sections which confer on individuals their rights to access, correct, erase or object to the use of their personal data. In the quarter prior to that (Q2 2022/23), it was roughly similar at 58.5% (5,522 of 9,443 complaints).[2]

9. It isn't clear what percentage of those requests relate to processing by organisations outside the UK but – whatever that proportion – I believe it is reasonable to assume that removing a route to access those rights would result in an increase in dissatisfaction from those individuals regarding their ability (or otherwise) to give useful effect to those rights – and correspondingly more complaints to the ICO.

10. The ICO would find cross-border enforcement significantly harder without the existence of a UK Representative

11. The UK Information Commissioner's Office (ICO) would face significant difficulties bringing effective enforcement of the UK data protection regime against businesses outside of the UK if they were not able to access those companies via a UK-based Representative.

12. As is the case for UK citizens who seek to exercise their rights, to undertake a useful investigation or enforcement action against a company outside the UK, it will be necessary for the ICO to be able to contact them – whether to request information, issue formal notice of proceedings, or provide details of any resulting enforcement action issued against them.

13. The existence of the UK Representative ensures that the ICO can do this for the subjects of their investigations which have no UK presence; the ICO's communications with the Representative would be acknowledged, and the physical post sent would be signed for, giving clarity as to the effective service of those communications and avoiding a situation where those non-UK businesses could deny or ignore receipt, delaying and frustrating the investigation and enforcement process.

14. The benefits of the Representative obligation to enforcement of the EU GDPR, the source of this obligation in the UK regime, have recently been set out in a report[3] by

[2] Data sets available for download here: https://ico.org.uk/about-the-ico/our-information/complaints-and-concerns-data-sets/data-protection-complaints/

[3] "Study on the enforcement of GDPR obligations against entities established outside the EEA but falling under Article 3(2) GDPR", https://edpb.europa.eu/system/files/2023-04/call_9_final_report_04112021_en_0.pdf

the European Data Protection Board[4]. They concluded that: "It is clear that the appointment of a controller/processor representative is crucial to the enforcement of [supervisory authorties'] investigative and corrective powers. Non-compliance with Article 27 GDPR should be punished under Article 83(4)a of the GDPR (administrative fines)."[5]

15. Another aspect of enforcement which is rarely discussed is the benefit of this obligation, when seeking to enforce data protection obligations against businesses outside the UK, if those businesses have ***not*** made this appointment.

16. It is easy for the ICO to identify a failure to appoint a UK Representative – the publicly available privacy notice of the business will include neither a UK contact address, nor an address at which their UK Representative can be reached – and, having identified that failure, to bring an enforcement action in the first instance for that failure. Compared to other parts of the data protection regime which permit for a degree of objectivity, this is effectively a strict liability offence (or at least one for which non-compliance can be presumed, and an argument to the contrary elicited from the allegedly non-compliant party as a result): no UK location + no UK Representative = UK data protection law violation.

17. Once that initial enforcement is achieved, that award can then be used to leverage access to the reticent business (e.g. via their internet host, which would decline to provide information until a court order to do so had been obtained) to investigate other issues with their personal data management, an opportunity which may not have been available if the Representative obligation did not exist.

18. This is the enforcement route taken by the Netherlands data protection authority against locatefamily.com, a website which processes large volumes of personal data, apparently without the necessary mechanism permitting them to do so – that company had refused to provide the authority with details of their incorporation, so it had not been possible to investigate them effectively without first fining them for the Representative failure[6].

19. Put simply, the *failure* by a business outside the UK to appoint a Representative, when they are required to do so, can also be of assistance to the ICO.

20. Without the Representative obligation, a business outside the UK which wishes to make it difficult for the ICO to investigate their activities (i.e. the types of business which the ICO are most-likely to want to investigate) will find it significantly easier to

---

[4] The European Data Protection Board (EDPB) is an independent European body, which contributes to the consistent application of data protection rules throughout the European Union, and promotes cooperation between the EU's data protection authorities. https://edpb.europa.eu/concernant-le-cepd/concernant-le-cepd/who-we-are_en

[5] Paragraph 2.6.5, https://edpb.europa.eu/system/files/2023-04/call_9_final_report_04112021_en_0.pdf

[6] https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-imposes-fine-%E2%82%AC525000-locatefamilycom, an article by the author relating to this enforcement action can be viewed here: https://www.datarep.com/2021/05/12/locatefamily-com-fined-e525000-gdpr-article-27-representative-enforcement-action/

frustrate those investigations than they would have done. The existence of the Representative obligation is therefore a win-win for the ICO; either the appointment has been made, making contact with the subject of their investigation easier, or no Representative has been appointed and an immediate enforcement action can be obtained for that failure.

21. The impact assessment provided with DPDI2, updated on 19 April 2023[7] (the "**Impact Assessment**"), proposed that businesses outside the UK may choose to appoint a UK Representative, despite there being on obligation to do so. Because, as explained above, it would be harder to enforce the UK data protection regime against companies outside the UK which had chosen not to make this appointment, appointing a UK Representative would be heavily disincentivised, especially for those businesses which know or suspect that they are not fully in compliance. In that context, "enabling them to make a decision"[8] may not be the best route to obtaining satisfactory management of UK citizens' personal data.

22. The argument has been made in a UK court that "the bad guys do not appoint Art.27 representatives"[9]; that failure to do so when required may ultimately be the omission which enables the ICO to bring effective action against them.

23. <u>The only benefit of removing the Representative obligation (removing a barrier to trade) has been significantly overstated</u>

24. The only likely benefit to be achieved by the proposed removal of the Representative obligation – that a barrier to trade with the UK would be removed – has been significantly overstated in the Impact Assessment.

25. It is clear that requiring a business outside the UK to appoint a UK Representative is an activity which would be an "administrative burden"[10], costing that business money, and potentially taking time, to achieve. In that regard, the accusation that it is a barrier to trade must be considered as a potentially reasonable observation.

26. However, the same can be said about the remainder of the UK data protection regime, and all other obligations placed on businesses trading in the UK; the relevant issue is whether the benefits of erecting that barrier outweigh the efforts required to overcome it.

27. Other than the cost, the Impact Assessment suggests a couple of potential positive impacts of removing the Representative obligation, without justifying them:

---

[7] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1151358/data_protection_and_digital_information_bill_impact_assessment_march_2023.pdf

[8] Impact Assessment, paragraph 595

[9] Rondon v LexisNexis [2021] EWHC 1427 (QB): https://www.bailii.org/ew/cases/EWHC/QB/2021/1427.html

[10] Impact Assessment, paragraph 590

a. That there are already obligations in the UK regime which permit the business processing the personal data to be contacted[11]; but the Representative obligation is not an obligation *permitting* contact, but requiring a route through which that contact can effectively be made; and

b. That removing the obligation to appoint a Representative may "reduce the potential for conflict with trade commitments"[12], without identifying any specific commitment or situation in which such conflict may arise.

28. With that being the case, it appears that the only real benefit to a business outside the UK which is intending to achieve compliance, is to remove the cost associated with the appointment of a UK Representative.

29. However, taking into account (a) the work and cost involved with meeting the remainder of UK data protection regime (even after the changes proposed by DPDI2), (b) that many of those businesses are also likely to need a Data Protection Representative in the EU/EEA, Switzerland, China and other jurisdictions, and (c) the fact that the Impact Assessment failed to identify any significant excessiveness in the cost of making this appointment (acknowledging themselves that there are a number of different options for pricing models and service levels available in the market[13]) the additional cost and work involved in appointing a UK Representative is likely to be comparatively minimal when viewed in the context of a wider compliance program. Even if the cost was currently excessive – which I do not believe is the case – the market would naturally rebalance to correct this position.

30. The authors of the Impact Assessment acknowledge that they "are unable to provide quantitative estimates of the impacts of removing the requirement for a representative"[14]. The author proposes that, when the benefits set out above are taken into consideration, the impact of relevant businesses outside the UK using existing information (created as part of an existing an ongoing compliance program) to obtain a UK Representative at a cost which is – in relative terms – reasonable, provides a worthwhile balance of benefits to the UK and does not comprise a significant barrier to trade.

31. <u>The current lack of evidence for the benefit of a Representative is the result of the brief period of enforceability of the current regime, not its overall effectiveness or benefits</u>

32. The reason little evidence exists as to the benefits of a UK Representative to the UK[15] (by way of aiding the enforcement of the UK data protection regime by the ICO), is

[11] Impact Assessment, paragraph 591
[12] Impact Assessment, paragraph 592
[13] Impact Assessment, paragraph 585
[14] Impact Assessment, paragraph 587
[15] Impact Assessment, paragraph 583

because the ICO has, to date, largely focused enforcement on UK-based organisations and large multi-national organisations which also have a UK location. As a result, there has been little (but not zero) need for them to make use of the UK Representative obligation as an enforcement tool against the organisations they have been investigating and enforcing against.

33. In due course, as (a) those UK and larger international organisations improve their data protection, (b) UK citizens increasingly ask the ICO to enforce their rights against smaller businesses, and (c) the ICO necessarily turns their attention to non-global businesses outside the UK (which can comprise some extremely large companies processing very large volumes of UK personal data in ways which may not be satisfactory to the individuals to which that data relates), the inability (for the reasons set out above) of the ICO to bring effective enforcement against those businesses without a UK Representative would make a mockery of the proposed regime and its stated aim to protect the personal data of individuals in the UK.

34. The current situation, where adherence to this obligation has not reached the level anticipated by the current regime, is not an incentive to remove it; it would – in the author's opinion – be odd to treat a reticence to comply with a law as a good reason to drop it. Because failing to meet this obligation is easily identifiable from publicly available information, this can be easily identified by the ICO in their investigations, giving them an immediate opportunity to bring to the table those businesses they believe are misusing, or not sufficiently protecting, the personal data of UK citizens.

35. Indeed, the perceived lack of complete compliance with the Representative obligation may be traced to the ICO's reluctance to enforce that obligation to date; were they to do so (e.g. by performing a quick review of companies which are likely to need a Representative), they would achieve a quick and public "win" against UK data protection law non-compliance, and simultaneously make compliance with the UK Representative obligation more desirable. If the ICO was inclined to do so, I'd propose the list of companies which remain signed up to the Privacy Shield as a starting point – these companies all trade with Europe with no EU location (and therefore also likely target the UK), and research undertaken by the author's organisation suggested it would be easy to identify non-compliance with this obligation.[16]

36. As a result, retaining the Representative obligation ensures a robust and effective data protection regime for the UK into the future, notwithstanding that it may not have been fully utilised (or complied with) to date.

37. <u>Removing the Representative obligation may be viewed negatively by the EU when considering the UK's GDPR adequacy status</u>

[16] https://www.datarep.com/2020/10/29/privacy-shield-research-were-privacy-shield-participants-compliant-with-gdpr/

38. Although removing this obligation, which exists under EU GDPR, may count as a negative effect when the EU reconsiders the identification of the UK as an adequate country for the purposes of GDPR, this is not on its own likely to be a deciding factor – some other countries which have been granted "adequate" status do not have an equivalent Representative obligation under their laws.

39. However, combined with other changes proposed in DPDI2, it would be part of the considerations of the EU when making this decision, and may add weight to the position that the UK is no longer adequate, which would lead to a significant barrier to trade for UK businesses aiming to sell to the EU, and much greater costs for those UK businesses than are currently faced by the businesses outside the UK which are required to appoint a UK Representative.

40. The weight which may be applied to the removal of the UK Representative obligation may ultimately be greater than that which would be applied to a country which never had this obligation. When considering whether the UK is adequate *and likely to remain so*, the EU is likely to consider the trajectory taken with its data protection regime – at a time when many countries are adding a Representative obligation to their data protection laws (e.g. Switzerland, Turkey, China, Thailand etc), the removal of this protection by the UK may be viewed by the EU as an indication that data protection rights will continue to be eroded in the UK, which may give rise to greater concerns when considering whether the UK adequacy status should remain in place.

Conclusion

41. When balanced against the single benefit of removing the UK Representative obligation (that businesses outside the UK would save a relatively small sum when they appoint a UK Representative) the benefits to the UK of retaining the UK Representative obligation – particularly the convenient access of UK citizens to their data protection rights, and the effectiveness of the ICO's enforcement activities against businesses outside the UK – are clear and overwhelming.