LEGAL & REGULATORY COMPLIANCE CONSULTANTS

WRITTEN EVIDENCE SUBMITTED BY

HANDLEY GILL LIMITED (DUAB20)

TO THE HOUSE OF COMMONS PUBLIC BILL COMMITTEE ON THE DATA (USE AND ACCESS) BILL

MARCH 2025

Contents

Executive Summary

1. We are grateful that Handley Gill Limited has been afforded the opportunity to submit written evidence to the Committee on the Data (Use and Access) Bill.

2. In preparing this evidence, we have had regard to our comprehensive briefing on the Bill (as introduced)[1] and the unofficial Keeling Schedules[2] we have prepared which demonstrate the changes that the Bill (as introduced) would have on the Data Protection Act 2018, UK GDPR and Privacy and Electronic Communications (EC Directive) Regulations 2003, respectively. We will also imminently publish updated unofficial Keeling Schedules to reflect the Bill as brought from the Lords. We have also published several briefings on the Bill and its passage, which are accessible via the Data Protection Reform page[3] of the Resources section[4] of our website.

3. Having regard to the restrictions on the submission of written evidence we have limited our evidence to the issued identified above and below.

4. In summary, our evidence to the Committee is as follows:

    a. The Bill adds further complexity to, rather than simplifying, the UK's data protection framework and fails to significantly reduce the burden imposed on the majority of data controllers;
    b. The Bill is half-baked, granting the Secretary of State widespread powers to make significant changes to the scope and effect of the legislation which will not be subject to appropriate input and scrutiny;

[1] https://www.handleygill.co.uk/handley-gill-blog/data-use-and-access-bill-hl-bill-40-as-introduced
[2] https://www.handleygill.co.uk/data-use-access-bill-unofficial-keeling-schedules
[3] https://www.handleygill.co.uk/data-protection-reform
[4] https://www.handleygill.co.uk/resources

c. Delay and inaction in enforcement of the data protection legislation, and the difficulties in pursuing collective action through the courts, have resulted in the regrettable situation that compliance does not pay, having an adverse effect on competition and hindering UK growth;
d. We do not consider that there is a high risk of the European Commission refusing to renew its adequacy decision in respect of the UK, notwithstanding the departures from the UK GDPR and EU approach to the regulation of artificial intelligence;
e. The Bill will materially diminish the level of protection afforded to data subjects in respect of overseas transfers of personal data;
f. The failure of the Information Commissioner to have any or proper regard not only to its obligation to ensure appropriate protection for data protection but to uphold other human rights, in particular the right to freedom of expression and information, poses significant concerns in connection with the proposed powers of interview and the panel process to be implemented in respect of codes of practice;
g. The processing of personal data utilising artificial intelligence will be significantly increased without appropriate safeguards or clarity as to the requirements of the law, and has the potential to particularly have an adverse impact on women;
h. Efforts to utilise the Bill to amend the Computer Misuse Act 1990 should be resisted; and,
i. Other measures could be implemented to improve the UK's approach, including: to permit the police to prosecute data protection offences; to impose a backstop timeframe for data controllers to respond to data subject complaints; to require all data controllers to monitor and record infringements; and, to implement effective consideration of the rights of data subjects in connection with processing likely to pose a high risk, to their rights and freedoms.

A Missed Opportunity

5. We remain disappointed that the government has failed to take the opportunity presented to reform and consolidate the UK's data protection legislation, making it simpler for organisations to understand and comply with, and that the Bill instead amends and augments the existing legislative framework and must be read in conjunction with it, bringing further complexity.

6. Furthermore, we anticipate that in practice the Bill will not have a significant impact for most data controllers in reducing the compliance burden imposed upon them.

7. The progress of the Bill independently of any measures to pursue the regulation of artificial intelligence and the promised Cyber Security and Resilience Bill, in particular, is unhelpful.

Enforcement

8. In response to a request under the Freedom of Information Act 2000, the Information Commissioner's Office recently revealed[5] that of the 28,582 data protection complaints it received in 2024 and which had concluded, it took regulatory action in respect of just one of those complaints. This is consistent with the position in previous years when a mere 0.02% of cases resulted in regulatory action[6]. It should also be considered against the backdrop that the ICO's own scorecard reveals that since Q4 of 2023/24 it has consistently failed to meet its target of assessing and responding to 80% of data protection complaints within 90 days and is getting progressively worse, with its performance in Q2 2024/25 languishing at 35.9%.

9. This is by design, with the Information Commissioner having informed The Times that *"I don't believe that the quantum or volume of fines is a proxy for impact"*[7] and suggesting that it was too difficult to impose fines on US Big Tech, notwithstanding Recital 148 to the UK GDPR[8] stating that *"penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation"*, albeit that it is suggested that minor infringements or those having a disproportionate burden may warrant a reprimand.

10. While we are advocates of proportionate regulation utilising the full range of enforcement powers available to educate, encourage trust and confidence and address infringements, regrettably the Information Commissioner's approach to the enforcement of data protection legislation fails to meet the requirement of being *"effective, proportionate and dissuasive"* and, coupled with the restrictive implications of court judgments for the ability to bring collective proceedings to hold data controllers to account, fails to create an environment in which compliance pays, thus distorting competition and particularly favouring foreign incumbents over UK companies, hindering UK growth. While clause 91 would require the regulator to have regard in carrying out its functions to the desirability of promoting innovation and competition, this appears to have been erroneously interpreted by the government and regulator as meaning not enforcing the law.

[5] https://ico.org.uk/media2/migrated/4032498/ic-353505-c3d8-response-letter.pdf
[6] https://questions-statements.parliament.uk/written-questions/detail/2023-06-09/188734
[7] https://www.thetimes.com/article/caba21bf-8171-441e-b5b5-a8c9ec34203c?shareToken=e06eb92e112d603979f069635d423959
[8] https://www.handleygill.co.uk/uk-gdpr/#Recitals

11. While the Bill will serve to enhance oversight of the regulator's performance by increasing transparency, it does not include any provisions in and of themselves aimed at increasing enforcement or improving outcomes for data subjects. Nor does it address the inadequate record keeping at the ICO which prevents its policy positions and performance from being interrogated.

The European Commission's Adequacy Decision in Respect of the UK

12. While we are aware that several commentators and Parliamentarians have expressed concern that any further departure from the EU GDPR would jeopardise the European Commission's adequacy decision in respect of the UK, we do not believe that the Data (Use and Access) Bill in its current form presents a significant risk of its withdrawal.

13. The European Commission's adequacy decision in respect of the UK was explicitly and uniquely subject to a sunset clause and stated to be based on the lack of divergence from the EU GDPR and *"adherence to the European Convention of Human Rights and submission to the jurisdiction of the European Court of Human Rights. Continued adherence to such international obligations is therefore a particularly important element of the assessment on which this Decision is based"*. This was coupled with a threat of early intervention if *"anything changes on the UK side"*. Despite this, membership of the Council of Europe and adherence to the ECHR is not a requirement for adequacy, as evidenced by the Commission's adequacy decisions in respect of Israel, Japan and the US.

14. We acknowledge and accept that UK law and regulation present several grounds upon which UK adequacy could be challenged, including the scope of protection for processing for national security, the commitment to the rule of law and submission to the Strasbourg court having regard to the Safety of Rwanda (Asylum and Immigration) Act 2024 and, the state of enforcement and the availability and effectiveness of remedies available to data subjects, and that there are increasing divergences between the EU and UK particularly in the context of the regulation of artificial intelligence (AI).

15. We consider that it is apparent from the Commission's decision pertaining to the US and data transfers under the Data Privacy Framework that an adequacy decision is largely a politically driven one. In 2022, the UK exported £340 billion of goods and services to the EU, 42% of total UK exports, whereas the UK imported £432 billion from the EU, 48% of total UK imports[9], and it is therefore in the economic and wider interests of both the UK and EU that barriers to data transfers are minimised.

[9] https://commonslibrary.parliament.uk/research-briefings/cbp-7851/

Secretary of State's Powers

16. The Bill is half-baked; the true extent of the impact of the Bill on the UK's data protection legislation remains unclear and incapable of scrutiny given the extent of the powers proposed to be granted to the Secretary of State to make regulations amending the Bill, including lawful bases for processing, exemptions etc. Having regard to the government's stated commitment to economic growth, we anticipate that these powers will be used to further relax the requirements of the data protection legislation, further diminishing the rights of data subjects.

Overseas Data Transfers

17. The threshold for making regulations permitting the transfer of personal data overseas will be materially lowered from the current requirement that the third country offer *"an adequate level of protection of personal data"* to one of meeting the *"data protection test"*, which means offering a standard *"not materially lower than the standard of the protection provided for data subjects by or under"* UK law and, in such cases, removing the obligation on data controllers to conduct International Data Transfer Impact/Risk Assessments in respect of the transfer. The factors to be taken into account are also relaxed, with the effectiveness of any data protection regulator in the third country no longer being relevant meaning that if on paper a country has strong laws but these are renowned for not being enforced then this would not prevent regulations being made. The obligation to conduct formal reviews every four years would also be removed. In practice, this significantly reduces the protections available to data subjects in relation to overseas transfers.

Implications for journalism

18. We are concerned by the potential for the panel process for the development of codes of practice (some of which continue to be outstanding) to be effectively hijacked by special interest groups. The Information Commissioner has not in recent years demonstrated a strong track record in complying with the obligations not only to ensure appropriate protection for data protection rights but also to protect other human rights, such as the right to freedom of expression and information[10], and we would therefore welcome clause 93 being amended so as to exclude the journalism code from its scope.

19. We are also concerned as to the scope for the regulator to compel witnesses to attend interview in connection with the processing of personal data for the purposes of journalism, notwithstanding the proposed carve out at clause 100.

[10] See: https://www.handleygill.co.uk/handley-gill-blog/ico-search-warrant-special-purposes and https://www.handleygill.co.uk/handley-gill-blog/data-protection-journalism-code-consultation-response

Artificial Intelligence

20. Particularly in light of the government's position to effectively gift copyright works to foreign tech companies[11], purportedly in the interests of UK growth, we are concerned that the proposals contained in Part 1 of the Bill will be re-purposed to require the publication and disclosure of proprietary and/or commercially sensitive data to AI developers.

21. We are concerned by the proposals at clause 80 of the Bill that would grant the Secretary of State power to make regulations establishing what constitutes meaningful human involvement in automated decision-making and what constitutes a decision having a similarly significant effect to a legal decision, and the minimal input and scrutiny to which any such regulations would be subject. We would welcome clarity in this regard however, and would prefer these to be mandatory.

22. We are advocates for the safe, ethical and responsible deployment of artificial intelligence[12] and support our clients to do so, but we are nevertheless concerned that, in the absence of any AI-specific legislation and any effective current regulation of artificial intelligence, whether by the ICO, the EHRC or sector specific regulators, or even industry codes of practice as to the responsible use of artificial intelligence, the knowledge and framework for the responsible and ethical deployment of AI is lacking and to remove restrictions on automated decision-making based on non-special category personal data, including characteristics such as sex (which is a protected characteristic under the Equality Act 2010 but does not constitute special category personal data) will result in a rapid expansion of the use of AI including in circumstances such as recruitment, which were recently identified as a matter of concern by the ICO following its audit of several providers and developers of AI tools for recruitment[13]. Expanding the restriction at clause 80 so as to apply not only to special category personal data but also to protected characteristics could seek to preserve some measure of protection. We would also welcome additional safeguards in respect of automated decision-making.

23. We would welcome clause 80 being amended to clarify the scope of information to be provided to data subjects in relation to automated decision-making relating to them, particularly in light of the recent decision of the CJEU in this regard[14] and to require the Secretary of State to make relevant regulations rather than having the liberty to do so.

---

[11] https://www.handleygill.co.uk/handley-gill-blog/copyright-artificial-intelligence-ai-consultation-response-web-scraping-data-mining

[12] https://www.handleygill.co.uk/handley-gill-blog/practical-magic-use-deploy-ai-safely-responsibly-ethically

[13] https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/11/ico-intervention-into-ai-recruitment-tools-leads-to-better-data-protecfion-for-job-seekers/

[14] https://www.handleygill.co.uk/handley-gill-blog/automated-decision-making-transparency-meaningful-information

24. We are concerned that proposals to permit the re-use of personal data for the purposes of scientific research, which will include the commercial training, validation and testing of AI models, without suitable transparency requirements are prejudicial to data subjects who ought to be provided with the opportunity to opt out, particularly having provided data in circumstances where this re-use could not have been reasonably envisaged.

Cyber Security

25. We note that efforts were made during the passage of the Bill through the House of Lords to introduce amendments to the Computer Misuse Act 1990 to permit third parties to conduct vulnerability scanning, other penetration testing activities and even wider conduct and access without the consent of network, system and device owners. We note that the proposals do not suggest that there should be any obligation to maintain records, to notify the owner of any vulnerabilities identified, standards of conduct or minimum qualification requirements, obligations in relation to any data accessed and/or downloaded etc.

26. We strongly advocate for effective measures to enhance the cyber resilience of UK plc and were successful in persuading the Institute of Directors to reflect risk management, including cyber risk, and business resilience as essential tenets of responsible business in their voluntary Code of Condict for Directors[15]. We will be making other proposals to improve the UK's cyber security and resilience in our response to the government's consultation on proposals to restrict the making of ransomware payments.

27. Nevertheless, notwithstanding the significant lobbying efforts of parts of the cyber security industry, we strongly object to these proposals[16] and would caution against efforts to introduce such measures.

Other Recommendations

28. In addition to the matters set out above, we would invite the Committee to consider the following:
    a. The ability to prosecute data protection offences should not be limited to the Information Commissioner or with the consent of the Director of Public Prosecutions by introducing a new provision to amend section 197 Data Protection Act 2018[17], which would support law enforcement when

[15] https://www.handleygill.co.uk/handley-gill-blog/directors-duties-institute-of-directors-iod-code-of-conduct-for-directors-responsible-business
[16] https://www.handleygill.co.uk/handley-gill-blog/whats-missing-computer-misuse-act-1990-consultation
[17] https://www.legislation.gov.uk/ukpga/2018/12/section/197

prosecuting these and related matters such as under the Computer Misuse Act 1990;

b. A time period for controllers to provide a substantive response to data subject complaints should be established, to provide a backstop to the requirement to respond without undue delay by amending clause 103(2) Data (Use and Access) Bill;
c. The obligation under section 81, Part 3 of the Data Protection Act 2018[18] that requires controllers processing personal data for the law enforcement purposes to monitor and report infringements of the Act should be extended to all data controllers, who should also be required to maintain records of infringements of the data protection legislation, similarly to how they would be required to record data breaches; and,
d. Article 35(9) UK GDPR[19], which indicates that, *"where appropriate"*, when conducting a data protection impact assessment (which is required when processing is likely to result in a high risk) data controllers should seek the views of data subjects or their representatives should be made mandatory and expanded to permit the appointment of a 'data steward', being an independent third party with appropriate knowledge, skills and experience to represent the interests of data subjects and make recommendations.

[18] https://www.legislation.gov.uk/ukpga/2018/12/section/81
[19] https://www.handleygill.co.uk/uk-gdpr/#ARTICLE35

About Handley Gill Limited

At Handley Gill Limited, we combine cost-effective, pragmatic and robust advice with the in-depth technical knowledge and expertise necessary to provide quality data protection, responsible artificial intelligence (AI), online trust and safety, content moderation and reputation management, information access, human rights, ESG, GRC and wider legal and regulatory advice, compliance and assurance services to our clients.

We are committed to supporting you to get the job done, right.

Our consultants have experience across the public and private sectors, working in-house as well as in professional services organisations, spanning a number of industries including:

- regulated industries, such as law firms and other legal professionals, financial institutions and other financial services providers, insurers and insurance intermediaries, including fintech and regtech providers;
- retail, branding, advertising & marketing;
- technology start ups;
- content providers, including publishers, broadcasters, social media platforms and online and editorial content creators;
- political parties and lobbying groups;
- law enforcement entities;
- charitable organisations;
- employment agencies;
- the public sector;
- sport and fitness; and,
- health care.

We work with organisations of all sizes, on projects from getting the basics of data protection law right for start ups, to advising on some of the most contentious emerging technology issues, which require a holistic approach drawing on data protection, human rights and equalities legislation and emerging AI best practice.

While the identity of the majority of our clients and the nature of our work on their behalf is confidential, it is a matter of public record that we have recently advised Hampshire and Isle of Wight Constabulary on its live facial recognition pilot, trialling the adoption and deployment of artificial intelligence (AI) and biometric technologies in law enforcement, and that we regularly advise the City of London Corporation in its capacity as Police Authority and the Commissioner of the City of London Police.

Our consultants have obtained relevant qualifications including the International Association of Privacy Professionals Certified Information Privacy Professional/Europe (CIPP/E) certification, and the accredited OU Introduction to Cyber Security and University of Michigan Data Science Ethics course, so you can be assured of our expertise. Our

consultants have also achieved OneTrust Certified Privacy Professional status, and we can work with your organisation using OneTrust, as well as other privacy management platforms, or work with you to develop your own framework to demonstrate compliance with data protection and wider ethical, environmental, social and governance (ESG) risk.

Our consultants have expertise in developing policy and legislation, particularly in the data protection and media, content and online safety spheres, and have developed position papers and lobbying documents and engaged in lobbying on behalf of clients and in the wider interests of industry. We work with think tanks and other organisations, as well as independently, to develop thought leadership and position papers in relation to data protection and content issues, online safety and responsible AI and associated regulatory matters and frequently respond to public consultations.

While our consultants are legally trained and qualified and have significant experience in providing legal services, our consultants do not act as solicitors or barristers and they are not subject to the rules regulating practising solicitors or barristers. We do not offer services in reserved legal activities i.e. the exercise of a right of audience (this does not restrict advocacy and representation before the First-Tier Tribunal (Information Rights)), the conduct of litigation, reserved instrument activities, probate activities, notarial activities, and the administration of oaths; nor do we provide immigration advice and services. We nevertheless aim to provide exceptional service, at a reasonable cost and significantly less than a law firm would charge for less experienced staff.

Handley Gill is the trading name of Handley Gill Limited. References to “Handley Gill”, “We” or “Us” are references to Handley Gill Limited.

To enquire about our services and how we can support you, please contact us:

Handley Gill Limited
International House
64 Nile Street
London
N1 7SR

www.handleygill.com
info@handleygill.com

020 7515 4694
0743 222 1894 (24-hour incident response hotline)

Handley Gill Limited is a limited company incorporated in England with registered number 12608561 and registered address at International House, 64 Nile Street, London N1 7SR, United Kingdom.

Handley Gill Limited is registered on the register administered by the Information Commissioner's Office under the Data Protection Act 2018 with registration number ZA767642.

Handley Gill Limited is VAT registered: 375 4884 49.