Written evidence submitted by UK Finance. To the DATA PROTECTION AND DIGITAL INFORMATION (No. 2) Public Bill Committee, (DPDIB26).

UK Finance is the collective voice for the banking and finance industry.

Representing more than 300 firms across the industry, we act to enhance competitiveness, support customers and facilitate innovation.

UK Finance supports the goals of the Data Protection and Digital Information Bill (the Bill). We support strong individual data rights and effective data governance but constructed in such a way as to enable beneficial and responsible innovation. We support the Bill's goals of achieving this balance.

We particularly support the following elements:

- In relation to the data protection law reforms in Parts One and Four:
    - Clarification of key concepts such as 'personal data' and 'compatibility', as well as the in which the exemptions from data subject access rights apply.
    - Added certainty of the legal basis for the detection and prevention of crime.
    - Clarifying the rules for automated decision-making (ADM).
    - Adding flexibility to the cookie rules in appropriate situations.
- The creation of a framework for UK digital identities in Part Two.
- The creation of a framework for data sharing schemes (Smart Data) in Part Three.

We also support the goal of maintaining adequacy.

We do, however, have several suggestions for amendments to add clarity, avoid unintended consequences and achieve effective implementation, notably by strengthening consultation requirements before the use of Statutory Instruments. Our proposals cover (in clause order):

- Adding safeguards to provisions facilitating disclosure of personal data to public authorities by firms.
- Clarifying that data controllers how the exemptions for data subject access requests (DSARs) apply where a third-party acts for the individual.
- Guidance and public consultation on the implementation of the new rules for ADM.
- Resolving technical uncertainties around record keeping rules.
- Information Commissioner's Office (ICO) independence and regulatory certainty.
- Effective implementation of Smart Data schemes.
- Clarifying that communications sent for regulatory purposes are not 'direct marketing'.
- Technical fixes to the electronic marketing rules to resolve challenges for businesses operating as groups and remove unwarranted exclusions from new cookie rules.

We have annexed a more detailed analysis of these matters.

Annex – detailed analysis of positions and proposals for the Bill

Data protection reforms – Part One of the Bill

Overarching considerations and 'adequacy'

1. Although it is constructive to refine UK data protection rules where there is a clear benefit in doing so, we should avoid diverging so far from EU rules that our adequacy decision is put at risk. Losing 'adequacy' would significantly impede the flow of data from the EU to the UK and raise costs to businesses.
2. On the whole, we think that the Bill currently strikes an appropriate balance in this regard.
3. However, we do note that there may be concerns with certain specific provisions, notably the independence of the ICO, as we outline below. Potential new amendments should also be carefully scrutinised for potential adequacy impacts.
4. Furthermore, a determination of adequacy by the European Commission necessarily includes a subjective element. As such, it is important to consider the perceptions of key EU stakeholders. We understand that HMG officials have been discussing the Bill and adequacy with European Commission officials and this should continue.

Clauses 1 and 6 – Helpful clarifications

5. *We support moves to add clarity to key provisions. These include key concepts such as* 'compatibility' and the re-use of personal data, as well as the definition of 'personal data' itself. Greater certainty on these concepts is helpful for business innovation.
6. Nonetheless, ICO *guidance* will also be necessary to address uncertainties around such issues as data re-use for model training.

Clause 5 – The prevention and detection of crime

7. The financial sector has a central role to play in detecting and preventing money laundering, fraud, terrorist financing and other crimes but there has been uncertainty in the past as to the legal basis for these activities. This is in large part because Recital 47 of the General Data Protection Regulation (GDPR) seemed to treat fraud prevention as being more important than other types of crime prevention.
    - *We are therefore supportive of the clarification in paragraph 5 of Annex 1 that data processing to detect and prevent criminal acts can have a 'legitimate interests' legal basis.*
8. This new provision complements the Economic Crime and Corporate Transparency Bill (ECCT Bill) to facilitate information sharing as a means of tackling economic crime. The DPDI Bill covers data protection issues, while the ECCT Bill addresses civil liability challenges.
9. We highlight, though, that that there needs to be some kind of safeguard to ensure that firms consider proportionality and mitigate risks to individuals, and we note that the Bill removes the 'balancing of interests' control for data processing that comes under Annex 1. The risk assessment process in clause 17 can serve this role, though industry will need supplemental ICO guidance.

Contingency option

10. We note that there has been recent concern about crime prevention measures and data protection impacts, notably *this letter* by the European Data Protection Board, which raises doubts about new EU measures to facilitate anti-money laundering data

sharing. *If a view were to emerge* that paragraph 5 of Annex 1 under the Bill is not appropriate, for example due to emerging adequacy concerns, a fallback option is available.

- ***As a fallback alternative to Annex 1, paragraph 5****, we recommend – if required – adding 'the detection, prevention or investigation of crime' to UK GDPR Article 6(9) via Bill clause 5.*

11. A clarification in Article 6(9) would still help resolve the uncertainty under the current GDPR, despite not going as far as the current Annex 1 provision.

<u>Clause 5 – Acquisition of personal data by public authorities</u>

12. *We wish to raise concerns about Annex 1, paragraph 1* (and the corresponding paragraph 1 in Annex 2).
13. This provision allows a controller to make a disclosure to a public sector body that asserts the data is needed in the public interest, without any need for due diligence by the disclosing controller. We understand this provision was motivated by concerns at the challenges faced by government when attempting to access personal data needed to monitor and manage the Covid-19 pandemic. We sympathise with this but are concerned that the Bill provides a *blanket* permission for controllers to make disclosures on receipt of *any* kind of request for information from a public body.
14. As an industry we already encounter situations where public authorities seek large data sets that we consider disproportionate and beyond what is needed to protect the public interest. In one case millions of 'random records' were requested to be used in large-scale profiling of individuals to identify signs of wrongdoing, to then pursue them in the courts or apply penalties. This is in our view a fishing exercise but was nonetheless judged to be proportionate and in the public interest by the relevant authority.
15. These provisions in the Bill risk encouraging such practices by undermining the procedural safeguards that generally govern public bodies' acquisition of personal data from private organisations, such as the need to obtain judicial approval of a production order. Instead, a public authority could simply take a view internally that the data is needed in the public interest, and then seek to convince the private sector organisation to supply it, for example by offering to buy the data. Alternatively, the public authority could pressure the firm to provide the data, which might be difficult to resist in the absence of a legal requirement for due diligence on the firm, despite any proportionality concerns. This data sharing would occur without any external oversight.
    - ***We suggest narrowing these provisions*** *to apply only in specific circumstances. For example, the Bill could clarify that:*
        i. *they only apply in an emergency, and / or*
        ii. *the data acquired can be used in broad studies but not to take decisions in relation to specific individuals.*
    - *Alternatively – or in addition –* ***safeguards could be added****. These could include:*
        i. *A requirement on the public authority to publish its data protection impact assessment, or at least provide it to the firm being asked to make the disclosure.*
        ii. *The ICO could be called on to produce a statutory code for public authorities in relation to 'public interest' data acquisition, similar to the provisions in sections 121-124 of the Data Protection Act (DPA).*
        iii. *A requirement on the public authority to notify the ICO of such data requests could be added to the Bill.*

Clause 7 – Data Subject Access Requests (DSARs)

16. The Bill changes the exemption for data subject rights by moving to a 'vexatious or excessive' test. This change, combined with the considerations expanding on that test in new Article 12A(4) helpfully provide greater clarity to firms.
17. However, by far the largest source of vexatious and excessive data subject access requests in financial services is certain claims management companies (CMCs) and law firms. For example, our members have experienced third parties lodging 1000s of DSARs that do not pertain to genuine customers, threatening to lodge 1000s of DSARs if a firm does not provide certain information, or acquiring authorisation from customers to lodge a DSAR without making it clear to the customer that this would result in the CMC acquiring all of the individual's data. These kinds of abuses of the DSAR process put consumer data at risk and take firm resources away from efforts to comply with legitimate customer inquiries.
    - ***The Bill should clarify in new Article 12A*** *the, where an information right is being executed by a third party on behalf of an individual, data controllers can consider the conduct of the third party, not just that of the individual, when determining whether the request is vexatious or excessive. This is stated in the Bill's Explanatory Note but should be made on the face of the Bill.*
    - *We are happy to support ICO work on supplemental guidance.*

Clause 11 – Revision of the ADM regime

18. We support the repeal of the DPA's prescriptive 'one size fits all' safeguards for ADM, and their replacement with principles-based requirements and a power for Statutory Instruments (SIs) to finesse the rules when needed. This flexibility will allow for greater innovation by enabling safeguards to be set that account for new or unanticipated use cases.
19. However, it is still uncertain what the scope of a 'significant decision' is. For example, is the execution of transactions in scope? If so, this would need careful consideration to ensure that payments are not interrupted unnecessarily and that measures protecting customers from fraud are not undermined.
    - *There needs to be close cooperation between the ICO, HMG and industry ahead of Bill implementation to ensure that the regime provides effective protections to individuals, and that SIs address any use cases that might not fit cleanly within the statutory framework. A reasonable implementation timeline will also be needed to ensure that all pieces of the puzzle are in place in time for firms to comply effectively.*
20. We also note concerns about the extent of the SI powers in this clause. The SI powers are important to future-proof the regime and allow for the emergence of new use cases. However, adding a clearer consultation requirement to the Bill would help ensure the SIs are well designed and do not give rise to unintended consequences.
    - ***Clause 44 (New Regulation 91A) should be amended*** *to require a full 12-week public consultation before making UK GDPR regulations.*

Clauses 12 to 18 – The accountability framework

21. Robust governance and accountability requirements are necessary but should avoid excessive prescription. Clauses 12 to 18 of the Bill strike a reasonable balance, leaving core GDPR structures in place, while increasing flexibility for firms to set up processes aligned to their own business, and allowing the ICO to provide detail for different circumstances. This is supportive of the risk-based approach.
    - *We support the overall approach taken in the Bill.*

22. New Article 30A(1)(a) states that the record keeping requirements apply to controllers that conduct high risk processing. It is unclear whether the intention is for controllers to only maintain the relevant records of their high-risk processing, or whether a controller that does some high-risk processing must also maintain records of its lower risk processing.
    - ***New Article 30A(1)(a) should be amended*** *to clarify its scope.*
23. We are unsure of the intention behind Article 30A(2)(a). It might simply require keeping a record of which country certain data is stored in. However, the provision seems to require more than this, given the text in parentheses refers to "*including*" information about data stored outside of the UK. If instead the intention is that a record of the *system* in which the data is kept, or some kind of information about geographical region, this would be more prescriptive than the current GDPR requirement. It is unclear why this level of granular detail would be required – particularly given that systems can change – but there is no explanation in the Explanatory Note, so the intention is unclear.
    - **New Article 30A(2)(a) should be clarified:**
        i. *If the intent is only for the country to be recorded, this should be made explicit.*
        ii. *If the intent is for the system to be recorded, it should be clarified that only the category or type of system needs to be recorded.*

Clauses 27 to 33 – Updates to the Information Commissioner's Office

24. With regards to the changes to the ICO, we largely agree with the provisions in the Bill. It is important that the ICO have a modern and effective governance structure with democratic accountability, a clear hierarchy of objectives and robust justification for significant regulatory interventions.
25. However, we do wish to highlight clause 31, which requires the ICO to have any codes of conduct approved by the Secretary of State. We note that this goes beyond the existing framework under the DPA, which allows Parliament to reject a code of conduct. We are concerned at the risk posed to regulatory independence and regulatory certainty, the risk of inadvertent regulatory capture, and the potential impact on public trust and our international standing.
26. The existing provision might also weaken the UK's adequacy status, given the requirement to have an independent regulator under GDPR.
    - *We encourage the Committee to* ***consider whether this provision in the Bill should be removed, or softened****, for example by:*
        i. *requiring the Secretary of State to consult affected stakeholders before overriding the ICO draft code, or*
        ii. *in the place of an approval power, allowing the Secretary of State to provide an opinion to the ICO in relation to a code, which the ICO must take account of when finalising the text.*

Digital identity – Part Two of the Bill

27. We support the Bill's provisions on digital identity. The development of a market in reusable digital identity – available to consumers who choose to opt in – will enable a variety of customer benefits, while make identity proofing easier and more secure.
28. We support the introduction of regulation of digital identity and believe it will build trust.
29. The disclosure by public authorities of personal information to trusted digital identity providers will help ensure digital identities can be created and trusted. It will be important that government bodies follow up the creation of a legal gateway by putting in place the technology to allow the data sharing in practice.

30. The government is also developing its own digital identity service – One Login – interoperability with private schemes will be needed, as will effective co-ordination between public and private approaches, since some transactions will involve parties from both (for example, home buying).
31. It will be important too for government to support the development of trust in digital identity by citizens and encourage their use. Acceptance and adoption of digital identity will be a key challenge. The public will need to understand the safeguards and be reassured; the passage of the Bill will be an opportunity to do this.
32. It is important we begin to understand that digital identity will be an essential utility in the future, as digital transactions become an increasing part of daily life and we introduce new ways of transacting digitally for example through a central bank digital currency.

'Smart Data' – Part Three of the Bill

33. Open banking is a live example of Smart Data. We support the Bill allowing the introduction of Smart Data into other sectors.
34. We agree with the underlying rationale: through the safe sharing of their data to authorized third parties, customers can benefit from new products and services. In the future, the benefit could derive from customers mobilizing a more holistic view of their data to inform (with advisers) their life choices.

Implementation considerations

35. The Bill addresses the asymmetry in the market, where bank account data is available to authorized providers but banks themselves cannot access data from other accounts their customers hold. It is important that further asymmetries are not created between sectors: should Open Banking data become available to other sectors, there should be consideration given towards reciprocity: i.e. banks being able to access data held by firms in other sectors when those firms have accessed Open Banking data (subject of course to obtaining consumer consent).
36. Any new Smart Data standards should strive to be interoperable to lower barriers to entry and implementation costs, and broaden potential adoption. This should be reviewed as part of any impact assessment process. These considerations are particularly relevant to use cases that involve affordability assessments. For instance, an energy Direct Debit does not necessarily reflect actual energy use or expenditure, meaning that access to more complete customer data from the energy company would allow for more precise assessments.
37. The Bill provides the power to mandate participation in Smart Data schemes where voluntary approaches do not emerge. These powers need appropriate safeguards to ensure:
    a. customer benefit
    b. scheme sustainability
    c. minimal unintended consequences
    d. proportionate costs
38. Not all products and services within a sector should necessarily fall in scope of a Smart Data scheme. If clear merits are not found for including a given product or service, the default position should be that the product or service is excluded from the Smart Data Scheme.
39. Banking has led the way on Smart Data. There are lessons that other sectors can learn from Open Banking, including:
    a. Integrating data protection principles into policy discussions from inception, to facilitate data sharing and benefit consumers.

b. The need for a consumer education initiative to build consumer understanding and trust.
c. Ensuring any levies are proportionate, equitable and fair, to ensure all market participants are adequately incentivised to develop and introduce new data sharing schemes in an expedient and cost-effective way. Open Banking demonstrates the importance of incorporating incentives to industry into mandatory schemes.
d. The careful consideration of how to tackle issues surrounding fraud and economic crime. This includes considering liability, as well as roles and responsibilities across value chains, especially given these could grow in complexity as markets develop.

Implications for the Bill

40. The Bill creates significant new powers. As such there needs to be a clearer process to follow when exercising these powers, to ensure that the complexities of each scheme are well considered.
    - ***We recommend amending clause 74(5)*** *so that, before implementing Statutory Instruments:*
        i. *an Impact Assessment is required (exemption rules not applying), and*
        ii. *a full 'call for evidence' consultation of at least 12 weeks is required.*
    - ***We also recommend strengthening the post implementation review requirement*** *by adding to paragraph 3 of clause 75; "This report must be subject to full scrutiny by the independent verification body" (as defined by the Small Business, Enterprise and Employment Act 2015, –currently the Regulatory Policy Committee). The HMG Evaluation Taskforce can also assist with this.*

Privacy and electronic communications – within Part Four of the Bill

Clause 79 – Cookies and other online tracking

41. *We support the clarifications made to PECR that a range of important uses of cookies and similar technologies can be used by default*. For our members, these include in particular their use to maintain device security, authenticate users and protect customers from fraud.
42. *We also support the framework set up enabling the Secretary of State to facilitate use of technologies like internet browsers to express consent to tracking technologies or to object to their use.* This will need to be done carefully and with further public consultation, however, in order to ensure the regime functions as intended and does not lead to unforeseen consequences, such as a reduction of consumer control or ambiguity over the liability of the browser provider versus the website provider.

Technical amendments

43. However, some of the provisions in Clause 79 intended to allow low-intrusion and functional cookies to be used without user consent are drafted too narrowly and will exclude low-intrusion uses that do not quite fit within the specific terminology used in the Bill. In particular:
    a. The drafting in new Regulation 6(2A) only allows for statistical cookies to be used to make improvements to the 'information society service' or 'website'. It is unclear

why statistical data could not also be used to make improvements to other products and services provided by the website operator, notably financial products and services. This is no more intrusive for the consumer.

- ***New regulation 6(2A)(a) and (b)(i) should be amended to clarify*** *that the statistical data can be used to make improvements to any product or service provided by the person operating the website or information society service.*
- *Given that it is common for a website to be provided by one entity in a group, with financial products provided by a related company in the same group – as outlined above –* ***a reference to 'related companies' or similar should be added to Regulation 6(2A)(b) and (c)).***

b. The drafting in new Regulation 6(2A) does not extend to the use of 'email pixels'. Provided these are only used to gather *statistical* data for product and service improvement purposes – such as better ensuring that communications meet regulatory obligations – email pixels should be brought within scope.

- ***New regulation 6(2A)(a) should be amended*** *to also include situations where the person stores / accesses data in a user's device via an email.*

Clause 81 – Direct marketing and regulatory communications

44. The PECR regulations rightly impose rules to protect consumers from undesirable electronic marketing.
45. However, the role of *regulatory communications* should be made clear. In financial services, as in other regulated sectors, firms are increasingly expected by regulators to proactively advise existing customers when an alternative product may provide them with greater value. For example, a customer might be scheduled to soon switch automatically onto a standard variable rate mortgage, or indeed currently hold such a mortgage, when the customer would qualify for a lower rate product.
46. Under the new FCA Consumer Duty, firms are required to enable and support customers to achieve their financial objectives and avoid foreseeable harm. They are also required to give effective support to customers and to meet higher standards in customer communications. As part of this, the FCA has indicated that firms should be prompting their customers to consider whether their products continue to meet their needs and objectives. Such communications are likely to need to include information about alternative products.
47. Unfortunately, the sending of communications about products for regulatory purposes is not anticipated by the 'direct marketing' definition in data protection legislation. As such, under the latest ICO guidance it is highly likely that such communications would be considered 'direct marketing' under PECR.
48. This leaves firms potentially unable to send the explanations expected by the sectoral regulator to customers who have not consented to marketing, impeding efforts to prevent consumer detriment and provide fair value to customers.

- ***We recommend amending clause 81*** *of the Bill to clarify in regulation 2(1) that communications sent in order to satisfy the rules or guidance of a regulatory authority are not 'direct marketing' for the purposes of PECR.*

Clause 82 – The 'soft opt-in' rule and groups of entities

49. The ability of firms that operate as a group to do direct marketing to their existing customers should be clarified in PECR regulation 22.
50. Under the current law, provided certain 'unsubscribe' options are given, firms are allowed to send direct marketing to their existing customers. This is sometimes known as the 'soft opt-in'.

51. However, in the financial sector as in many sectors, firms typically operate as a group of related companies. This is due to regulatory obligations to separate certain functions, past mergers or acquisitions, and general business management.
52. Regulation 22(3) currently allows firms to rely on the 'soft opt-in' only where the "person" sending the direct marketing communication obtained the contact details of the recipient during a sale or negotiation. Furthermore, the marketing must be in respect of "that person's similar products and services only". The word 'person' would generally be taken to refer to a single legal entity. This implies that where an entity has a customer, it cannot use the soft opt-in to send marketing for products issued by other group entities, even if these are of similar nature and under the same brand.
53. At the end of 2022, the ICO updated its PECR guidance to make clear that firms *cannot send* direct marketing to customers of other legal entities within the same group of related companies.
54. There therefore exists an arbitrary commercial disadvantage for firms that are structured as a group of entities and – more importantly – risks customer confusion, as consumers are unlikely to know which legal entity technically provides which products. They will likely be confused as to why they are asked to consent to some marketing materials and not others from the same firm, potentially leading to complaints.
55. We recognise concern that consumers of highly diverse business groups could find themselves receiving marketing in relation to products and services with no connection to their existing relationship to the firm. However, regulation 22 already limits use of the soft opt-in to where the marketing is "in respect of…similar products and services only". We consider this to already be an effective safeguard.
    - ***We recommend amending regulation 22*** *to clarify that business groups can also make use of the 'soft opt-in', for example by adding a reference to 'related companies'. We would be happy to assist with drafting suggestions.*

May 2023.