Written evidence submitted by the Open Data Institute (DUAB09)

Written Evidence to the Public Bill Committee on the Data (Use and Access) Bill

The Open Data Institute (ODI) welcomes the Data (Use and Access) Bill as a crucial step towards unlocking the benefits of data for the UK. We commend the Bill's aims to modernise data protection, promote innovation through smart data, and enhance digital verification. This submission focuses on key areas where we believe amendments and clarifications are necessary to ensure the Bill achieves its full potential and avoids unintended consequences. Our recommendations centre on:

- Establishing robust smart data standards and a central authority.
- Implementing a user-centric, automated privacy framework.
- Streamlining subject access requests (SARs) through open API standards.
- Ensuring international interoperability of digital verification services (DVS).
- Leveraging decentralised data technologies like solid.
- Financial support for new independent bodies.
- Protection of sensitive data.

About the Open Data Institute

The ODI is a non-profit organisation dedicated to building an open, trustworthy data ecosystem where people can make better decisions using data and manage any harmful impacts. We are a not-for-profit institute and a company limited by guarantee.

Key issues and recommendations

We organise our recommendations according to the relevant parts of the Bill, where possible, to make it easy for the committee to follow.

Access to customer and business data (smart data)

- **Issue:** The Bill's success in enabling smart data schemes hinges on interoperability and clear standards. Without these, we risk creating new data silos, hindering innovation.
- **Recommendations:**
    - **Establish a central authority (new clause/amendment):** We strongly recommend the Bill be amended to mandate the creation of a central authority responsible for developing and managing cross-sector smart data standards. This body should:
        - Ensure interoperability between different smart data schemes.
        - Oversee the development of open APIs for data access.

        - Engage with industry, civil society, and international standards bodies.
    - **Prioritise AI-ready data standards (new clause/amendment):** The Bill should mandate the development and use of AI-ready, contextual data standards (e.g., enterprise knowledge graphs) to maximise data usability and support responsible AI development.
    - **International alignment (amendment to relevant clauses):** Any "interface bodies" established under the Bill should be explicitly required to align standards with international interoperability frameworks (e.g., those developed by W3C, ISO, IEEE) to facilitate cross-border data portability.
    - **Early-stage funding (amendment to section 13 or new clause):** Provide early-stage funding for independent implementation bodies (similar to the open banking model) to ensure impartial standards development and build public trust. This funding should transition to industry-based funding over time.
    - **B2C smart data standards:** In the Gamma trust framework for DVS there is now a holder where citizens can store data safely and securely, we recommend that it be possible for citizens to pull data into their holder wallet to reshare at their discretion.
        - Citizens should be able to use the holder in the gamma framework to pull in data to reshare at their discretion.

Changes to the UK's data protection regime (GDPR)

- **Issue:** Existing GDPR consent mechanisms are often ineffective and lead to user fatigue (e.g., cookie pop-ups). The Bill presents an opportunity to create a more user-centric and effective approach.
- **Recommendations:**
    - **Mandate an automated privacy framework (new clause/amendment):** We recommend a new clause tasking the Secretary of State, in consultation with relevant standards bodies (W3C, ISO, IEEE) to develop an automated privacy framework. This framework should:
        - Enable organisations to digitally describe their data processing activities in a standardised, machine-readable format.
        - Empower users to declare privacy preferences ("privacy signals") that are usable across different devices and platforms.
        - Explicitly permit automation in communicating consent decisions, respecting user intent.
    - **Strengthen consent requirements (amendments to relevant GDPR provisions within the Bill):** Amend the Bill's modifications to GDPR consent requirements to explicitly support technological tools that allow individuals to

communicate their privacy preferences automatically, moving beyond reliance on website-based pop-ups.

- **Dynamic consent mechanisms (new clause/amendment):** Introduce provisions requiring the implementation of dynamic privacy mechanisms that allow users to give, modify, or withdraw consent over time easily.

Subject access requests (SARs)

- **Issue:** The process of exercising the right to data access (SARs) is often cumbersome and inconsistent.
- **Recommendations:**
  - **Clear guidelines for "reasonable and proportionate search" (guidance/secondary legislation):** The government should issue clear guidelines (either through guidance or secondary legislation) defining what constitutes a "reasonable and proportionate search" for personal data in response to a SAR. This is crucial to prevent organisations from abusing this provision to avoid providing meaningful access.
  - **Mandate open API standards for SARs (new clause/amendment):** The Bill should mandate the development and implementation of open API standards for handling SARs. This will ensure consistency, efficiency, and machine-readability of responses.
  - **Consistent and quality responses:** Advocate for measures to ensure consistency and quality of SAR responses that can't be gamed to provide obfuscatory responses.

Digital verification services (DVS)

- **Issue:** The DVS trust framework must be robust, trustworthy, competitive, and transparent.
- **Recommendations:**
  - **Consultative approach (amendment):** the UK government should continue with an open and transparent consultative design and rollout of DVS to build and retain public trust in their use.
  - **Prevent the "cookie consent problem":** (amendment) build consent and data privacy mechanisms into the Bill to allow data sharing within credentialed systems to prevent the need for repeated consent requests from the user.
  - **International interoperability:** The Bill should explicitly require that the DVS trust framework aligns with international standards and verification systems. This could include:
    - Mandatory consultation with international standards bodies (W3C, ISO, IEEE) during framework development

        - Provisions for cross-border recognition of digital credentials
        - Mechanisms to ensure compatibility with major international digital identity systems
        - Requirements for regular review and updating to maintain alignment with evolving global standards
        - Without proper international alignment, the UK risks creating an isolated verification system that limits international digital trade and creates unnecessary barriers for businesses and individuals operating across borders.

Financial assistance

- **Issue:** Section 13 financial assistance for compliance.
- **Recommendations:**
    - **Independent oversight (amendment to secondary legislation):** Establish independent bodies to oversee the implementation of smart data schemes, funded in the initial stages, to ensure impartial operation and foster public confidence. Consider a structure akin to the open banking model, commencing with a task force followed by an implementation entity.

Sensitive data

- **Issue:** Processing of special categories of personal data.
- **Recommendation:**
    - **Define robust safeguards for genomic and other sensitive data categories (new clause/amendment).** By clearly defining protections for sensitive data categories, the UK can set a high standard in data ethics and privacy. This would align with international frameworks, ensuring compliance with global data protection norms while supporting research initiatives that depend on securely managed data.

Potential of Solid

The ODI recommends that the committee explore the potential of Solid (social linked data), whic is an open standard for decentralised data management, as a technology that aligns with the Bill's objectives. Solid:

- Empowers individuals to control their data in personal online data stores (pods).
- Supports digital identity verification through the management of verified attributes.
- Enables granular control over data sharing, aligning with the Bill's vision for smart data schemes.

- Promotes interoperability and secure data sharing through its open standard approach.

We believe exploring and potentially leveraging Solid could provide a robust technical foundation for the Bill.

Questions for the Committee to take into consideration

To ensure the Bill's effectiveness and address key concerns, we urge the committee to put the following questions to the Secretary of State and relevant ministers:

- **Regarding the automated privacy framework:**
    - How will the Bill ensure that the automated privacy framework effectively balances user control with the need for efficient data processing, particularly in light of the Bill's expanded provisions for lawful processing?
    - What specific mechanisms will be implemented to ensure that organisations respect privacy signals communicated through the automated privacy framework?
    - How will the framework specifically address and prevent the use of deceptive patterns in cookie consent pop-ups and online dialogues?
- **Regarding subject access requests:**
    - What specific criteria will be used to determine whether a search for personal data is considered "reasonable and proportionate" under the new provisions?
    - What steps will the Government take to ensure the timely development and implementation of open API standards for SARs, and how will this be resourced?
    - What measures will be implemented to guarantee the consistency and quality of responses to SARs, particularly concerning the provision of data in machine-readable formats?
- **Regarding the DVS trust framework:**
    - How will the DVS trust framework be developed to ensure alignment with international standards, and what specific consultations will be undertaken with organisations such as W3C, IEEE, and ISO?
    - How will the governance of the DVS register be structured to allow for adaptation to future needs, considering the potential limitations imposed by the detailed provisions in articles 32-44?
    - What measures will the Government take to mitigate the risk of creating a fragmented digital identity landscape if international interoperability is not sufficiently prioritised?

- What specific provisions will be included in the Bill to ensure that the international interoperability of the DVS framework does not compromise UK data protection standards or citizen privacy?
- How will the government balance the need for international compatibility with maintaining UK sovereignty over verification standards and processes?

The Data (Use and Access) Bill represents a significant opportunity to create a modern, data-enabled UK. The Open Data Institute believes that by incorporating the recommendations outlined above, particularly regarding robust standards, user-centric privacy frameworks, international interoperability, and individual empowerment, parliament can ensure that this Bill delivers on its promise to unlock the benefits of data responsibly and effectively. This will foster a data ecosystem that promotes innovation, trust, and economic growth for the UK. The ODI stands ready to provide further clarification or detail to the committee as needed.

February 2025