Department for
Science, Innovation
& Technology

DATA BROKERS CALL FOR VIEWS QUESTIONS

PART 1 QUESTIONS: DEFINITION AND SERVICES OF DATA BROKERS

QUESTION 1: Does your organisation take part in any data broking activities? [Y/N]

QUESTION 2: What types of data does your organisation primarily handle and what are the characteristics of this data? For example, is the data handled: on UK or non-UK businesses, infrastructure or data subjects, identifiable, anonymised, pseudonymised, etc.

QUESTION 3: From where, and using what methods, does your organisation source its data?

QUESTION 4: Does your organisation keep a record of data sources, including original sources? If no, please explain why.

QUESTION 5: What are the primary data broking services and/or data products offered by your organisation? For example, raw data sets, aggregated data sets, bespoke insights, etc.

QUESTION 6: Do you agree with the Government's understanding of data broking as set out in Part 1 and that the term 'data broker' is best used to describe organisations that conduct this type of activity? If you disagree, what term(s) would you use to describe organisations that conduct data broking activities?

QUESTION 7: Do you consider your organisation to be part of the data broking industry? Please describe your organisation's role in the data ecosystem and the reasoning for your answer.

QUESTION 8: What social and economic impact do you consider the data broker market to have in the UK? Please consider both positive and negative effects.

PART 2 QUESTIONS: NATIONAL SECURITY RISKS

QUESTION 9: To what extent are you/is your organisation aware of hostile exploitation of UK data and the extent to which this contributes to the risks outlined in Part 2? [Multi-select list: Very aware, Aware, Not very aware, Not at all]

QUESTION 10: (if answered aware) Please describe your understanding of how hostile exploitation of UK data can harm the UK's national security?

QUESTION 11: To what extent are you concerned about the collection and use of UK data by organisations conducting data broking? [Multi-select list: Very concerned, Concerned, Not very concerned, Not at all concerned]

QUESTION 12: (if answered concerned) What are the most concerning threats you or your organisation is observing from access to UK data on the open market and how do you see these evolving?

PART 3 QUESTIONS: SECURITY AND REGULATORY FRAMEWORKS

QUESTION 13: Do you consider current legislation and regulations to sufficiently protect UK data from misuse? Please explain the reasoning for your answer.

QUESTION 14: Do you believe there are sufficient standards within the data broking industry to ensure UK data is shared safely?

QUESTION 15: How do you ensure the data your organisation handles is stored securely (for example, via encryption or adhering to certain cyber security frameworks)?

QUESTION 16: In which country or countries is your organisation's data stored? If your organisation stores data in multiple countries, please describe how the stored data is split across each country.

QUESTION 17: Who has access to the data handled by your organisation? Please consider the following in your response:

- Do all directly employed staff have access to all or any of the data held by your organisation?
- Do contractors or third-party providers have access to all or any of the data held by your organisation?
- Do you employ measures to restrict access to the data your organisation holds, for example, access controls or the principle of least privilege?
- If your organisation holds data outside the UK, which of the above actors can access the data stored there? Are these actors also outside the UK?
- If direct access is not given, are any explicit measures in place to restrict access to any of the above actors?

QUESTION 18: Does your organisation use any privacy enhancing technologies such as pseudonymisation or data clean rooms? If yes, please provide details.

QUESTION 19: How do you ensure the data your organisation sells/licenses is transferred securely, including across borders, to adequate and non-adequate jurisdictions? For example, do you send data via secure channels using encryption or password protection and does this differ for international transfers of data?

QUESTION 20: What governance arrangements does your organisation implement to understand and manage data or cyber security risks? Please consider the following in your response:

- Does your organisation complete any checks or screening of staff, contractors, and third-party providers who may have access to the data?
- Does your organisation provide training on data security awareness to staff?
- Does your organisation have a single point of contact at board level who is responsible for the security of the data you hold and sell?
- Does your organisation have a process for conducting reviews or lessons learned following a data security incident. If so, could you describe what that process entails?
- How frequently does your organisation conduct security audits to identify potential threats?
- How does your organisation share information with other data brokers or organisations across the data ecosystem on data security risks, threats and mitigations?

QUESTION 21: Does your organisation conduct any vetting practices before selling, licensing or making available data products or services to potential or existing clients? If yes, please provide a description. If no, please explain why.

QUESTION 22: What, if any, barriers exist in relation to your ability to vet potential or existing customers? For example, cost/resources, etc.

QUESTION 23: Does your organisation ever refuse to sell or licence data products or services to a potential client? If yes, what are the most common reasons for refusal? If no, please explain why.

QUESTION 24: Does your organisation place any limits on the type of data that can be sold? For example, personal data, deanonymised data, pseudonymised data, etc.

QUESTION 25: Does your organisation set any restrictions on how customers can use the data bought from your organisation? For example, the use of contracts or data-sharing agreements that stipulate uses, 'seeding' datasets, or tracking the data to prevent misuse. If yes, how do you ensure compliance? If no, please explain why.

QUESTION 26: Could you describe your pricing structure? For example, do you charge by complexity of datasets or by number of records provided?

QUESTION 27: How does your organisation currently comply or plan to comply with international rules or regulations in relation to data security? For example, the US Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern.

QUESTION 28: Is your organisation a member of an industry body relating to its data broking activities? If yes, please provide details of the industry body/bodies of which you are a member.

PART 4 QUESTIONS: CUSTOMER BASE, CONSUMER AWARENESS AND TRANSPARENCY

QUESTION 29: Who constitutes the primary customer base of your organisation (for example, advertisers, businesses, government entities)?

QUESTION 30: What proportion of your organisation's sales are to UK-based customers vs. overseas customers?

QUESTION 31: Can your organisation provide a geographical breakdown of your customer base? If yes, please provide details. [Multi select list of the 'G20 countries'

and 'other' with multiple choice answer e.g., a) 0% b) 0-25%, c) 25%-50%, d) 50-75%, e) over 75%]

QUESTION 32: Does your organisation have a record which identifies customers you sell to, including individuals, businesses or other organisations, and a record of the ultimate beneficial owners of any businesses you sell to?

QUESTION 33: Is your organisation able to track what data is purchased by or licensed by your customers over the duration of their custom?

QUESTION 34: Does your organisation place a threshold for how much data a customer can purchase on a specific topic, either in one purchase or over the period of their custom? If yes, what thresholds do you have in place and how is your organisation notified if this threshold is triggered? If no, please explain why.

QUESTION 35: Please describe what types/characteristics of data customers most frequently purchase and how you segment these? Please consider the following to guide your response:
- What are the characteristics of this data?
- Do you sell personal data?
- Do you sell individual profiles or group the data?
- Is the data anonymised, etc.?

QUESTION 36: What purposes do customers use this data for?

QUESTION 37: Have you ever been a customer of a data broker? If yes, what product(s) or service(s) did you use and for what purpose?

QUESTION 38: How aware are you of the data broker industry and the role it plays in the data ecosystem? [Multi-select answer: Very aware, Aware, Somewhat aware, Not very aware, Not at all]

QUESTION 39: (If answered aware) What is your view on data brokers and the role they play in the data ecosystem?

QUESTION 40: How much trust do you have in organisations conducting data broking for marketing, research or other purposes? Would this trust differ if you had more transparency about how your data is used?

QUESTION 41: How can organisations who conduct data broking improve transparency or awareness of their operations to instil confidence in consumers about data security?