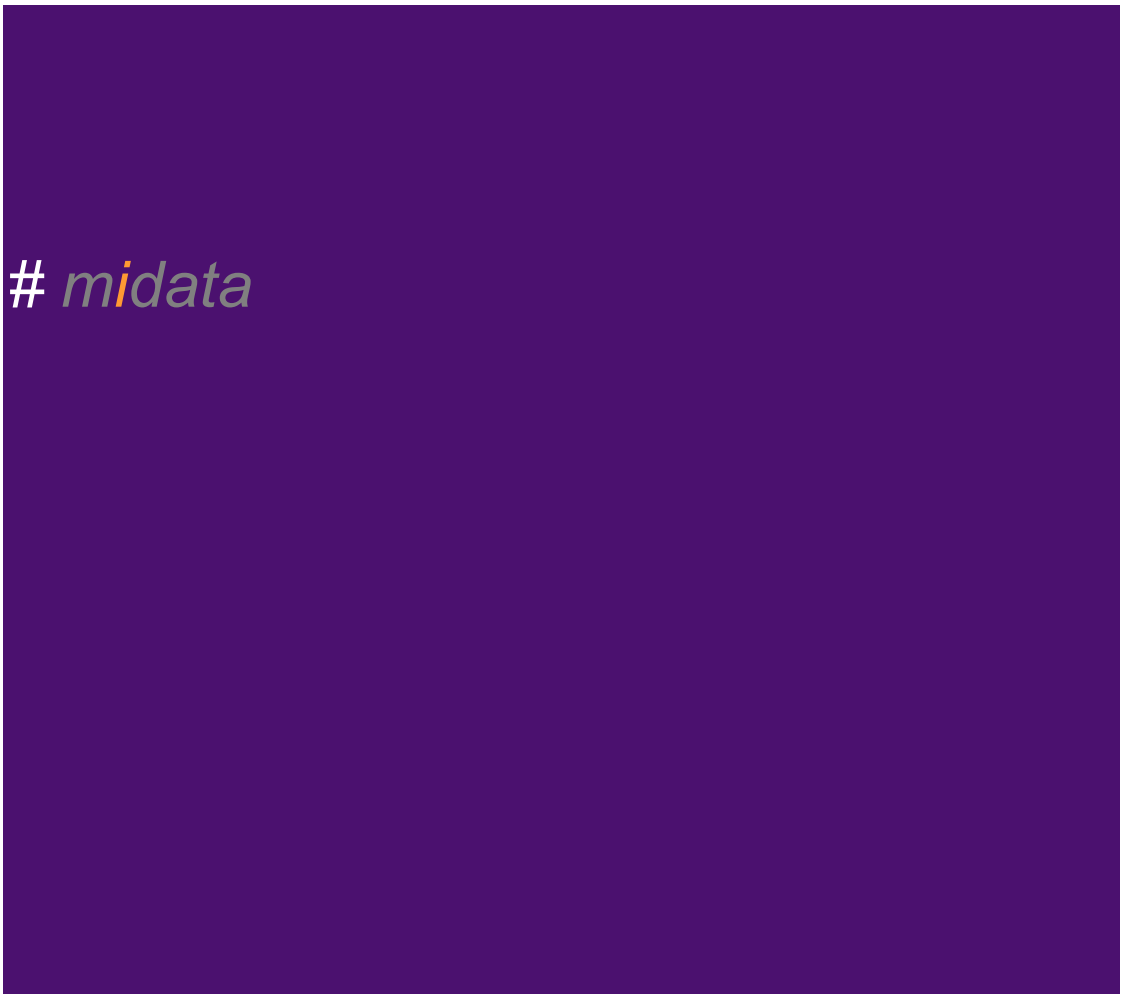
Department for Business Innovation & Skills

midata

Privacy Impact Assessment Report



Contents

Executive Summary

Background

1. In April 2011 the Government published the consumer empowerment strategy, Better Choices: Better Deals; Consumers Powering Growth, and work on midata was part of the "power of information" element of that strategy. The aim of the midata programme is to give consumers access to their transaction data in a way that is electronic, portable and safe. Since April 2011 midata has been a voluntary partnership between the UK Government, businesses, consumer groups, regulators and trade bodies.

2. midata is part of the Government's growth agenda; it will help achieve economic growth by improving information sharing between organisations and their customers, sharpening incentives for businesses to compete keenly on price, service and quality. It will also facilitate the creation of a new market for personal information services that empower individuals to use their data for their own purposes.

3. In July 2012 the Government published a consultation reviewing midata and inviting feedback on a proposal to create an order-making power that would enable the Government to require transaction data to be released by suppliers in an electronic, machine readable format at the consumer's request. The consultation closed on 10 September 2012.

4. The Government response[1] to the consultation sets out that the Government intends to proceed with its plan to legislate for a power to impose a duty on businesses which collect this kind of data, with an initial focus on four sectors: energy supply, mobile phones, current accounts and credit cards. The Government will retain the possibility of regulating other sectors should there be an evident need, but with a high bar for doing so.

5. The Government wishes to see the voluntary midata programme under Professor Nigel Shadbolt's chairmanship continue, with close cooperation and engagement between Government, business and consumer groups. Should the Government come to the view that it is appropriate to bring forward secondary legislation under the power, it will undertake further consultation and engagement with business and other stakeholders.

[1] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/43392/12-1283-midata-government-response-to-2012-consultation.pdf.

6. The consultation demonstrated widespread support for the aims of the midata programme, although there was less agreement that regulating in this area has become necessary. Privacy issues were raised in the consultation responses. Similar issues were also reflected in the consumer research and Interoperability Board[2] analysis undertaken as part of the midata programme. A key part of the existing voluntary programme has been to identify ways to ensure appropriate security and privacy for consumers' data.

7. The Government response also sets out that in the next few months the voluntary programme will focus on data privacy, security and redress and that this work will be completed as a priority. As part of this the Government has established a number of working groups consisting of representatives from business, consumer organisations, regulators and Government Departments to address consumer protection and trust.

Approach

8. The proposal is to take a regulation making power. Of itself the power will not effect any substantive change in the law. If the power is exercised, the regulations will effect such a change. In addition the regulation making power, and if utilised the regulations themselves, will not directly affect the handling of personal data as defined in the Data Protection Act (DPA) 1998, but instead will facilitate the release of data to a customer, in a specified, electronic and portable format which the DPA does not require. This only applies to transaction that is already held electronically by businesses. The data held by the businesses who are in scope of the proposed midata legislation are and will continue to be subject to the requirements of the DPA, regardless of whether the duty to release it electronically and in a portable format is utilised.

9. Given this we have decided to undertake a small scale Privacy Impact Assessment (PIA) in relation to the midata power proposal, and would conduct a more detailed full-scale Privacy Impact Assessment if regulations are made under the power. The full scale PIA would therefore only be completed once the working groups have had time to feed back their learning, and following further consultation with business and stakeholders.

10. This will allow the Government to make a more informed analysis of the impact any regulations themselves would have on the privacy protections and security of data released as part of midata.

[2] The Interoperability Board sits under the BIS midata programme and is tasked with identifying and addressing cross-cutting issues such as standards and data protection/security issues for business and consumers that midata must address. Members include representatives of industry, consumer and privacy organisations and regulators.

Findings

11. This small scale PIA[3] sets out that the proposals, of themselves, are likely to have a limited impact on the security of data released as part of the midata proposal. This is because the data released by existing data controllers as part of midata will continue to be subject to the controls and protections set out in the DPA. It is important to note in this regard that under the DPA consumers already have the right to access personal data held on them by any person (including businesses and other organisations) and have this released to them in an intelligible format under a Subject Access Request (SAR). The current DPA right requires the delivery of information within 40 days and can be subject to a charge of up to £10 per request. The midata proposal will do nothing to alter consumer's rights to access information held on them as part of a SAR request. Instead, it is an additional right that will allow them to access consumption/ transaction data held on them by a business in an electronic, portable format if the business already holds that information electronically.

12. However, the Government recognises that there could be risks associated with the security of data under the midata proposals. Specifically these risks are probably greatest if the consumer gives access to their data either directly or indirectly to third parties in order for them to analyse and interpret behaviours and usage. For most consumers this will be necessary if they are to make the best use of that data and get the best deals or to receive beneficial advice on their lifestyle or spending habits.

13. In order to address these issues the midata Interoperability Board created a number of working groups. These groups will identify and recommend existing or new approaches that may be needed to ensure that where individuals wish to forward on their midata data to third parties, the consumer:

    - retains control over that data and how it is used;
    - has their privacy fully protected;
    - does not become subject to data misuse and exploitation.

    In making their recommendations the groups will have regard for existing best practices and available/emerging technologies.

14. The Government will have close regard to the above issues. As the Government develops thinking around the application of the power the learning, and lessons, from these working groups will form part of subsequent consultation(s) if and when secondary legislation is considered. The working groups will aim to publish their recommendations

[3] See page 6 for a definition of a small scale PIA

by summer 2013. Even if secondary legislation is not brought forward in the near future, the Government will take the action necessary to safeguard consumers as the voluntary programme progresses.

Review Process

15. The Interoperability Board's advice on data handling processes and procedures will continue to be monitored by the voluntary programme's Strategy Board chaired by Professor Nigel Shadbolt. If secondary legislation is brought forward then this work will inform a full-scale PIA that will accompany the measure. It may be necessary to undertake a further review of security risks arising from the release of midata after a period of time even if regulations are not made.

Partial (small scale) Privacy Impact Assessment on the proposal to legislate to give consumers access to data in an electronic, machine readable form

Background

16. A Privacy Impact Assessment (PIA) is a process that helps assess privacy risks to individuals in the collection, use and disclosure of information. PIAs help identify privacy risks, foresee problems and bring forward solutions. The primary purpose of a PIA is to visibly demonstrate that an organisation acts responsibly in relation to privacy. The deliverables and benefits of undertaking a PIA can be summarised as follows:

    - The identification and management of risk;
    - Avoidance of unnecessary costs;
    - Prevention of inadequate solutions;
    - Avoiding loss of trust and reputation;
    - Informing citizens and partners of the organisation's communications strategy;
    - Meeting and exceeding legal requirements.

17. The objective of conducting this PIA is to identify any data protection issues associated with the proposal to take a regulation making power which, if utilised, would compel suppliers of certain services and goods to provide to their customers, upon request, their historic transaction and consumption data in a machine readable format.

18. It is important to remember that ultimately the focus of a PIA is compliance with the Data Protection Act (DPA). However, compliance with any other relevant legislation (e.g. sectorally based legislation) will also been considered.

Underlying principle

19. Data sharing and testing must be undertaken within a clear legal framework with any intrusion upon an individuals' privacy to be kept to a minimum. By undertaking a PIA we ensure this principle is met. However, it is important to consider that the midata proposals do not deal with data handling directly but rather a power to require the release upon request of historic transaction and consumption data in a machine readable format back to consumers. The content of the data involved is mostly already available to consumers – midata regulations would only change the format in which it is to be provided.

HMG requirement

20. The Data Handling Review, published in June 2008, states that all Departments will "introduce Privacy Impact Assessments, which ensure that privacy issues are factored into plans from the start, and those planning services are clear about their aims. Similarly, information risk management will be considered as part of the Government's "Gateway" reviews that monitor progress of the most important projects". The Data Handling Review has now been subsumed into HMG Information Assurance Standard No 6 – Protecting Personal Information and Managing Information Risk. Accordingly, PIAs are to be carried out on projects and policies that involve the processing of personal data.

PIA Process

21. The process for conducting a PIA is described by the ICO as follows:

Initial assessment (i.e. the Screening Process) – Examines the project at an early stage, makes an initial assessment of privacy risk and decides which level of assessment is necessary. Where necessary, conduct, either:

- Full-scale PIA – a more in-depth internal assessment of privacy risks and liabilities. It includes the need to identify stakeholders, analyse privacy risks, consults widely with stakeholders on privacy concerns and brings forward solutions to accept, mitigate or avoid them; or

- Small-scale PIA – Similar to a full-scale PIA, but is less formalised. Requires less exhaustive information gathering and analysis. and

- Review – Sets out a timetable for reviewing actions taken as a result of a PIA and examines their effectiveness. Looks at new aspects of the project and assesses whether they should result in an updated PIA.

22. The Government considers that a full-scale PIA would be necessary should regulations be introduced. However, a small-scale PIA is more appropriate for the regulation making power.

23. This report deals with the small-scale PIA for proposal to take a regulation making power which, if utilised, would compel suppliers of services and goods to provide to their customers, upon request, their historic transaction data in a machine readable format.

Overview

24. In July the Government published a consultation on creating an order-making power to enable the Government to require certain consumption and transaction data to be released electronically at the consumer's request. The consultation closed on 10 September 2012.

25. The Government received over 400 responses to the consultation as well as over 60 attendees to the 5 Open Forums that were held in the BIS offices over the summer. Of these responses we received over 50 from major businesses and stakeholders. In addition a number of bi-lateral meetings were held with trade bodies and businesses from across all sectors, to both inform the response to the consultation and to build a robust evidence base for acting in this area.

26. The Government response[4] to the consultation sets out that the Government intends to proceed with its plan to legislate for a power to impose a duty on businesses which collect this kind of data, with an initial focus on four sectors: energy supply, mobile phones, current accounts and credit cards. The Government will retain the possibility of regulating other sectors should there be an evident need to do so, but with a high bar for doing so.

27. The Government set out the case that providing the midata programme with a legal framework, and so ensuring that consumers have access to their own consumption and transaction data, has key benefits for both consumers and the economy.

28. In assessing these benefits it will be important to balance them with important considerations around data security and privacy. For consumers to fully interact with the possibilities of midata it is important that they are confident that their data is secure, and that their privacy is protected.

[4] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/43392/12-1283-midata-government-response-to-2012-consultation.pdf.

Privacy considerations as part of the midata voluntary programme

29. The midata Strategy Board funded research into potential consumer demand for the midata concept and the services it would enable. The research identified an interest in new services that can help people manage their lives and budgets as well as raising consumers' concerns over the handling of personal data.

30. The research established that there is genuine concern about how data is managed and re-used after it is released to the consumer. There are existing protections in place through data protection and consumer law, but as part of its work the midata programme has considered whether additional systems or protocols are needed to provide protection and confidence using the new services that midata makes possible.

31. This work has been given renewed focus under the voluntary programme, in part because of the concerns raised through the consultation process. The Government has recently established working groups consisting of representatives from business, consumer and privacy organisations, regulators and Government departments to address consumer protection and trust. The remit of the groups is to prioritise and develop a range of solutions to issues including:

    - Assuring the identities of those making requests for data, to avoid breaching privacy;
    - Enabling the safe transmission of data from a business to a customer through appropriate encryption and protection;
    - The possibility of developing new safeguards around data release, transfer and sharing to minimise the risk of customers inadvertently agreeing to their data being shared or sold or losing their data;
    - What redress mechanisms there should be for customers if things go wrong and the relationship with current and potential future data protection rules; and
    - the appropriate role for third parties in accessing and analysing data and how this should be managed.

    Specifically the working groups are considering questions such as:

    - What existing regulation, best practice, protocols or standards could be applied or adapted to midata?
    - How might a business that receives a midata request from a third party for a customer's data satisfy itself that the third party has been

duly authorised by the customer to make the request and/or that the third party will only use the data in the way the customer wants the third party to use it?

- Do regulation, best practice, protocols or standards need to be strengthened, owing to the extra risks posed by midata? If so, how should this be done in a way that is proportionate to risk?

- How will midata interact with any other requirements in this area?

32. Protection may not necessarily lie in further regulation. The work will join up with other initiatives such as Cabinet Office's ID Assurance Programme and the Smart Metering Implementation Programme. The groups are meeting at regular intervals with the aim of developing recommendations by summer 2013.

Privacy considerations as part of the consultation process

33. In light of the issues that were highlighted as part of the voluntary programme a key element of the consultation was seeking respondents' views on the potential impact the proposal could have on privacy and security. To help better understand potential concerns in this area the consultation asked the following questions:

    - What is your view on the likely impact of the proposed approach on privacy, consent and information security and the implication for data protection?

    - Should a consumer be able to require the business to supply the data in electronic format directly to a specified third party?

    - Should a third party who is duly authorised by the consumer be able to seek the consumer's data in electronic format directly from the supplier?

    - What, if any, requirements should be placed on the secondary users of such data, albeit under the direction of consumers e.g. switching and advice sites?

Responses to questions relating to security

34. The views on requiring data to be supplied to third parties were finely balanced. On the one hand, it was recognised that the analytics provided by third parties would make the data more useful to consumers, including helping them getting a better deal. On the other hand, many respondents (both from consumers and business representatives) had concerns about data security and privacy, including the risk of data loss.

35. The need for a robust privacy and security framework was seen as necessary if businesses were to be required to disclose information directly to a third party at the customer's request or at a duly authorised third party's request.

Conclusion

36. Appropriate actions are in train to address privacy issues that might arise from the introduction of a new power to regulate for the release of transaction data in an electronic format upon request.

37. A further full-scale PIA will need to be undertaken should regulations under the midata power be introduced and will be informed by the recommendations emerging from the actions set out above.

38. Even if secondary legislation is not brought forward in the near future, the Government will take the action necessary to safeguard consumers as the voluntary programme progresses.

This publication is also available on our website at www.gov.uk/bis

Any enquiries regarding this publication should be sent to:

Department for Business, Innovation and Skills
1 Victoria Street
London SW1H 0ET
Tel: 020 7215 5000

If you require this publication in an alternative format, email enquiries@bis.gsi.gov.uk, or call 020 7215 5000.

BIS/13/604