CtrlShift
Unleashing the power of trust

PERSONAL DATA PROTECTION COMMISSION SINGAPORE

Public Consultation on Review of the Personal Data Protection Act 2012 – Proposed Data Portability and Data Innovation Provisions

Response from

CtrlShift
Unleashing the power of trust

For further information contact:
Liz Brandt, CEO, Ctrl-Shift
Email: liz.brandt@ctrl-shift.co.uk
Mobile: +44 (0) 7884 433108
Office: +44 (0)20 7759 1057
Postal Address:
Somerset House
Strand
London, WC2R 1LA

Ctrl Shift
Unleashing the power of trust

Background to Response

In 2018, Ctrl-Shift completed a major study for the UK Department of Digital, Culture, Media and Sport (DCMS) which uncovered the huge untapped economic potential that is liberated by Personal Data Mobility.

The 2018 DCMS report also identified what needed to be addressed for Personal Data Mobility to be achieved. This fell into two main categories - the infrastructure required to enable Personal Data Mobility and how it can be used to create valuable new services.

In 2019 Ctrl-Shift created the Data Mobility Infrastructure Sandbox specifically to bring together leading businesses, consumers and consumer organisations, government, regulators, and data facilitators to collaborate on addressing these core issues, within an independent, facilitated environment. Sandbox participants include Barclays, the BBC, BT, Centrica, Facebook and digi.me, the leading data facilitator. There are also a number of independent observers - the Centre for Data Ethics and Innovation, Consumers International, the DCMS, the Information Commissioner's Office and the Web Science Institute at the University of Southampton.

The Sandbox's central objective is to advance Personal Data Mobility to enable the safe and easy use of personal data, permissioned and controlled by the individual, enabling value that is fairly and safely shared by all.

This first phase of the Data Mobility Infrastructure Sandbox examined safe data sharing - one of the primary infrastructural challenges identified in the DCMS commissioned, 2018 Data Mobility Report. It has also investigated how new value can be unlocked by making data sharing safer for individuals and organisations.

Safe data sharing is of foundational importance to Personal Data Mobility. If it is not in place, there is a risk that individuals experience harm and businesses suffer reputational damage, leading to both sides being less willing to participate and the full potential value of Personal Data Mobility not being realised.

Prior to GDPR, data sharing took place between organisations with minimal (if any) consent from individuals and limited transparency provided by the organisations sharing data. GDPR has given individuals more control over their data but legal enablement needs to be matched with infrastructural enablement to ensure data sharing is safe. For example, unless users have some validation that the organisation to which they are about to port their data is secure, privacy respecting and will use the data transferred to it for the reasons agreed, the right to portability creates risks for individuals. It also potentially creates reputational risks for the businesses who supplied the data as individuals are likely to seek recourse from them if something goes wrong.

It is for this reason that the Data Mobility Infrastructure Sandbox explored safe data sharing via the Data Mobility Model. This is a model for safe, multi-lateral data sharing between four key stakeholders: data exporters (existing service providers holding data), individuals (who choose to share their data held by data exporters), data facilitators (who act on behalf of individuals, enabling them to transfer, store and use their personal data) and data importers (who use the newly mobilised data to create valuable products and services for the individual). And it was a key finding of the report that the presence of data facilitators is a key driver for both safe and valuable data sharing.

The report published on 17th June covers this first phase of work and describes the current enabling capabilities for data sharing and importantly defines the gaps that need to be filled for it to be safe and valuable. To signpost the way forward, it also identifies the gaps that the Data Mobility Infrastructure Sandbox has prioritised for attention in its next phase of work.

Conclusions

Ctrl-Shift welcomes any initiative to enhance Personal Data Mobility and the proposed data

portability provisions are a step in the right direction. However it is also our view that the huge potential value that Personal Data Mobility can deliver will only accrue when data is truly mobile – available via APIs on a persistent basis in real time and interoperable – and not just portable. Hence we would urge the PDPC to look beyond data portability as currently conceived and seek to make Singapore a leader in Personal Data Mobility.

Our research identified that the Data Mobility Model and the use of a data facilitator can help make data sharing safer and we would urge the PDPC to encourage the development of data facilitators who work on behalf of individuals, helping them to share their data more safely.

We also believe that legal enablement of data portability without infrastructural enablement creates a risk for users that they share data with an organisation that may cause them harm. A critical gap identified by our research is the validation or accreditation of the Third Party Providers (TPPs) with whom people are considering sharing their personal data. The current model of individual businesses undertaking due diligence on TPPs does not deliver consistency, efficiency or scalability. Similarly the centralised model of a regulator validating TPPs, as in Open Banking, also has scalability challenges, particularly if TPPs become the engine of innovation and their numbers increase dramatically. We believe the PDPC needs to address this challenge and in so doing could make Singapore a model for others to follow.

Similarly another gap identified is the absence of clear liability definition and communication. Without clear liability definition, who is responsible for carrying risks is not clear to all parties, meaning people may be incurring risk without realising it. Further, without clear liability definition, the creation of mitigations to the risks identified is constrained, meaning the risk in the market is higher than it otherwise would be. Once it is clear who is liable, there is an incentive for those parties to create mitigations or for others to create mitigations on their behalf (e.g. insurance products). Again we would encourage the PDPC to investigate the creation of a liability model for data sharing in Singapore that makes it an exemplar that other data protection authorities seek to emulate.

Response

Q1. What are your views on the impact of data portability, specifically on consumers, market and economy?

As highlighted in our 2018 report for the DCMS, personal data mobility is critical to the creation of digital value and thereby the growth of digital economies. The report's economic assessment identified a value opportunity in productivity and efficiency gains of £27.8bn in the UK alone. On top of which, the report identified significant innovation opportunities from combining data – expected to be worth many times the productivity uplift - and the gains to be had from creating healthier commercial markets.

In our view, much of this value arises when personal data is genuinely mobile rather than just portable. Personal data mobility goes beyond personal data portability. Under the GDPR people can port personal data from one provider to another, but currently this process tends to be manual and ad hoc. With personal data mobility, personal data flows safely and efficiently to where it can create maximum value, with the individual in control, ensuring that personal, social and economic benefits are distributed fairly. Our vision of personal data mobility equates closely to the UK Government's definition of Smart Data in the most recent consultation document.

Q2. What are your views on the proposed Data Portability Obligation, specifically –

a) Scope of organisations covered;

Our findings suggest that both breadth and depth of data are key to value creation. The provision of government services requires the collection of significant amounts of personal data and if this is excluded, it limits the innovation opportunity. For example in the UK, data from the National Health Service is a regarded by innovative service providers as a major source of potential value in helping people to better manage their health and wellbeing.

b) Scope of data covered?

The limitation to data that is in electronic form and has been provided by the user or generated from their behaviour is sensible in our view.

Q3. What are your views on the proposed exceptions to the Data Portability Obligation, specifically –

1. **a) the proposed exception relating to commercial confidential information that could harm the competitive position of the organisation, to strike a balance between consumer interests and preserving the incentive for first movers' business innovation;**

While this appears reasonable, the risk is that organisations seek to use this as a means for severely limiting what data is shared. Additional specification of what data falls into this category and what data doesn't would be helpful.

2. **b) the proposed exception for "derived data"?**

While it is reasonable for consumers to know what is being inferred about them, being able to port that data to another provider risks damaging the IP of the existing service provider and so could disincentivise investments in AI and Machine Learning.

Choosing the right scope of data is critical as the timescales to implementing data portability are not insignificant. Although all data is valuable and useful the enforced sharing of valuable data sets that are costly to create, categorised as inferred data, may prevent the creation of such data and in doing delimit the growth in the digital economy rather than enhance it.

Q4. What are your views on the proposed requirements for handling data portability requests?

As highlighted by our report, we believe that unless data is mobile – available immediately, delivered via APIs rather than via a one-off batch transfer, and structured in a genuinely interoperable format rather than just machine readable one – much of the value cannot be realised.

Q5. What are your views on the proposed powers for PDPC to review an organisation's refusal to port data, failure to port data within a reasonable time, and fees for porting data?

No additional comment to response provided to Q4.

Q6. What are your views on the proposed binding codes of practices that set out specific requirements and standards for the porting of data in specific clusters or sectors?

No additional comment to response provided to Q4.

Q7. What are your views on the proposed approach for organisations to use personal data for the specified businesses innovation purposes, without the requirement to notify and seek consent to use the personal data for these purpose?

We see business innovation as the major source of value creation for individuals, businesses and society as a whole. We agree with the proposed approach as the alternative - requiring consent to use personal data that an organisation currently holds about an individual for innovation purposes – would create a barrier to the creation of new services of value to the individual.

Q8. What are your views on the proposed definition of "derived data"?

We would agree with the proposed definition of derived personal data.

Q9. What are your views on the proposal for the Access, Correction and proposed Data Portability Obligations not to apply to derived personal data?

We would argue that giving individuals the right to access and correct derived personal data serves both parties. For example, if the derived data – for example a classification of someone or a prediction of their interests – is inaccurate, then the organisation benefits from being informed that this is the case, and the individual is not presented with offers or recommendations that are of no interest to them. The ability to update advertising preferences in Google and Facebook, derived from data that those businesses have access to, would be a case in point.

Transparency is also critical to gaining trust, more importantly lack of transparency promotes distrust. Without trust, data sharing is significantly reduced and the potential value it can create is significantly limited.

The risk to existing providers is also limited as the degree to which it is possible to reverse engineer their algorithms from the sub-set of customer data that a new provider can access is very much open to question - their algorithms having been derived from processing personal data over an extended period of time across a much wider base. Further any new provider that focuses on replicating the predictions and classifications of an existing provider, by definition, will not offer a significant uplift in value and so are unlikely to displace.

West Wing, Somerset House
Strand, London, WC2R 1LA
Tel: 020 7000 1907
Email: info@ctrl-shift.co.uk