Privitar's contribution to PDPC's Public Consultation on Approaches to Managing Personal Data in the Digital Economy[1]

19.9.17

Organisation:
Privitar
Capital Tower
91 Waterloo Road
London
SE1 8RT
United Kingdom

Contact:
Guy Cohen
Policy and Strategy Lead
guy.cohen@privitar.com
+44 7557 331543

[1] https://www.pdpc.gov.sg/docs/default-source/public-consultation-5---act-review-1/public-consultation---approaches-to-managing-personal-data-in-the-digital-economy-(270717)f95e65c8844062038829ff0000d98b0f.pdf?sfvrsn=2

PRIVITAR

1. **Introduction to Privitar's response**

This response represents the view of Privitar Ltd. with regards to the Personal Data Protection Commission's (PDPC) consultation on approaches to managing personal data in the digital economy. Privitar is a UK based privacy engineering enterprise software company, with commercial interests in Singapore. This response specifically relates to Questions 3 & 4 of the consultation.

Privitar supports the PDPC's proposed expansion of the legal basis for processing. Privitar believes the PDPC should clarify and expand the additional legal basis for processing to make clear that legitimate business interests are not contingent on wider public interests. Privitar believes that this expansion should be supported by, and contingent upon, stronger privacy safeguard requirements.

This response explores the rationale for why it would be appropriate to expand the legal basis for processing, and what it should be expanded to include. It does this by commenting on specific aspects of the proposal. Annexes A & B expand on some of the potential safeguards which Privitar believes could effectively minimise privacy risk.

Privitar believes that this approach will benefit the economy of Singapore by encouraging data usage and innovation, whilst simultaneously improving the privacy protections afforded to individuals whose data is collected and processed in Singapore.

In this response to the consultation Privitar refers to data subjects and data controllers to refer to those individuals whose data is being processed and the organisations which are doing that processing, in line with the definitions used in the EU General Data Protection Regulation (GDPR).

2. **Comments**

Comments on 2.2-2.5

Paragraphs 2.2 to 2.4 effectively summarise the problems with using consent as a legal basis for processing. Highlighting the issues of purpose limitation, consent fatigue and the challenges of obtaining informed consent.

Paragraph 2.5 identifies the economic benefits of data, and demonstrates a desire to utilise data assets for the economic benefit of Singapore.

Privitar strongly supports both of these positions. Following from these points, Privitar believes that the potential value of personal data should drive regulators to find a better way of protecting individual's privacy whilst enabling the broader, wider use of data.

Privitar believes an effective way of doing this is to require organisations to act in the interests of their data subject' privacy by making the ability to process personal data contingent on demonstrating that any privacy risks posed to the data subjects has been effectively mitigated.

To be clear, where consent can still be meaningful, Privitar believes consent should be used as a legal basis. And where data is processed not on the basis of consent, data subjects should retain the right to object to that processing and be able to have their data excluded from the processing, if appropriate. The purpose of allowing processing without consent is to ensure that those who do not engage actively in considerations relating to their privacy are still afforded a high level of protection, but this should not prevent those who do wish to be actively engaged in decisions relating to how their data is processed from retaining a high level of control of that processing.

Unlike the data subject, the data controller has the time, resources, access, and expertise to consider the potential privacy risks posed by any processing. Making their ability to process the data reliant on their ability to demonstrate that they have mitigated any significant privacy risks to the data subject, is therefore an effective way of aligning the party best suited to protect privacy with the incentives to do so.

Comments on 3.15

"*In addition, PDPC considers that it may not be meaningful to notify individuals of the collection, use or disclosure for a Legal or Business Purpose since the individual may not withdraw consent*."

Given the earlier paragraphs relating to processing on the basis of notification, Privitar interprets the PDPC's position as viewing notification and business interests as alternative bases for processing. Privitar would encourage, even when processing on the basis of a business interest, the PDPC to require controllers to notify data subjects when their data is being collected, how it will be processed and how they can object, unless there is a good reason why this is not feasible.

As mentioned above, whilst organisations should have the ability to collect and process data without obtaining consent, as the PDPC outlines in paragraph 3.9, Privitar believes that that right is not absolute and should be open to challenge to ensure that data subjects' rights remain protected. Data subjects should retain the ability to object to the processing of their data when the data is not being processed on the basis of consent. They should also retain the right to appeal to the PDPC, or an equivalent impartial authority, if they are unsatisfied with how their objection has been dealt with. In order for the right to object to be meaningful, they must be informed of the processing of their data. Whilst it may not be feasible for organisations to prove that data subjects have been informed, they should still make reasonable efforts to inform the data subjects, both at the point of collection (where possible) and online, for instance through a clear, visible and easily accessible privacy notice on their website.

There are instances where this may not be feasible, such as in the example cited by the PDPC relating to fraud detection, where the public interest would conflict with the individual's right to object to processing. In these instances, the rationale for why notification is not feasible should be publicly available to be reviewed by data subjects and the PDPC.

Comments on 3.15(b) and 3.16

In reading the proposition from the PDPC it was not clear to Privitar what constituted a legitimate business interest. The focus on a public benefit in 3.15(b) and the example cited in 3.16 both imply a focus on the public benefit, but do not make it clear whether processing which had no wider benefit to society outside of the benefit achieved through the furthering of the organisation's business interests, would be permitted.

"*The proposed Legal or Business Purpose would be subject to the following conditions… the benefits to the public (or a section thereof) clearly outweigh any adverse impact or risks to the individual*"

Privitar supports the public interest as a basis for data processing. However, to ensure organisations operating in Singapore are able to innovate, improve services and remain competitive, Privitar believes it is important to explicitly state that a legitimate business interest without any wider public benefit, is an acceptable basis for processing. This could be done by stating clearly that a legal business benefit is considered a public benefit.

For example, should an organisation wish to process customer data to improve their product offerings, this should be allowed to be done without the consent of their customers, so long as they have effectively safeguarded against any significant privacy risks posed by the processing to their customers.

Comments on 3.17

Privitar welcomes the introduction of privacy impact assessments (PIAs) as a method for identifying risk. However, Privitar would encourage the PDPC to go beyond recommending a methodology for identifying risk, and support organisations further by also recommending specific safeguards which should be considered for mitigating any risks identified. It is only of limited value to identify potential privacy risks if the data controller is not equipped to effectively act upon these risks. The PDPC is well positioned to issue guidance on potential safeguards. Some safeguards which are worth considering are listed in Annexes A & B.

3. Conclusions

Question 3: Should the PDPA provide for Legal or Business Purpose as a basis for collecting, using and disclosing personal data without consent and notification?

Yes. Furthermore, Privitar would encourage the PDPC to clarify what constitutes a legal or business purpose, and to include within the definition of legal and business interests solely business interests, where there is no public benefit beyond the furthering of the business objectives of that organisation.

Question 4: Should the proposed Legal or Business Purpose approach be subject to conditions? If so, what are your views on the proposed conditions (i.e., not desirable or

appropriate to obtain consent and benefits to the public clearly outweigh any adverse impact or risks to the individual)?

Yes. Safeguards should be used to ensure that the stated purposes and interests do not represent an unacceptable risk to individuals' privacy. Additionally, individuals should be granted the right to object to the processing of their data when it is not being processed with their consent. For an expansion on potential conditions for processing please see Annexes A & B.

Annex A – Privacy Safeguard categories

The following table is an extract from the European Union Agency for Network and Information Security's (ENISA) paper 'Privacy by design in big data – an overview of privacy enhancing technologies in the era of big data analytics'. It categorises the various ways in which data subjects' privacy can be protected.

	PRIVACY BY DESIGN STRATEGY	DESCRIPTION
1	Minimize	The amount of personal data should be restricted to the minimal amount possible (data minimization).
2	Hide	Personal data and their interrelations should be hidden from plain view.
3	Separate	Personal data should be processed in a distributed fashion, in separate compartments whenever possible.
4	Aggregate	Personal data should be processed at the highest level of aggregation and with the least possible detail in which it is (still) useful.
5	Inform	Data subjects should be adequately informed whenever processed (transparency).
6	Control	Data subjects should be provided agency over the processing of their personal data.
7	Enforce	A privacy policy compatible with legal requirements should be in place and should be enforced.
8	Demonstrate	Data controllers must be able to demonstrate compliance with privacy policy into force and any applicable legal requirements.

Table 1: Privacy by design strategies [6]

Source: https://www.enisa.europa.eu/publications/big-data-protection

Annex B – Privacy safeguard technology examples

Below is a list of illustrative examples of where privacy enhancing technologies can be deployed to safeguard data subjects in line with the strategies identified by ENISA.

1. **Minimise**

Pseudonymisation and generalisation with *k*-anonymity

Pseudonymisation prevents individuals from being identified when a dataset is looked at in isolation. It works by replacing direct identifiers with pseudonyms. It is sometimes also referred to as tokenisation or masking.

Further protections can be placed on data through use of statistical anonymisation techniques including generalisation or perturbation. These approaches add further protection to pseudonymisation by ensuring that individuals cannot be identified even if their data is combined with other datasets. It works by making changes to indirect identifiers such that individuals become indistinguishable from one another. When all individuals are indistinguishable from at least *k*-1 others, then the dataset is considered to be *k*-anonymous.

2. **Hide**

Encryption including homomorphic encryption schemes.

Encryption can be used to prevent access to sensitive data. Homomorphic and partial homomorphic schemes can be used to enable some compute operations in semi or untrusted environments. E.g. Leveraging partially homomorphic encryption, datasets can be linked without the linking identifiers being visible. This enables datasets to be joined whilst ensuring that the identities of those within the dataset remain hidden.

3. **Separate**

Multi party computation

Multi party computation allows for processing to be distributed such that no individual party is able to see all of the sensitive data being processed.

4. **Aggregate**

Set based aggregation and differential privacy

Query privacy operates by providing users with the ability to execute aggregate queries against sensitive data . Users are able to submit queries to the dataset, and receive back aggregate responses. To prevent differencing or tracker attacks, where the user executes multiple allowable queries in combination to isolate a target, noise can be added to the responses to ensure that the interface is differentially private.

5. **Inform**

Layered and just in time privacy notices

As explored in the UK's Information Commissioner's Office's (ICO) code of practice on privacy notices, layered and just in time privacy notices ensure that users are provided with the appropriate information at the time when it is relevant for them to be aware of that information. For further information, see:

https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

6. **Control**

Open APIs and data discovery tools for data subject requests.

APIs offer a way of allowing organisations to easily respond to certain kinds of request from data subjects. For instance, the standardised APIs which will be built to support compliance with the UK's Open Banking Initiative following the EU's Second Payments and Services Directive, allow data subjects' requests for their data be extracted from one organisation and transferred to another organisation of their choice to be automated. Similarly, data discovery tools which allow organisations to search for sensitive data types, or data relating to specific individuals, allow organisations to effectively respond to data subjects' requests.

7. **Enforce**

Policy management systems

Central policy engines provide a way of controlling which privacy policies are applied to which datasets for varying user groups and domains. This allows for a consistent approach across the enterprise and ensures that an organisation can set and enforce minimum standards across their organisation. Policies are recorded, providing an auditable account of what data has been provided to whom, with information on the policies applied.

8. **Demonstrate**

Data governance tools and data watermarking

There are a range of tools which support auditability of processing. For instance, the data discovery and policy management tools described above allow organisations to audit what data they have and what policies they have applied. Watermarking can build on these audit and accountability tools by protecting data from being used inappropriately.

Data watermarking is a method whereby a signal is inserted in a dataset which makes that dataset uniquely identifiable. Watermarking acts as a deterrent and ensures that data controllers can identify the provenance of a dataset, what is in the dataset, and who was responsible for it.