Singapore Personal Data Protection Act (PDPA)

Frequently asked questions (FAQ) guide

2 October 2018

ReedSmith

Driving progress
through partnership

Singapore issues new guidelines on the Personal Data Protection Act for national identification

As of 1 September 2019, all private sector organisations in Singapore will be prohibited from collecting, using or disclosing all national identity cards, their copies and numbers, unless they are required to do so under law, or if it is necessary to verify individuals' identifies to a "high degree of fidelity".

Under Singapore's Personal Data Protection Act 2012 (PDPA) contraventions of these rules could lead to an organisation facing a financial penalty of up to S$1 million.

This document is intended to clarify some commonly raised questions on the applicability of the guidelines. We hope you find this guide useful; however, if you would like further information, please get in touch with **Charmian Aw**.

Charmian Aw
Counsel
Singapore
+65 6320 5367
caw@reedsmith.com

Applicability

Do the guidelines apply only to the national registration identity cards (NRICs) of Singapore citizens?

⊗ No

They apply to both pink NRICs for Singapore citizens and blue NRICs for Singapore permanent residents, as well as birth certificate numbers, passport numbers, foreign identification numbers (FIN) (which are unique identification numbers assigned to foreigners who are issued with immigration and/or work passes in Singapore; for instance, a student's pass or a work pass) and work permits.

Do the guidelines apply to the collection, use and disclosure of NRICs and other national identification numbers by any of the public agencies of Singapore (i.e., government ministries, statutory boards and organs of state)?

⊗ No

The guidelines themselves clarify that as with primary legislation, the PDPA itself, public agencies are not subject to their rules.

Do the guidelines treat any differently: (a) physical NRICs and other national identification cards; (b) their photocopies; and (c) the personal data that is contained therein (for instance, an individual's full name, photograph, thumbprint and residential address)?

∅ Yes, to an extent

The guidelines regard physical NRICs (and other national identification documents containing the NRIC numbers or other national identification numbers, such as a driver's licence, passport and work pass) as requiring the most stringent protection. Specifically, the guidelines stipulate that businesses must refrain from retaining individuals' physical NRICs (and other national identification cards) unless such retention is specifically required under the law.

In relation to any physical NRICs or other national identification cards, photocopies of NRICs or of other national identification cards, any NRIC numbers or other national identification numbers, organisations will only be allowed to collect, use or disclose these if:

- They are required to do so under the law or an exception in the PDPA applies; or
- It is necessary to accurately establish or verify the individuals' identities to a high degree of fidelity.

Such organisations would still need to comply with other applicable obligations under the PDPA, including the notification and consent obligations.

Finally, in respect of all other personal data that is contained in any national identification cards, such data will continue to be subject to the requirements under the PDPA.

Definitions

What does a high degree of fidelity mean?

This would need to be ascertained on a case-by-case basis. However, examples include where a failure to accurately establish the individual's identity to such high degree of fidelity may:

- Pose a significant safety or security risk
- Pose a risk of significant impact or harm to an individual and/or the organisation itself (for instance, with regards to fraudulent claims).

Impact

How do these guidelines affect the collection, use and disclosure of employees' data?

Under the Employment Act, all employers are required to maintain detailed employment records of employees covered under the Employment Act. Such records include an employee's NRIC number. Hence, an employer would be able to collect, use and disclose its employees' NRIC information so long as they are covered by the Employment Act.

On 2 October 2018, the Employment (Amendment) Bill was read for the first time in Parliament. The bill seeks to amend the Employment Act such that the latter will cover all employees. Previously, managers and executives earning a basic monthly salary of more than S$4,500 would not otherwise have been covered by the act. The amended act will come into operation on a future date which is to be gazetted.

As there is no requirement prescribed by law for an employer to ask for the NRIC numbers of prospective candidates for the purpose of job applications, it would be left to such employer to justify that its collection, use and/or disclosure of NRIC or other national identification information is necessary to accurately establish or verify identities to a high degree of fidelity.

Given the above changes to the law, it would therefore be useful for an organisation to review its practices relevant to its hiring of employees, to ensure that not only its employment contracts, job application forms and other employment-related documentation, but also its data protection policies, contain the necessary provisions to ensure the organisation complies with the PDPA in respect of its collection, use and disclosure of all personal data including that of NRICs and other national registration identification.

Are there any alternative means of ascertaining an individual's identity other than from their NRIC (or other national registration identity card)?

Instead of retaining physical NRICs and other national identification documents of individuals, an organisation may wish to implement procedures for its authorised personnel to merely inspect such cards for identity checking purposes.

Also, instead of asking for NRIC photocopies or recording NRIC numbers in full, organisations can consider recording only the last three numerical digits and checksum contained in an NRIC number (i.e., 567A instead of S1234567A), in line with the data minimisation principle.

A global team you can trust

Our team of more than 90 attorneys across the United States, Europe, the Middle East and Asia has deep experience in compliance, regulatory, litigation defence, technology, contracting and data analysis. As part of the firm's IP, Tech & Data Group, our team brings strength and increased connectivity in today's information economy by developing a collaborative, cross-discipline practice focusing on data security, information governance, technology and intellectual property services. Our team provides practical privacy compliance advice on cutting-edge issues; guides companies through major incidents of data theft, loss and unauthorised access; and defends bet-the-company litigation and disputes over privacy issues.

Key contacts

Anthony J. Diana
Co-Chair, IP, Tech & Data
New York
+1 212 549 0332
adiana@reedsmith.com

Cynthia O'Donoghue
Vice Chair, IP, Tech & Data
London
+44 (0)20 3116 3494
codonoghue@reedsmith.com

Charmian Aw
Counsel
Singapore
+65 6320 5367
caw@reedsmith.com

Carolyn Chia
Consultant, ResourceLaw
Singapore
+65 6805 7329
cchia@resourcelawasia.com

Howard Womersley Smith
Partner
London
+44 (0)20 3116 3498
hwsmith@reedsmith.com

Xiaoyan Zhang
Counsel
San Francisco
+1 415 659 5957
xzhang@reedsmith.com

Global recognition

Our IP, Tech & Data Group is globally recognised by leading publications and directory submissions for excellence in data protection by *BTI Consulting*, *Chambers*, *Legal 500* and *Juve Commercial Law Firms. Our* lawyers are individually recognised by *Global Data Review*, *Incident Response 30*, *Who's Who*, *Chambers*, *Legal 500* and *Juve Commercial Law Firms.*

Thought leadership

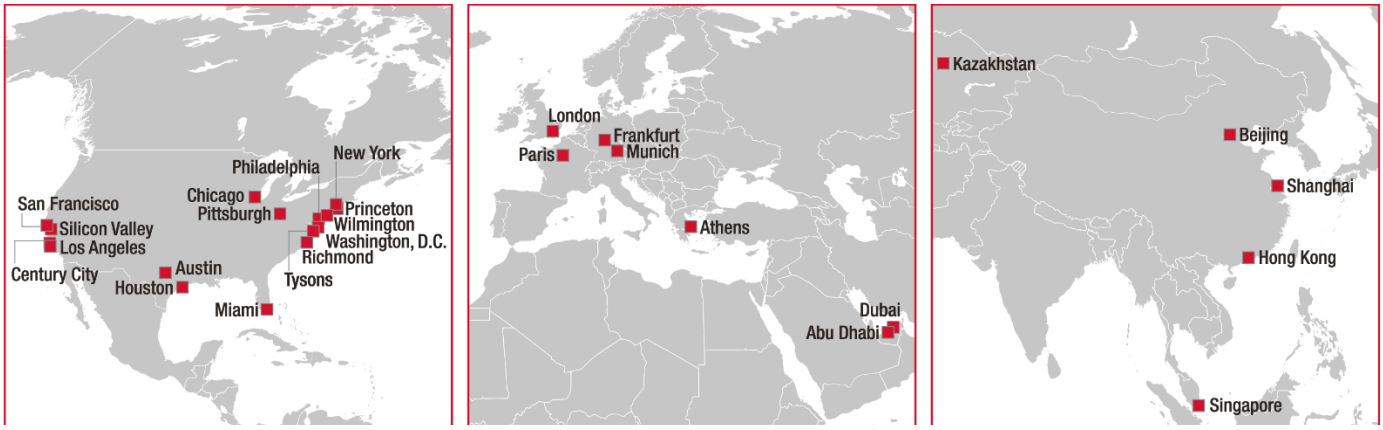
We provide regular updates and practical discussions on technology and the law. Follow us:

www.technologylawdispatch.com @ReedSmithTech www.linkedin.com/showcase/reed-smith-tech

Reed Smith LLP is licensed to operate as a foreign law practice in Singapore under the name and style, Reed Smith Pte Ltd (hereafter collectively, "Reed Smith"). Where advice on Singapore law is required, we will refer the matter to and work with Reed Smith's Formal Law Alliance partner in Singapore, Resource Law LLC, where necessary.

Reed Smith is a dynamic international law firm, dedicated to helping clients move their businesses forward.

Our long-standing relationships, international outlook, and collaborative structure make us the go-to partner for speedy resolution of complex disputes, transactions, and regulatory matters.



ABU DHABI
ATHENS
AUSTIN
BEIJING
CENTURY CITY
CHICAGO
DUBAI
FRANKFURT
HONG KONG
HOUSTON
KAZAKHSTAN
LONDON
LOS ANGELES
MIAMI
MUNICH
NEW YORK
PARIS
PHILADELPHIA
PITTSBURGH
PRINCETON
RICHMOND
SAN FRANCISCO
SHANGHAI
SILICON VALLEY
SINGAPORE
TYSONS
WASHINGTON, D.C.
WILMINGTON

reedsmith.com