Your World First

C/M/S/ Holborn Asia

A guide to GDPR for companies in Singapore

Risk, Resilience and Reputation

About this guide

The EU's General Data Protection Regulation (**GDPR**) applies to companies in Singapore that offer goods and services to, or monitor the behaviour of, individuals in the EU, even if those companies do not have a presence in the EU. For companies in Singapore that are already compliant with Singapore's Personal Data Protection Act (**PDPA**), this raises the question of what additional steps they need to take in order to ensure compliance.

This guide is designed to help. It summarises the extent to which each of the key requirements under the GDPR is more or less stringent and/or wider in scope than those under Singapore's Personal Data Protection Act (**PDPA**) and suggests practical steps for enabling compliance.

Does the GDPR apply to my organisation?

The GDPR has extraterritorial effect. For companies in Singapore, therefore, the starting point is to determine whether the GDPR is applicable in the first place.

It applies if your organisation processes the personal data of individuals in the EU, where the processing relates to:

(a) offering goods or services, regardless of whether payment is required, to such individuals in the EU; or

(b) monitoring the behaviour of such individuals in the EU.

For example, if your organisation sells its products to individuals in the EU (e.g. e-commerce) or monitors their behaviour (e.g. online behavioural advertising) then your organisation will be subject to the GDPR.

My company is already compliant with the PDPA. What else do we need to do?

The good news is that if your company is PDPA-compliant, you will already be a long way down the track towards being GDPR-compliant. However, there are several aspects of GDPR compliance that go beyond the requirements of the PDPA. We summarise the key requirements below.

Key

- Broadly equivalent in scope
- GDPR is slightly more stringent and/or wider in scope than PDPA
- GDPR is much more stringent and/or wider in scope than PDPA

Comparisons between GDPR and PDPA and recommended actions

Issue	Position under GDPR	Position under the PDPA	Practical steps if subject to GDPR
Types of data that are subject to the law	GDPR applies to **virtually all types of personal data**, being "any information relating to an identified or identifiable natural person."	The PDPA applies to **personal data but business contact information is exempt** from PDPA's data protection obligations. The PDPA defines personal data as "data, whether true or not, about an individual who can be identified from that data or from that data and other information to which the organisation has or is likely to have access."	— Carry out a new data mapping exercise and ensure that it takes into account GDPR's definition. — Ensure that existing documents and contract terms are broad enough to take into account GDPR's definition. — Reconsider strategy if your organisation has been relying on the PDPA exemption for business contact information.

Issue	Position under GDPR	Position under the PDPA	Practical steps if subject to GDPR
Types of organisations that are subject to the law	GDPR applies to a **broad range of entities**. It applies to both private sector and public sector entities, entities located outside the EU, and it imposes a number of direct obligations on data processors.	The PDPA applies to a **narrower range of entities**. It does not apply to public agencies or organisations acting on their behalf. Whilst the PDPA technically has extraterritorial effect, in practice, it is not actively enforced against entities located outside Singapore. Unlike GDPR, data processors have fewer direct obligations under the PDPA, i.e. they only need to comply with the security and retention requirements.	— Public agencies or organisations acting on the public agency's behalf need to determine whether they are subject to GDPR. — Organisations that typically act as processors or intermediaries need to comply with the more stringent requirements of the GDPR.
Sensitive personal data	GDPR provides extra protection for "**special categories of data**", which includes data about an individual's race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, health information as well as genetic and biometric data.	There are no **specific rules for sensitive personal data**, although guidance from the Personal Data Protection Commission (PDPC) does suggest that personal data of a sensitive nature should be accorded a higher level of protection as a matter of good practice.	— As part of a new data mapping exercise, determine if special categories of data are processed and, if so, apply the more stringent GDPR requirements, e.g. obtaining the data subject's 'explicit' consent to the processing of their sensitive personal data or limiting the processing of such data to the specific circumstances listed in GDPR.
Purpose and data minimisation	Organisations must ensure that it collects personal data for **specified, explicit and legitimate purposes** and does not further process the data in a manner that is incompatible with those purposes. The processing must also be **adequate, relevant and limited to what is necessary in relation to the purposes** for which they are processed.	Organisations should only collect, use or disclose personal data for **purposes that a reasonable person would consider appropriate** in the circumstances.	— Review policies and apply the more stringent GDPR requirements.

Issue	Position under GDPR	Position under the PDPA	Practical steps if subject to GDPR
Notice and Consent	GDPR sets a **high standard for consent**. Organisations must obtain consent in a clear, open, specific and transparent manner. The consent obtained must be unambiguous, specific, freely given, informed and given by a statement or affirmative action. In practice, this means that there must be a positive opt-in from individuals. Pre-ticked boxes or any other types of default consent are not acceptable. Consent is not the only basis for processing personal data under GDPR. There are other bases for processing data which may be better suited to your organisation's specific circumstances.	Unlike GDPR, consent is the only basis of processing under the PDPA. As a result, while the **principles on obtaining consent are the same**, the PDPA **sets out a less restrictive standard of consent** as compared to GDPR. For instance, the PDPA allows consent to be deemed if the individual voluntarily provides the personal data, or if it is reasonable that the individual would voluntarily provide the data. There are also various exceptions that allow an organisation to process personal data without consent, such as if the data is publicly available or if it is collected by a news organisation solely for its news activity.	— Determine whether consent is an appropriate basis for processing personal data under GDPR. — If relying on consent as a basis for processing personal data, review notices and consents to ensure that they meet the more stringent GDPR requirements – fine print and pre-ticked boxes are not acceptable. — Consider whether "re-permission" is required (but only where you are relying on consent as the basis for processing personal data and where GDPR-compliant consent has not already been obtained). — Notices should spell out the data subject's additional rights under GDPR – see "Rights of data subjects" below.

Issue	Position under GDPR	Position under the PDPA	Practical steps if subject to GDPR
Accuracy and completeness	Organisations must ensure that all personal data processed is **accurate**, and where necessary, kept **up to date**.	Organisations must make a reasonable effort to ensure that personal data collected by or on behalf the organisation is accurate and complete. However, unlike GDPR, this **requirement arises *only*** when the personal data is likely to be: (1) used by the organisation to **make a decision affecting the individual** to whom the personal data relates; or (2) likely to be **disclosed by the organisation to another organisation**.	— Put in place processes to ensure that the personal data processed is accurate and complete, regardless of how that personal data is used.
Data protection by design and data protection impact assessments (DPIAs)	Organisations must **integrate data protection principles as well as technical and organisational safeguards into their processing activities**, from the design stage right to the end of the activity. DPIAs help organisations to identify and reduce data protection risks in their processing activities to facilitate data protection by design. DPIAs are **mandatory where the processing likely results in a risk to the rights and freedoms of natural persons**. If the DPIA identifies a high risk, the organisation must consult the relevant regulators before it begins the processing.	There is **no express data protection by design or DPIA requirement** in the PDPA, but the PDPC considers it good practice for the organisation to conduct DPIAs and have appropriate policies and processes in place for handling personal data before its embarks on any data processing.	— Put in place policies and processes in place to ensure data protection by design. — Provide technical and development teams with training on data protection by design, and keep the relevant training records. — Carry out DPIAs for new or updated data processing projects, and keep records. — Consult with the relevant regulators if the DPIA concludes that the data processing activity is high risk.
Documenting compliance	Controllers must **maintain a record of all processing activities** under their responsibility. Processors must maintain a record of all categories of processing activities that they carry out on behalf of the controller.	An organisation must keep records on the ways it has used or disclosed personal data for at least 12 months as part of its obligation to provide individuals with access to their personal data (see page 10 below).	— Put in place processes to ensure that processing records are kept.

Issue	Position under GDPR	Position under the PDPA	Practical steps if subject to GDPR
Data processing agreements	All processors **must be contractually bound to the following**, regardless of whether the processing takes place within the EU or outside the EU: (1) process personal data only on instruction from the controller; (2) ensure that persons authorised by the processor to the personal data have committed themselves to confidentiality; (3) take all measures required to ensure the security of the personal data; (4) not engage a sub-processor without written authorisation from the controller, and if a sub-processor is engaged, the processor must ensure that its obligations flow down to the sub-processor; (5) assist the controller with the data subject requests; (6) assist the controller with data breach reporting, remediation and DPIAs; (7) delete and/or return the personal data to the controller when such data is no longer necessary to achieve the purposes of the processing (unless a statutory exception applies); and (8) make available to the controller all information necessary to demonstrate compliance with the GDPR and contribute to audits (including inspections) by the controller.	The PDPA **does not require processors to be contractually bound to a defined set of obligations** – the only exception is where personal data is transferred by the controller to a processor based outside Singapore. In practice, processors in Singapore are often subject to contractual processing terms but these rarely go as far as GDPR's requirements.	— Enter into GDPR-compliant contracts with the relevant processors whenever they are engaged to process the personal data of data subjects located in the EU. In practice, this can require a large amount of contract remediation work as appropriate contracts or data processing addenda are put in place.

Issue	Position under GDPR	Position under the PDPA	Practical steps if subject to GDPR
Data protection officer (DPO)	**All controllers and processors must appoint a DPO** if they are a public authority, or where their core activities involve the regular and systematic monitoring of data subjects on a large scale, or where they process sensitive personal data and data on criminal convictions and offences on a large scale. The DPO is responsible for: (1) informing and advising the organisation on their GDPR obligations; (2) monitoring compliance with the GDPR; (3) providing advice on DPIAs and subsequent review; (4) cooperating with and acting as the organisation's point of contact for regulators; and (5) conducting training, awareness-raising, conducting data protection audits and allocating data protection responsibilities within the organisation.	**All controllers must appoint a DPO**, regardless of the nature of the processing. Processors do not need to appoint a DPO. **Unlike GDPR, the DPO is responsible only for one task**, i.e. he or she must ensure that the organisation complies with its data protection obligations under the PDPA.	— If required, appoint a DPO (particularly if you were not required to do so under the PDPA, such as if your organisation is only a processor). — Ensure that the DPO is properly appointed in terms of mandate, position in the organisation, confidentiality and resources. — Ensure that internal governance processes require the DPO to be involved in data protection issues. — Provide information about your DPO to the regulators and on the notices on your website.
Security	Organisations must implement **appropriate technical and organisational measures** to ensure a level of security appropriate to the risk, such as pseudonymising and encrypting personal data, being able to restore availability and access to personal data timeously in the event of a data breach, and regularly testing, assessing and evaluating the effectiveness of these measures.	Organisations are required to protect personal data in its possession or under its control by making **reasonable security arrangements** to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.	— Although both the PDPA and the GDPR require that personal data is kept secure, follow guidance issued by both regulators to determine what is considered "reasonable" and appropriate" in each jurisdiction. — If you haven't already, consider pseudonymisation and/or encryption of personal data.

Issue	Position under GDPR	Position under the PDPA	Practical steps if subject to GDPR
Data breach reporting	There are **specific data breach notification obligations**. Where a data breach occurs, the organisation is required to notify regulators without undue delay, and generally no later than 72 hours, where there is a risk to the rights and freedoms of affected individuals. The organisation is also required to notify affected individuals of the breach where the risk to the rights and freedoms of affected individuals is high.	There is **no specific requirement to report data breaches**, although the PDPC strongly recommends data breaches to be reported, and its Guide to Managing Data Breaches sets out in great detail the kinds of information to be reported, the frequency and expected timelines, much of which is similar to GDPR. However, there will be amendments to the PDPA in 2018 introducing mandatory breach notification requirements. **While the amendments will bring the PDPA more in line with the GDPR, there will be differences in the threshold test to determine whether breach notification is required**. Unlike GDPR, the PDPA will require an organisation to notify regulators as soon as practicable, and generally no later than 72 hours, where the scale of the breach is significant (e.g. involving data of more than 500 people) or where there is risk of impact or harm to the affected individuals. For the latter, the organisation will also need to notify affected individuals as soon as practicable.	— Implement procedures and processes to ensure that personal data breaches are notified to the regulator within 72 hours of becoming aware of the breach. — Implement procedures and processes to ensure that personal data breaches are communicated to affected data subjects promptly where required. — Train your staff on how they should respond to data breaches, including the remedial actions that they can take and how they should handle communication with data subjects, the media and the general public. — Document all personal data breaches, including the relevant facts, effects and remedial actions taken. — Ensure that your processor contracts require processors to inform you of data breaches promptly so you can communicate the breach to the regulatory and/or affected data subjects within the stipulated timeframes.

Issue	Position under GDPR	Position under the PDPA	Practical steps if subject to GDPR
International transfers	The GDPR's international transfer obligations do not apply to transfers of personal data from Singapore to other territories. Instead, they apply to transfers of personal data from the European Economic Area (**EEA**) to other territories outside of the EEA. The transfer of personal data to territories outside the EEA is **permitted, provided that the transfer is, amongst other things**: (1) to a territory (or one or more specified sectors within the territory) that is deemed to provide an adequate level of protection; (2) made pursuant to a set of model clauses adopted or approved by the European Commission; (3) made pursuant to binding corporate rules; or (4) made to an importer who has signed up to an approved code or obtained approved certification.	Transfers of personal data from Singapore to other territories are **permitted as long as the necessary conditions are met**; for instance, if the organisation has entered into a binding contract or binding corporate rules with the transferee to ensure that the personal data will be accorded a level of protection that is comparable to the protection under the PDPA.	— If your organisation transfers personal data from within the EEA to outside of the EEA, put in place an appropriate legal mechanism (e.g. intra-group data transfer agreement following the model clauses) for doing so.

Issue	Position under GDPR	Position under the PDPA	Practical steps if subject to GDPR
Rights of data subjects	GDPR introduces additional rights for individuals, including: (1) the right to obtain access to his or her personal data (**right of access**) (2) the right to request erasure of their personal data (**right to erasure**); (3) the right to block or supress further use of his or her information by the organisation (**right to restrict processing**); (4) the right to receive their personal data in a structured, commonly used, and machine-readable format, and to request that it be transferred to another organisation (**right to data portability**); and (5) the right not to be subject to a decision based solely on automated processing which produces legal effects on or significantly affects him or her (**right to object to automated decision-making**).	Organisations must, upon request, **provide access to and/or correct** an individual's personal data.	— Update your information notices to include the required additional transparency/fair processing information, including regarding data subject rights. — Ensure your systems are set up to deal with the enhanced data subject rights (e.g. 30-day response time, data portability, processes for notifying other data recipients of erasure and restriction requests). — Ensure that processors are contractually obliged to pass on data subject requests and provide assistance with these. — Train relevant staff on responding to data subject requests, and keep training records.
Penalties for non-compliance	Depending on the nature of the non-compliance with the GDPR, an organisation can be issued with a fine of up to **€20 million or 4% of the organisation's worldwide annual revenue** (whichever is greater), or up to **€10 million or 2% of the organisation's worldwide annual revenue** (whichever is greater). Data subjects affected by a data breach can take **action against both controllers and processors** for losses and damages suffered as a result of the breach.	The PDPC can impose **fines of up to $1 million** for non-compliance with the data protection requirements in the PDPA. Unlike GDPR, data subjects affected by a data breach can only bring an **action against controllers (and not processors)** for losses and damages suffered as a result of the breach.	— Brief your board on the significantly higher fines that result from non-compliance with the GDPR. — Organisations that typically act as processors need to be aware that they may be liable to direct claims from data subjects affected by a data breach under the GDPR.

What should my organisation do next?

The good news is that the key principles of the GDPR are mostly aligned with those of the PDPA – so for most Singapore organisations, GDPR compliance will simply involve building an additional layer of protections into the organisation's privacy practices, rather than a fundamental rethink of the organisation's compliance framework.

Given that the GDPR is now already in effect, if you have not done so already you should consider as soon as possible whether or not your organisation is subject to the GDPR and, if so, what additional steps you need to take. For support in determining whether the GDPR applies and, if so, what your organisation needs to do, please contact the CMS Holborn Asia team.

Contact us

Matt Pollins
Partner, Commercial & TMT
T +65 9648 7800
E matt.pollins@cms-cmno.com

Jeremy Tan
Director, Commercial & TMT
T +65 9730 1190
E jeremy.tan@cms-holbornasia.com

Quah Pern Yi
Associate, Commercial & TMT
T +65 9770 0337
E pernyi.quah@cms-cmno.com

Loren Leung
Associate, Commercial & TMT
T +65 9631 3466
E loren.leung@cms-cmno.com

Elaina Foo
Associate, Commercial & TMT
T +65 9630 2789
E elaina.foo@cms-holbornasia.com

CMS Cameron McKenna Nabarro Olswang LLP
Cannon Place
78 Cannon Street
London EC4N 6AF

T +44 (0)20 7367 3000
F +44 (0)20 7367 2000

1807-0060685-4