

Article

Understanding PIPA: The Role and Requirements of Privacy Officers

Authors: Julie McLean, Director | Andrew Barnes, Associate | Sarah Blair, Associate

In a four-part series, Conyers continues its series on different topics relating to Bermuda's privacy legislation, including: why we need privacy legislation and its purpose, how do we prepare for PIPA and what are our rights as individuals? In this third part, Conyers discusses the role and requirements of privacy officers.

Getting ready for PIPA may seem daunting — PIPA being Bermuda's new(ish) privacy legislation, the Personal Information and Protection Act 2016. While we continue to await publication of the date that PIPA's obligations will come into force, many organisations are wisely already underway with their preparations. Someone who could, and should, be crucial to the preparatory tasks is an organisation's privacy officer. In this third part of the Conyers PIPA series, we discuss the role and requirements of this position.

Do all organisations need a privacy officer?

By way of recap, we set out some questions in the second part of the Conyers PIPA series to help establish whether or not PIPA applies to an organisation. In brief, PIPA applies to all organisations that use personal information in Bermuda where that personal information is used wholly or partly by automated means and/or forms part of a structured filing system.

If PIPA does apply to the organisation then the answer is 'yes', it must appoint a privacy officer. It is a mandatory requirement, with no exceptions.

What are the responsibilities of a privacy officer?

The privacy officer is the designated representative of the organisation for the purposes of compliance with PIPA and who will have primary responsibility for communicating with the Privacy Commissioner. These responsibilities can generally be categorised into two groups, the two 'C's: Compliance and Communication.

In terms of 'Compliance', it's the privacy officer's role to oversee the organisation's compliance with PIPA. These duties will vary depending on the organisation and what tasks are needed for compliance. The duties would ordinarily include: advising the organisation about PIPA; developing a privacy programme to ensure the organisation meets its PIPA obligations (e.g. developing procedures, policies, training and appropriate documentation); monitoring PIPA procedures to ensure continued compliance; assessing risk and determining security safeguards and evaluating overseas transfers to third parties.

In terms of 'Communication', the privacy officer will be the organisation's primary contact for the Privacy Commissioner and for the public. Their details will be set out in the organisation's privacy notice so that individuals can contact the organisation with questions and/or requests to exercise their rights under PIPA, such as an information access request (for more information about individuals' rights, see part 4 of our Conyers PIPA series). The privacy officer will need to be able to demonstrate an understanding and knowledge of the organisation's position in respect of personal information and PIPA.

Can the privacy officer delegate their duties?

Particularly if an organisation is large, the duties and responsibilities of a privacy officer may seem daunting. The good news is that PIPA specifically provides that the privacy officer may delegate his duties to one or more individuals. The officer can therefore build a team suitable for the organisation's needs. PIPA also allows for a group of organisations under common ownership and control to appoint a single officer provided they are accessible from each organisation.

Who should the privacy officer be?

In light of their obligations, the Office of the Privacy Commissioner suggests that the privacy officer should hold a position of responsibility within an organisation, “*with sufficient authority to oversee and ensure compliance with PIPA*”.

Given that their duties relate to compliance and communication, ideally the privacy officer would be someone sufficiently senior that they're authorised and empowered to lead the organisation's PIPA policy and to speak on behalf of the organisation.

Can we outsource the role of privacy officer?

In short, yes – the delegation of duties can be to an external provider. Third parties can provide ‘privacy officer services’ including, for example, providing legal or technical advice on PIPA compliance, responding and managing PIPA rights requests, managing communications with the public and/or Privacy Commissioner. However, it's important to remember that it is the organisation that will remain ultimately responsible for the duty of compliance with PIPA.

Is the privacy officer personally liable for non-compliance with PIPA?

Generally, it is the organisation that is liable for non-compliance with PIPA. However, in some circumstances, there may be personal liability for individuals — irrespective of whether they are the privacy officer or not. For example, it is an offence to wilfully or negligently use personal information in a manner that's inconsistent with PIPA and is likely to cause harm to individuals, or knowingly make a false statement, or knowingly mislead (or attempt to mislead) the Privacy Commissioner. It's therefore important that *everyone* within an organisation understands PIPA's obligations and the organisation's policies and procedures.

PIPA also provides that where a company commits an offence, a director, manager, secretary or similar officer could also be committing an offence when it is committed with their consent, connivance of, or is attributable to, any neglect on the part of that individual. It is therefore important to document the organisation's PIPA policy and procedure development and the steps taken by such individuals to ensure compliance. If anyone is uncertain about their obligations and liabilities, they should seek and obtain legal advice.

We have now discussed the background and context of PIPA, who it applies to and some of the steps an organisation can take to prepare for its implementation. Our final article will discuss an issue that has been briefly touched on in each of these articles: an individual's rights under PIPA. Understanding these rights is also critical for an organisation preparing for PIPA.

Disclaimer: Nothing in this article constitutes legal advice and is for general purposes only. If you would like to obtain legal advice on PIPA, please contact the Conyers team:

Authors:

Julie McLean

Director

julie.mclean@conyers.com

+1 441 299 4925

Andrew Barnes

Associate

andrew.barnes@conyers.com

+ 1 441 278 8054

Sarah Blair

Associate

sarah.blair@conyers.com

+ 1 441 279 5335

This article is not intended to be a substitute for legal advice or a legal opinion. It deals in broad terms only and is intended to merely provide a brief overview and give general information.

For further information please contact: media@conyers.com