

Data protection officers may have tremendous job security under [Article 38\(3\)](#) of the European Union's General Data Protection Regulation, but the job may also come with hidden risks. In some countries, DPOs – or their equivalent under local law – may be held personally liable for failing to comply with local privacy law. For example, an employment agency's sole corporate director recently pleaded guilty to a [criminal offense](#) under Hong Kong's Personal Data Privacy Ordinance, specifically for failing to respond to a summons for investigation under section 50B(1)(b) of PDPO. Although criminal prosecutions under the law are not new, this case marked the first time it has occurred for the mere failure to respond to an investigation.

In fact, a number of data protection and privacy laws around the world expose DPOs to personal civil and criminal liability under a variety of circumstances. Prospective DPOs may want to ask their employers a number of questions, addressed below, regarding how best to mitigate the risk of personal responsibility.

## Personal liability provisions under data protection laws

### 1. Canada

Canada's Anti-Spam Law ([CASL](#)) prohibits sending any "commercial electronic message" without the prior express or implied consent of the recipient. Fines are assessed by the Canada Radio Television Commission, which oversees and enforces CASL. However, a section of CASL provides for a private right of action allowing individuals and corporations to sue

alleged infringers of the law, although that section, which was due to come into force July 1, 2017, [has been suspended](#) pending parliamentary review.

Should this right come into force, it would mean that, in addition to potential statutory damages, courts will be able to order individuals held liable under CASL to pay the complainants an amount equal to their actual loss or damage. Under this law, companies' directors and officers can be found personally liable under certain provisions of CASL if they directed, authorized, assented to, acquiesced in or participated in the commission of a contravention of CASL.

### 2. Hong Kong

Hong Kong's Personal Data (Privacy) Ordinance ([PDPO](#)), overseen by Hong Kong's Privacy Commissioner for Personal Data, allows civil or criminal proceedings against any "data user" (defined as "a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data"), for a variety of offenses, including failing to acquire consent before using data in direct marketing, providing personal data to a third party without consent, providing false information to the commissioner, even failing to comply with an enforcement notice. Further, section 66 provides for compensation to "an individual who suffers damage" (including "injury to feelings") from the data user for that damage. Data subjects can even apply to the commissioner for assistance in recovering that compensation. Maximum penalties for breaches under the PDPO are fines of up to HK\$1 million (approximately U.S. \$130,000) and imprisonment for up to

five years. Notably, while an employer can be held liable in civil matters for the actions of an employee or designated third party, the law states explicitly that this is not the case in criminal matters.

### 3. Ireland

Ireland's Data Protection Act 1988, amended by the [Data Protection \(Amendment\) Act 2003](#) (and as governed by the Office of the Data Protection Commissioner (ODPC)), creates criminal liability for both the company and its officers. Personal criminal liability attaches at the individual level when an offence has been committed and the violation is found to have been committed with the director's or officer's consent or connivance and/or is attributable to any negligence on their part (see U.K. DPA for very similar language on liability). Criminal offences are subject to a maximum fine of 3,000 Euros (approximately U.S. \$3,536) for summary offences and a maximum fine of 100,000 Euros (approximately U.S. \$117,891) for indictable offences.

Because the GDPR does not expressly address personal liability for company officers or directors, those Member State laws that do create such liability may still apply after May 2018 when the GDPR comes into effect.

### 4. Malaysia

Malaysia's Personal Data Protection Act 2010 ([PDPA](#)), as governed by the Minister of the Malaysian Communications and Multimedia Commission, imposes criminal [penalties](#) for violations including fines and imprisonment. For example, a company's failure to cease using personal data for direct marketing purposes following a data subject's objection to its use could result in a fine of up to 200,000 Malaysian Ringgit (approximately U.S. \$62,800)

and/or imprisonment of up to two years. A violation of the law's cross-border restriction could result in a fine of up to 300,000 Malaysian Ringgit (approximately U.S. \$94,200) and/or imprisonment of up to two years. If a corporation violates the Act, individual officers may be charged severally or jointly in the same proceedings. The extent to which an individual can be held responsible is measured against that person's involvement in the management of the company.

### 5. Philippines

The Philippines' Data Privacy Act ([DPA](#)) of 2012, as administered and enforced by the National Privacy Commission, specifies the penalties for violations pertaining to personal information and sensitive personal information that include unauthorized processing, accessing due to negligence, improper disposal, processing for unauthorized purposes, unauthorized access or intentional breach, concealment of security breaches, malicious disclosure, and unauthorized disclosure. Violations carry potential fines ranging from 100,000 Pesos (approximately U.S. \$1985.00) to 5,000,000 Pesos, (approximately U.S. \$99,247.00), and imprisonment ranging from six months to seven years. According to the statute, "[i]f the offender is a corporation, partnership or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime."

### 6. Singapore

Singapore's Personal Data Protection Act 2012 ([PDPA](#)), enforced by the Data Protection Commission, includes rules governing the collection, use, disclosure and care of personal data and provides for the establishment of a Do Not Call Registry.

Under the [law](#), corporate officers may be personally liable with employers held vicariously liable. Violations carry potential fines of up to SING\$10,000 (approximately U.S. \$7,500) for certain offenses in relation to the Do Not Call Register and up to SING\$1 million (approximately U.S. \$7,500,000) for failure to meet general data protection obligations. Criminal liability attaches with imprisonment of one to three years under certain breaches. A private right of action also exists which could give rise to additional damages. The law applies to organizations, including “any individual, company, association or body of persons, corporate or unincorporated, whether or not: (a) formed or recognized under the law of Singapore; or (b) resident, or having an office or a place of business, in Singapore.”

## 7. United Kingdom

The United Kingdom’s Data Protection Act 1998 ([DPA](#)), allows for criminal liability for violations under the law. For example, failure to comply with an enforcement notice or providing deliberately false information is a criminal offence subject to fines that may be of an unlimited amount. When offenses under the DPA are committed by a corporation, liability can be extended to management as well. This may result in personal criminal liability if the violation is found to have been committed with director or officer consent or connivance, or be attributable to any neglect on their part.

While currently there is no personal civil liability under the statute there is [support](#) for the concept by the law’s governing body, the Information Commissioner’s Office (ICO). The support [stems](#) from a lack of ability to collect fines imposed at the corporate level due to company liquidation post violation.

## Mitigating the risk

Given the seriousness of the penalties outlined above, a DPO will want to mitigate the risk as much as feasible. One issue to explore is whether the employer’s Directors & Officers and/or Errors & Omissions insurance policies would indemnify the DPO in the case of civil liability. Exposure to criminal liability should be explored separately as the majority of insurance policies exclude coverage for criminal acts. According to the IAPP’s insurance broker, data breaches are most likely covered, if at all, under an organization’s cyber liability policy. If a cyber liability policy is in effect, coverage under the organization’s Directors & Officers and Errors & Omissions policies, at least to the extent they are addressable under the cyber policy, would likely be excluded. To the extent the D&O or E&O policy does address cyber perils (assuming they are not expressly excluded) the coverage is likely less comprehensive than what would be required to defend the claim.

After reviewing insurance coverage, a DPO will want to understand under what circumstances and for what territory coverage on the DPO’s behalf would be barred. Given the nature of electronic information exchange, the majority of cyber policies will provide coverage for claims that arise anywhere in the world. However, there may be other restrictive provisions such as exclusions based on reference to a specific statute.

Accordingly, DPOs may want to inquire whether their employers’ insurance policies provide appropriate levels of protection for the DPOs in their official capacities, given the nature and scope of duties they will be performing, and whether the employers will defend and indemnify the DPOs for all incurred costs and expenses, including legal fees, should they face civil or criminal liability.

## Appendix: Personal Liability for Privacy and Data Protection Officers

	Statute	Civil liability	Criminal liability	Penalty	Imprisonment
Canada	<a href="#">CASL</a> (Section 31, currently suspended)	"[I]f directed, authorized, assented to, acquiesced in or participated in" violation of CASL	N/A	Statutory damages and compensation for actual loss or damage	N/A
Hong Kong	<a href="#">PDPO</a>	"Subject to subsection (4), an individual who suffers damage by reason of a contravention- (a) of a requirement under this Ordinance; (b) by a data user; and (c) which relates, whether in whole or in part, to personal data of which that individual is the data subject, shall be entitled to compensation from that data user for that damage."	Data user: "a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data"  "[I]f the data is provided for gain, to a fine of \$1000000 and to imprisonment for 5 years"	Statutory damages and compensation for damage	Up to 5 years
Ireland	<a href="#">Data Protection (Amendment) ACT 2003</a> (Section 29)	N/A	"[C]ommitted with the consent or connivance of or to be attributable to any neglect on the part of a person"	Statutory Damages	N/A
Malaysia	<a href="#">PDPA</a> (Part X, Section 133)	N/A	"[W]as in any manner or to any extent responsible for the management of any of the affairs of the body corporate or was assisting in such management— (a) may be charged severally or jointly"	Statutory Damages	Up to 2 years
Philippines	<a href="#">DPA</a> (Rule XIII, Section 61)	"[T]he penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime."	"[T]he penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime."	Statutory damages	6 months -7 years
Singapore	<a href="#">PDPA</a> (Part X, 52 (1))	"Where an offence under this Act committed by a body corporate is proved (a) to have been committed with the consent or connivance of an officer; or (b) to be attributable to any neglect on his part..."	"[T]he officer as well as the body corporate shall be guilty of the offence and shall be liable to be proceeded against and punished accordingly."	Statutory damages and private right of action	1-3 years
United Kingdom	<a href="#">DPA</a> (Part VI, Section 55A)	N/A	"(a) [K]new or ought to have known (i)that there was a risk that the contravention would occur, and (ii) that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but (b) failed to take reasonable steps to prevent the contravention."	Statutory Damages	N/A