

Security breach! & Bird & Bird

A closer look from a data protection law perspective

November 2014




Gabriel Voisin (Associate)

Why is this a challenge?

- When personal data is compromised, mandatory or recommended notification requirements may apply. This means for your organisation, possible obligations to inform:
 - Competent authorities; and/or
 - Affected individuals
- If not addressed properly:
 - Possible risks of sanctions (e.g. criminal liability, fines, damages)
 - Potential impact on share price or bad publicity (e.g. Target & theft of customer data)
- It is therefore of the utmost importance to have a very practical understanding of the issue



Current legal NORAC framework

Countries	<u>General</u> breach notification regime?
	YES: well established patchwork of multiple – and sometimes conflicting – mandatory notification regimes
	YES: distinctions per province (i.e. mandatory regime in Alberta, recommended regimes elsewhere)
	YES: mandatory regime

Current legal EU framework

EU LEVEL

Only PECS (e.g. telco or ISP) are subject to data breach requirements from Directive 2002/58/EC updated by Regulation 611/2013




Keep an eye on EU developments (i.e. draft DP regulation, cyber security directive)

MS LEVEL

Possible recommended or mandatory **general** data breach requirements from member states (e.g. UK, Ireland, Germany, Belgium)

Possible **sectorial** breach requirements (e.g. financial institutions, critical infrastructure providers in France)

Sample of the legal APAC framework

Countries	<u>General</u> breach notification regime?
	NO
	YES: mandatory regime
	YES: recommended regime

What amounts to a 'breach'?

- Issue to be looked at from a country level perspective
- Any incident leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed

Practical scenarios	Breach?
Four laptop computers were stolen from the HR department...	YES
An employee has given to a third party the login and password for an account with global access read only right to the client database. Logs evidence use of the account by this third party.	YES
As above, but the data was unintelligible for the third party...	YES, but...
Inadvertently sending an email to 1,800 customers: instead of placing the addresses in the “bcc” line, the “to:” line is used...	Possibly

Timing dilemma

- Depending on the breach notification regimes applicable to your organization, different – and sometime conflicting – timing obligations may apply
- Illustrations:
 - notification within 24 hours
 - notification within 72 hours
 - notification without undue delay
- In practice, many affected organisations do not satisfy short timing notification obligations



Key things to do in case of a breach

- Involve your in-house and/or external counsel to benefit from privilege
- Think about your possible contractual obligations (e.g. providers, PCI)
- Anticipate the following questions:
 - Root cause of breach (e.g. criminal conduct, documents lost?)
 - What information was accessed?
 - Type of access = view vs. edit/download
 - Affected individuals:
 - Number of affected individuals
 - Internal only – or also external
 - Potential harm
- Roll-out your remediation plan
- Stay discrete

My 4 tips for you today

Trap/bug your
data sources

Implement a
breach policy
procedure

Meet w/ your
broker or
insurance people

Stay calm!

Questions & Bird & Bird

gabriel.voisin@twobirds.com

Follow me on Twitter: [@gvoisin](https://twitter.com/gvoisin)

Bird & Bird is an international legal practice comprising Bird & Bird LLP and its affiliated and associated businesses.

Bird & Bird LLP is a limited liability partnership, registered in England and Wales with registered number OC340318 and is authorised and regulated by the Solicitors Regulation Authority. Its registered office and principal place of business is at 15 Fetter Lane, London EC4A 1JP. A list of members of Bird & Bird LLP and of any non-members who are designated as partners, and of their respective professional qualifications, is open to inspection at that address.

twobirds.com