Financial institutions
Energy
Infrastructure, mining and commodities
Transport
Technology and innovation
Life sciences and healthcare

NORTON ROSE FULBRIGHT

cdbp Complete Data Breach Protection

Complete Data Breach Protection

Assisting insurers and their insureds manage data breaches and cyber incidents across Australia, the Asia Pacific region and globally.

An increasingly complex web of national and international laws govern the treatment of data in Australia and around the world. With its unmatched global network, Norton Rose Fulbright is ideally placed to advise on complex cyber incidents. We are strong across the key industry sectors: Financial Institutions; Energy; Infrastructure, Mining and Commodities; Transport; Technology and Innovation; and Life Sciences and Healthcare. We provide an end-to-end service offering which covers both the advisory and contentious stages of the data breach lifecycle including:

Protect

We have dedicated privacy, IT and IP lawyers who advise organisations on their data security and privacy obligations and potential cyber security risk exposures including:

- conducting digital risk audits – advising on the best way to collect, store and dispose of data
- incident response readiness – preparing organisations for data breach incidents includingdeveloping tailored incident response plans
- cross-border data flows – advising on cross-border data transfers
- IT vendor risks – advising on third party contractual arrangements including IT outsourcing, cloudcomputing and data analytics
- regulatory risks – advising on regulatory obligations, risks and penalties.

Respond

As 'breach coach' we work with you to provide a streamlined incident response service across a range of incident types, including data breach and network interruption.

We coordinate the entire response by assessing the size and nature of the incident, taking steps to contain it, coordinating our panel of carefully selected third party vendors, all the while managing stakeholders' interests and mitigating potential loss.

Our early involvement and establishment of legal professional privilege protects you to the maximum extent possible as far as sensitive communications are concerned.

Recover

Following containment of an incident, we take steps to reduce potential harm and respond to any fallout.

We help you manage notification to affected parties, law enforcement and regulatory bodies; coordinate credit monitoring and ID protection services; and respond to any media coverage.

We can also act in defence of your organisation and its directors and officers in third party liability claims and regulatory or PCI investigations. Our end-to-end capabilities mean we are best placed to understand how the breach, investigation, response, remediation and notification aspects will impact on litigation. We also advise on recovery options.

NORTON ROSE FULBRIGHT

Pre-Incident Services at a Glance

As part of our Complete Data Breach Protection service offering, we have developed four global best practice cyber risk management packages to help organisations address cyber risks, and prepare for and respond to incidents as follows:

Cyber-security contract terms – Vendor Management Framework	Where IT service providers and vendors have access to your data or supply systems or facilities on which your data is stored, it is essential to manage the data risk with detailed contractual terms. The centrepiece of this framework is the template Vendor Data Security Schedule which sets out cutting-edge data security provisions. The Vendor Data Security Schedule is designed to be customised by your in-house team with the assistance of other documents in the framework including an annotated guide, a set of negotiating points and an FAQ schedule.
IT Incident Response Plan Package	This package contains a detailed methodology to guide your in-house team in coordinating and preparing an IT incident response plan. These plans can dramatically reduce the potential costs and liabilities of a data breach. The package also includes a template Data Breach Response Plan as the starting point for your own plan.
Data Breach Response Tabletop Exercise	We work with your organisation to conduct a simulated data breach in order to reveal risks and organisational blind spots relating to data breaches. Your organisation can then address those issues, before a real breach occurs.
Mandatory Data Breach Reporting Package	The Australian government has passed new laws requiring mandatory notification of serious data breaches where the breaches involve personal information. Our package will help your organisation get ready for those new laws and to act as a critical resource if a breach occurs. The package includes an explanation of the new laws, a notification checklist and template notification letters.

CDBP Key Australian Contacts

Tricia Hobson
Partner and Chairman, Head of Insurance for Asia Pacific
Sydney
Tel +61 2 9330 8609
tricia.hobson@nortonrosefulbright.com

Jacques Jacobs
Partner, Insurance
Sydney
Tel +61 2 9330 8156
jacques.jacobs@nortonrosefulbright.com

Nick Abrahams
Partner, Global Head of Technology & Innovation
Sydney
Tel +61 2 9330 8312
nick.abrahams@nortonrosefulbright.com

Matthew Ellis
Partner, Insurance
Melbourne
Tel +61 3 8686 6329
matt.ellis@nortonrosefulbright.com

Bernard O'Shea
Partner, Technology
Melbourne
Tel +61 3 8686 6573
bernard.oshea@nortonrosefulbright.com

Jim Lennon
Special Counsel, Technology
Sydney
Tel +61 2 9330 8426
jim.lennon@nortonrosefulbright.com