## Data breaches, privacy leaks, sensitive personal information falling into the wrong hands…

Why do these things happen even with the existence of data protection laws, with hefty fines as punishment? And why do they happen even in organisations that have instituted all the policies and procedures required by the law?

Because privacy breaches can happen *despite* legal compliance and good information governance. They happen because of failures in *operational* compliance.

So how do you avoid privacy breaches happening to you?

Drawing on a wealth of real-life case studies and onsite data protection audits, **99 PRIVACY BREACHES TO BEWARE OF** investigates the range of things that can easily go wrong on the ground – and indeed *have* gone wrong!

From careless practices and indiscreet communications to IT vulnerabilities and third-party risks, this book shows you where the weakest links are in the collection, usage, retention, disclosure and disposal of personal data.

Authors Kevin Shepherdson, William Hioe and Lyn Boxall have consulted with over 100 companies internationally in the area of data protection compliance. Their combined experience in technology, management and law give this book exceptional breadth and depth.

With action checklists in every chapter, you will be able to put theory into practice right away, and avoid operational lapses that compromise the security and integrity of personal data under your care.

The authors are members of

DPEX
DATA PROTECTION EXCELLENCE NETWORK

visit our website at:
www.marshallcavendish.com/genref

Marshall Cavendish Business

BUSINESS
ISBN 978-981-4794-64-0
9 789814 794640

Kevin Shepherdson
William Hioe & Lyn Boxall

99 PRIVACY BREACHES TO BEWARE OF
Practical Data Protection Tips from Real-Life Experiences

Marshall Cavendish Business

UPDATED FOR TECHNOLOGY DEVELOPMENTS AND THE GDPR

# 99 PRIVACY BREACHES TO BEWARE OF

## Practical Data Protection Tips from Real-Life Experiences

"99 chapters that will help you develop all the procedures you need to prevent data breaches – without having to read all the legislation"

**Wojciech R. Wiewiórowski**
European Data Protection Assistant Supervisor

"an authoritative guide … by experts with deep practical experience"

**Prof. Ang Peng Hwa**
Nanyang Technological University, Singapore

"excellent … delves into privacy at a granular level, providing structured guidance"

**Terry McQuay** CIPP CIPM
President, Nymity Inc.

**Kevin Shepherdson**
**William Hioe & Lyn Boxall**

"Today, an increasing number of jurisdictions require notification of data breaches to relevant supervisory authorities. The details of the laws differ widely, but the mistakes that lead to breaches are the same wherever they happen – for example, you had a 'bad day' and clicked the wrong button, giving an employee's ex-wife access to his health data, or you accidentally sent the data of one of your students to 1,900 parents. The authors have gathered hundreds of hints in 99 chapters that will help you develop all the procedures you need to avoid data breaches – without having to read all the legislation."

**— Wojciech R. Wiewiórowski, Assistant Supervisor, European Data Protection**

"This book is exceptional on a number of levels. Well-written and logically constructed, it draws upon the experience of the authors to provide a roadmap for addressing day-to-day privacy issues at a pragmatic level. The book is directed primarily at people in business who have a responsibility for handling information, and provides direction in the form of guidelines, checklists and practical examples. Although aimed primarily at laypersons, lawyers will also find this book extremely useful as a means of advising their clients as to how best to achieve legal compliance. The book is quite unique in the approach it adopts, and should prove to be an invaluable addition to the library of anyone involved in – or even just interested in – the adoption of best practice in the handling of data in the 'information age'."

**— Gordon Hughes, Partner, Davies Collison Cave, Melbourne, author of *Data Protection in Australia*, and co-author of *Private Life in a Digital World***

"Finally, a book focusing on operational practice, rather than the law, has been written. It has been long awaited! I am delighted that the authors have decided to share the wide experiences they have in this new area of IT practice and information governance. I wholeheartedly endorse this comprehensive and practical effort and hope it will become the standard bible for data protection practices not just in Singapore, but in Asia too!"

**— Dr Toh See Kiat, veteran lawyer in Data Protection, Intellectual Property Rights, Information Technology and E-commerce Law, and former Member of Parliament of Singapore**

"Much has been written previously for compliance officers, privacy professionals and lawyers about data protection laws in Singapore, Malaysia and the region. But this handbook is for the layperson – easy to read and practical. It fills in many gaps and answers many questions about how to comply with the law as well as the do's and don'ts in day-to-day business operations. Now that I've seen it, I wonder why something like this wasn't produced years ago. There is now no reason why anyone involved in processing personal data should say that they don't know what to do to protect the personal information of those under their care."

**— Professor Abu Bakar Munir, author of *Data Protection Law in Asia*, Professor of Law, University of Malaya, and Associate Fellow at the Malaysian Centre for Regulatory Studies (UMCoRS)**

"This book achieves a rare feat: making personal data protection practical, understandable and actionable. It is a valuable resource for marketers at all levels, and we recommend it as a reference to all our members."

**— Lisa Watson, Chairman, Direct Marketing Association of Singapore**

"In this book, Shepherdson, Hioe and Boxall do three things very well. First, they focus on the very important topic of personal data protection and data privacy, and clarify how data protection, information security and data privacy protection are interrelated. Second, they explain data protection and privacy in the context of how real-world organisations actually function and how people get their work done on a day-to-day basis. This makes it easy for any type of administrator, professional, manager or executive to understand the contents of this book and relate to it. Third, from the perspective of education, learning and cognition, this book is designed in a very clever way so that it is delightfully fast and easy to find exactly what you are looking for, and to grasp what you need to understand about whatever specific aspect of data protection and privacy you need to clarify. As such, this book can be used as a handy 'on-demand' reference at the time of need. Or, you can read it cover to cover, and then keep referring to the relevant chapters 'on-demand' as the need arises."

**— Professor Steven Miller, Dean, School of Information Systems, Singapore Management University**

"As discussed in this book, taking an operational compliance approach is the responsible and most effective approach to achieve ongoing and demonstrable compliance while minimising the chances of a breach. This book provides an excellent review of privacy by looking at the principles of privacy from the perspective of an information life cycle. This perspective provides a structure to enable truly practical guidance, and as you can ascertain from the title of the book, it delves into privacy at a granular level, providing structured guidance to privacy professionals."

**— Terry McQuay, CIPP, CIPM, President, Nymity Inc.**

"This book helps provide real-life illustrations to walk business leaders through the choices they will have to make in designing their products, services and processes whilst keeping privacy in mind. As 'being reasonable' is one of the requirements in the PDPA (Personal Data Protection Act), it is no longer just about obtaining consent, but knowing how to properly balance privacy obligations with business desires."

**— Ken Chia, Principal, Baker McKenzie.Wong & Leow**

"This book provides practical solutions to the current global privacy challenges. I recommend it to both experienced practitioners and those new to implementing privacy programmes."

**— Patricia Adusei Poku, Executive Director, Data Protection Commission, Ghana**

"With new chapters relating to technological developments in particular, this second book of the same series provides even more comprehensive coverage and analysis of data protection breaches and cases in many of the important aspects of our lives. Written for the layman and presented in a professional manner, this book is a very handy and practical reference that readers will find relatable and useful. I have the pleasure of congratulating the authors on this further achievement in their admirable mission to promote the importance of personal data privacy protection as a business culture. "

**— Stephen Kai-yi Wong, Privacy Commissioner for Personal Data, Hong Kong, China**

# 99 PRIVACY BREACHES TO BEWARE OF

Practical Data Protection Tips
from Real-Life Experiences

**Kevin Shepherdson**
**William Hioe & Lyn Boxall**

Marshall Cavendish Business

Reprinted 2020

Published in 2018 by Marshall Cavendish Business
An imprint of Marshall Cavendish International

A member of the
Times Publishing Group

In association with Straits Interactive Pte Ltd




Other Marshall Cavendish Offices:
Marshall Cavendish Corporation, 99 White Plains Road, Tarrytown NY 10591–9001, USA • Marshall Cavendish International (Thailand) Co Ltd, 253 Asoke, 12th Flr, Sukhumvit 21 Road, Klongtoey Nua, Wattana, Bangkok 10110, Thailand • Marshall Cavendish (Malaysia) Sdn Bhd, Times Subang, Lot 46, Subang Hi-Tech Industrial Park, Batu Tiga, 40000 Shah Alam, Selangor Darul Ehsan, Malaysia.

Marshall Cavendish is a registered trademark of Times Publishing Limited

**National Library Board, Singapore Cataloguing-in-Publication Data**

Name(s): Shepherdson, Kevin Linus. | Hioe, William, author. | Boxall, Lyn, author.
Title: 99 privacy breaches to beware of : Practical data protection tips from real-life experiences / Kevin Shepherdson, William Hioe & Lyn Boxall.
Description: Singapore : Marshall Cavendish Business, 2018. | Includes index.
Identifier(s): OCN 1043907341 | ISBN 978-981-4794-64-0 (paperback)
Subject(s): LCSH: Data protection. | Business–Data processing–Security measures. | Computer security.
Classification: DDC 658.478--dc23

Printed in Singapore

# Contents

**Section F:**

## Security, Storage, Retention & Disposal of Personal Data

**Section G:**

## Disclosure of Personal Data



**Section H:**

## New Areas, Developments and Technological Concerns

# Foreword

by Commissioner Raymund E. Liboro,
Philippine National Privacy Commission

I take pleasure in being invited to write this foreword; Kevin, after all, is not only a friend, but a fellow scholar and advocate whom I look up to, and to whom I owe a debt of gratitude for his help – directly and indirectly – in enriching my understanding of privacy.

The Philippine Data Privacy Law was enacted only in 2012. Late to the party as we were, one can imagine furthermore how its concepts would be slow to pick up among the Filipino public. My country, after all, is famous for its openness. This openness is a necessary byproduct of our warm and hospitable nature.

But while it is only fair for every culture to preserve the touchstones of its identity, it would also be dangerous to remain unaware of the threats that have emerged as technology progresses. As they say, we are at an age when information is the new oil. Along with the increased value attached to information come those who would try to exploit every avenue to obtain it, often through unscrupulous means.

Such was the context within which I found myself as I took the reins of the Philippine National Privacy Commission in early 2016. We were a nascent government organisation, and nascent too was the concept of privacy in the Philippines. Those who could purchase or order books from abroad had a distinct advantage; for many who wanted to learn about data privacy, the previous edition of this book was the only available resource on breaches available in Manila.

But even then, though, perhaps our local data scholars and advocates of data privacy and security should consider themselves fortunate. *88*

*Privacy Breaches to Beware Of* provided the sector with an invaluable resource as the country joined the rest of the world in institutionalising privacy rights and concepts.

This book remains an important work, and it was an integral fount of information as we at the NPC strived to elevate the level of public discourse on privacy in the country. It would not be an exaggeration to say that we have come a long way in terms of enlightening our citizens. Aside from our regular memorandum circulars and dialogues with relevant sectors, the NPC has also been constantly crafting materials for the consumption of the greater public. From advertisements to awareness drives; from statements and columns to social media advocacies; from simplified guidelines to a comprehensive privacy toolkit, we have considered it among our primary imperatives to educate our fellow Filipinos on their privacy rights and what they and society as large must do to uphold these; on the risks that we expose ourselves to if we misappreciate the value of privacy; and on the resiliency mindset required to prevent and manage these risks. As I said in recent talk, "Gone are the days when it was seen as an isolated aspect; perhaps for the first time, boardrooms are having discussions on issues that were once limited to server room banter. Company hierarchies are recognising the importance of their IT departments. From being merely support groups called on to fix the WiFi or the printer, they now have a chance to spearhead efforts that affect the very survival of your company."

A sea-change, indeed, is sweeping over the way our public approaches the discourse on privacy. For this, we owe a debt to resources such as *88 Privacy Breaches*, which gave us a reliable backbone in terms of both the knowledge it shared, and its approach to communication. It was in-depth and comprehensive; it was clear without oversimplifying; it respected and articulated the complexities of the material without resorting to opaque and hypertechnical language. Most importantly, it was useful.

We all trace the genesis of modern information privacy rights to US Supreme Court Justice Louis Brandeis' treatise on "The Right to Privacy," and privacy laws the world over credit the OECD and

European Union's Directive 95/46/EC as an originating framework. For sure, this book you hold now will be remembered in the coming generations as another seminal work, contributing to the growing reservoir of knowledge on data privacy and security, and providing a solid foundation for the constant forward movement of global discourse.

# Preface

Until the Facebook–Cambridge Analytica breach report in March 2018, most of the highly publicised data privacy breaches in the news involved cyber-attacks. Suddenly, there was a massive privacy breach where no data was hacked. Instead, it involved the unauthorised disclosure and inappropriate sharing of personal information involving up to 87 million Facebook users.

Following Facebook's apology amid the public outcry and a falling stock price, the whole world woke up to the importance of privacy and trust in the organisations that hold our personal information.

Privacy is now a must in today's data-sharing economy and technological age.

We wrote *88 Privacy Breaches to Beware Of* back in early 2016. We drew on our experience consulting on data protection implementation programmes with a wide range of organisations in Singapore. We took lessons from enforcement cases around the world, such as in Australia, Hong Kong, Ireland and the United Kingdom, too. We wanted to show that at each phase of the information life cycle – whenever an organisation collects, uses, discloses or stores any personal data – there are many ways it can get into trouble with data protection / privacy laws.

In early 2016, the data protection obligations in Singapore's Personal Data Protection Act (PDPA) had been in force for a little more than 18 months, since 2 July 2014. Shortly after the book was published, the Personal Data Protection Commission of Singapore (PDPC) published

its first enforcement decisions. It has continued to do so quite regularly since then, with around 50 enforcement decisions now. And almost from the start, we saw the organisations that were either fined or warned by the PDPC doing the same things we had highlighted and warned about in our book as common potential privacy breaches to be aware of.

We can't claim to have been particularly prescient: in many cases there isn't a great deal of difference between the things that have gone wrong in Singapore since July 2014 and the things that have been going wrong for years in other jurisdictions where data protection / privacy legislation has been in place for many years. In Singapore, as elsewhere, failure to protect personal data is a significant factor, if not the main factor, in the majority of cases. The high-profile cases that get media attention are only the tip of the iceberg.

By late 2017, we decided we should update *88 Privacy Breaches*. As we started to think through how that might best be done, what we should cover in a second edition, we were surprised to realise how much difference a mere two years had made in the data protection / privacy environment.

Technology that was just coming into existence and beginning to display signs of future potential in late 2015 had become mainstream, or was well on its way to becoming mainstream, by late 2017. Smart devices and the Internet of Things (IoT) was accelerating its pace; mobile apps were more prolific than ever before; artificial intelligence was being applied in a range of situations; social media sites and start-ups continued to push the boundaries of these privacy-invasive technologies; and, unfortunately but not surprisingly, data breaches continued to proliferate, culminating with the Facebook–Cambridge Analytica privacy breach.

In mid-2018, with the General Data Protection Regulation now in force (as of 25 May 2018), we expect to see more privacy breaches by organisations – whether done deliberately or not – coming under the spotlight, as well as a renewed focus on regulatory activity in the EU.

In fact, publicity around technological and privacy issues debated in the context of the development and approval of the GDPR have

perhaps been catalysts for regulatory developments in various countries outside the EU. We are now seeing data protection / privacy laws introduced into, or enforced more vigorously in, an increasing number of countries; breach notification laws are becoming more common; and the requirement for organisations to appoint a Data Protection Officer is heading towards becoming a baseline regulatory requirement.

Consequently, *88 Privacy Breaches* has become *99 Privacy Breaches*, not so much by adding 11 new areas covering privacy breaches, but by painting a broader landscape reflecting technological and regulatory developments to be aware of around data protection / privacy.

June 2018

# 99 PRIVACY BREACHES TO BEWARE OF

# Introduction

Two good friends walked into a local tour agency to book a cruise holiday for their respective families. They were puzzled that they had to scan in their national identity cards to obtain a queue number. While waiting for their queue number to be called, they could hear distinctly a customer service officer (CSO) taking a customer's booking over the phone and confirming the customer's personal particulars in a very loud voice. They were quite sure everyone else in the waiting area could hear what the CSO had just said. When their turn came, they walked towards the assigned counter and sat opposite the CSO, who greeted them with a standard scripted message.

When the two friends asked why their national identity cards were required to obtain a queue number, the CSO replied that it was the standard company policy for record purposes. They were even more shocked to see personal data, credit card slips and cheques of previous customers strewn all over the CSO's work area. The CSO then asked them which cruise packages they were interested in. As they were not quite familiar with what the tour agency could offer, they asked the CSO to recommend some of the more popular ones.

"We have a mobile app that gives you great recommendations," the CSO replied, and proceeded to help them with the download of the application to their smartphones.

The two friends were both certified privacy professionals and before downloading the application they proceeded to read the application's privacy policy and permission details. They were horrified to find that the app requested multiple permissions to access their phone's

device ID, camera, microphone, app history, detailed location, and contacts. This was inconsistent with the information in the privacy policy, which did not state the purposes for which the app required all these permissions. The two friends felt that such access to the personal information in their devices was excessive and not proportionate to what was needed by a simple travel guide application.

"It's OK," said the two friends. "We will forgo the app. How about you tell us which are the popular packages from your own experience?"

Imagine their horror when the CSO turned her computer terminal around and showed them the records of past customers who had booked the most popular cruises! The two friends shook their heads and whispered to each other: "This tour agency has not taken appropriate measures to handle and safeguard the privacy of their customers' personal data. We don't trust our personal data with them. Who else will they share our data with without informing us or getting our consent? Let's go and look for a more privacy-conscious agency."

Such a scenario is real and has happened. In a number of countries, the level of awareness among organisations and individuals with regard to the proper handling and protection of personal data is still low. Even in countries with data protection or privacy laws in existence for many years, we hear in the media of massive data breaches where thousands or even millions of individuals' personal records have been compromised. Where data protection or privacy laws are relatively new, the level of awareness among organisations is often even more wanting.

In either case, not only do these organisations have to face the penalties imposed by regulators and lawsuits from affected individuals, they also have to live with financial and reputational losses. These can be particularly damaging for organisations that do not have the financial resources or a deep pool of loyal customers to help them weather the storm while they rebuild trust among their stakeholders. Organisations should therefore recognise that regardless of their size or the industry sector they are in, they are all vulnerable to privacy breaches if they do not have proper data protection practices.

Faced with high-profile regulatory actions and multi-million-dollar fines and lawsuits, many organisations around the world today are forced to strengthen their data protection practices. Similarly, when

they consider the adverse implications, particularly in terms of stakeholder trust, of even a limited privacy breach, many organisations choose to strengthen their data protection practices simply because it is a sensible way for them to conduct their business.

Governments are reviewing and revamping their data protection laws to address new challenges because of emerging technologies and to require organisations to treat data protection as one of their critical business functions.

For example, the European Union has responded to privacy concerns arising from today's digital revolution and the need to deal with the complexity of data by implementing the General Data Protection Regulation (GDPR), a single unifying data protection law across all its member countries that came into force on 25 May 2018. In China, the Personal Information Security Specification similarly deals with such privacy concerns and came into effect on 1 May 2018.

In the Association of South-East Asian Nations (ASEAN), all the member governments have committed to legislating and implementing data protection laws in their respective countries. This is part of the establishment of the ASEAN Economic Community, an effort to integrate the region's diverse economies into a single market with free movement of goods, services, investments, skilled labour and freer flow of capital.

India, after its Supreme Court held in August 2017 that privacy is a fundamental right of each of its 1.3 billion citizens, has extensive privacy regulations under development that may become law as soon as late 2018 or early 2019.

In short, virtually every organisation doing business in the European Union, China, India or ASEAN will sooner or later have to grapple with new or updated data protection laws. So must boards, senior management and employees generally. They must either press the reset button with regard to legal compliance or adopt a new mindset in terms of processing personal data as part of their everyday operations.

We need to move from the "What" to the "How" of data protection. Unfortunately, there are few, if any, books that go into the operational aspects of data privacy and protection, and uncover the operational risks, threats and vulnerabilities facing organisations.

Data protection and privacy must not be a mystery, especially to employees at the operational forefront of organisations. Operationally, they must not be something that only lawyers can understand. They must be "owned" by all employees of organisations.

### About data protection and privacy

Data protection and privacy have different ideological roots – human rights and economics – but share many of the same sets of obligations or principles, although they may be expressed in different language or use different terms (see Glossary).

We are often asked: "What's the practical difference between data protection and privacy?"

In the U.S. the term "privacy" is used in policies, laws and regulations while in the EU and many other countries, the term "data protection" often identifies privacy-related laws and regulations. Hence, there is no difference of definition between a privacy law and a data protection law, or between a privacy policy and a data protection policy, which we often come across in the online world. From a privacy professional perspective, they are synonymous.

"Data protection" may be used to mean "information security". When there is a data breach – when there is a media report, for example, about payment card information being stolen or other customer information being stolen from a company – that is a failure to protect data. The data might be "personal data" or "personal information" about individuals or it might be confidential data such as an organisation's intellectual property or other business information.

Colloquially, a data breach occurs when someone hacks into a computer system and steals data. This is well known. Newspapers are full of stories about hacking. But a data breach also occurs when data is leaked or exposed in some other way. Classic examples include individuals leaving a file behind on public transport or in a café. Other examples include employees simply sharing data with their colleagues who do not have a right to see it and individuals speaking loudly in public places and being overheard by others.

As for privacy, it has been described broadly as the right to be left alone or freedom from interference or intrusion. Data privacy or

information privacy is the right of individuals to have some control over how their personal data – data that identifies them or relates to them – or personal information about them is collected, used and disclosed, as well as how it is stored or disposed of. When it comes to data privacy or data protection laws, the term refers to rules and practices regarding the handling of personal information or personal data, such as the concepts of notice, consent, choice, purpose, security, etc.

A data breach that involves a theft of personal data or an inadvertent exposure of personal data intrudes into an individual's privacy. But an intrusion into an individual's privacy can occur without a data breach, such as where an organisation insists on collecting excessive personal data from individuals or retains their personal data for longer than is justifiable.

Hence, in this book, when we use the term "privacy breaches", we mean more than data breaches, where there could be non-compliance or contravention of the data protection law.

### About information security and privacy

Another question people have often asked is: "What's the difference between information security and privacy?"

Although the two concepts are different in certain aspects, there is a symbiotic relationship between them. Privacy practitioners have recognised that there can be no privacy without security.

Information security is concerned with three main elements: confidentiality, integrity and availability, or "CIA" for short. In a nutshell, it means that secure measures must be put in place to protect personal data and other confidential information from being stolen, or from being accessed or modified without proper authorisation. Users of personal data and other confidential information must trust its accuracy and currency to make timely decisions or to handle business transactions. And the right information must be available to the right person at the right time.

Designing information security systems without privacy in mind could result in treating all personal data and other confidential information in the same manner. But from the privacy perspective,

some personal data and other confidential information are private, especially sensitive personal data such as health, financial, ethnic group, religious or political affiliations, or membership of trade unions. Such sensitive data, in particular, must be accessible only to people with the appropriate "need to know". Hence information security systems must be designed to allow/restrict access to users based on their job roles. They must also be designed to have different levels of security for different classes of personal data and other confidential information.

While information security is about "CIA", data privacy is about having rules that govern how personal data is collected, used, disclosed and stored. Data protection laws around the world have obligations or principles to which organisations are required to adhere. If they don't, enforcement actions can be taken, resulting in either a fine or imprisonment. When organisations fail to comply with these rules, whether they simply flout them or fail to abide by them despite their best efforts, we call this a privacy breach.

Therefore, while information security is about governing "unauthorised" access to information (which includes personal data), conversely, it can be said that data privacy is about governing "authorised" access to information that is personal data. However, there can be a privacy breach even when an individual is authorised to access that personal data. For example, the individual could have illegally collected the personal data, or could have legally collected it and later used it for some other unauthorised secondary purpose, or could have illegally disclosed it to a third-party. In addition, while processing it, the individual may have failed to protect the personal data, resulting in the data being exposed, leaked, lost or even stolen.

To prevent privacy breaches, organisations should put practical measures in place to ensure information security. The measures should not be an afterthought. "Privacy by Design", a movement that originated in Canada, is now gaining wide acceptance and traction around the world and is also a requirement under the GDPR. Privacy professionals are working closely with information security professionals and IT developers to build privacy elements into IT and information security systems upfront during the design stage.

### The importance of operational compliance

Search for any obligation under a data protection law or principle under a privacy law and you'll be rewarded with an array of results about what the law means and what must be done to comply with it – from a legal perspective. But legal compliance alone is not enough. Check the enforcement cases made available by the regulators in Australia, Hong Kong, Ireland, Singapore and the United Kingdom, and you will notice that most if not all of these breaches happened because of operational lapses.

Search for "data breach" and you'll be rewarded with an array of results about hackers cleverly infiltrating corporate IT systems and stealing personal data and other confidential information. Read behind the scenes and more often than not the root cause was the action or inaction of an employee or ex-employee, sometimes careless and sometimes malicious. While more often than not the malicious employee or ex-employee succeeds only because of negligence in their IT system's governance, it is also clear that IT system governance alone is not enough.

One of our main motivations in writing this book is to fill the gap between legal compliance (complying with the obligations and requirements of data protection laws through organisational policies) and operational compliance (embedding privacy practices in the everyday operations and processes of the organisation).

While legal compliance is obviously necessary, it is not sufficient. All employees in an organisation must know at a very practical level – at an operational level – what to do and what not to do when they handle personal data and other confidential information on a day-to-day basis.

In addition, third-parties such as suppliers, vendors, intermediaries, brokers and agents must know what to do and not do when they handle personal data or other confidential information on behalf of an organisation.

In short, everyone who has a part in handling personal data or other confidential information in the possession or under the control of an organisation must understand their individual roles, responsibilities and accountabilities – at a practical level – throughout the information life cycle.

### Responsibility and accountability

As we wrote, we were reminded of the so-called Parable of Responsibility: "Everybody, Somebody, Anybody and Nobody were members of a group. There was an important job to be done and Everybody was asked to do it. Everybody was sure that Somebody would do it. Anybody would have done it, but Nobody did it. Somebody got angry because it was Everybody's job. Everybody thought Anybody would do it, but Nobody realised that Anybody wouldn't do it. It ended up that Everybody blamed Somebody, when Nobody did what Anybody could have done."[1]

Responsibility can be shared and can be assigned before or after an event. So, a lawyer can be assigned responsibility for legal compliance with the data protection/privacy law; an IT specialist can be assigned responsibility for technical systems compliance. Someone else can even be assigned responsibility for management of physical documents and other non-technical tasks. But none of this responsibility is worth anything unless individuals are accountable for their actions or inaction.

In fact, when an organisation gets into trouble under the data protection law, including as a result of a complaint by an individual, regulators will inevitably require the organisation to demonstrate accountability for compliance with it. Simply put, they will be looking for responsibility and ownership and they will require evidence of it.

Accountability applies only after something is done or not done. If an individual is accountable for something they are also answerable ultimately for it. There needs to be ownership in order for somebody to be responsible. We have written here about what individuals need to do or not do personally or what they need to do or not do as employees of an organisation.

Organisations, on the other hand, need to document their policies and practices to guide the actions of their employees. In addition, inevitably they have to provide evidence to the regulator, such as training records or disciplinary actions. Regulators will inevitably require them to demonstrate that they have done everything practically possible to prevent any privacy breaches from happening.

[1] Condensed version of Charles Osgood's "A Poem About Responsibility".

For these reasons, in this book we have provided checklists of good practices for both individuals and organisations. We intend these checklists to be a good starting place for operational compliance – both individuals and organisations should look at them through the lens of the practical situation they are facing and their own specific circumstances and supplement them appropriately to meet that situation and those circumstances.

In short, everyone must be accountable for operational compliance or nothing else matters. Without this, the blame game starts when someone gets into trouble, and lots of time and productivity is lost.

### Thrust of this book

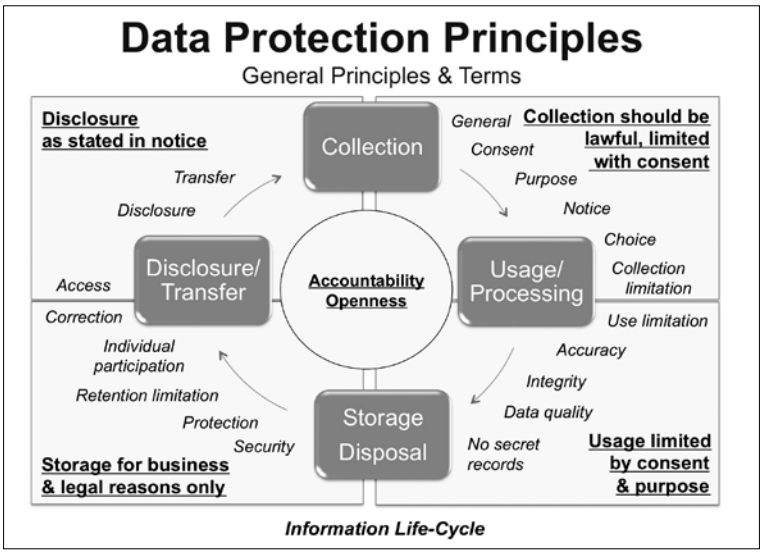
The majority of the chapters in this book are based on our real-life experiences, either in our personal capacities or as consultants and advisers to organisations that collect, use, disclose and store personal data.

We notice in our work with clients that everyday privacy breaches, in particular, happen despite legal compliance and despite good IT system governance. They happen because of a failure in operational compliance. We notice the same thing when we read reports about regulatory action around the world – files being left on a bus or in a café, USB drives being lost in taxis and so on.

So we set out to write about operational compliance – to highlight the things that can easily go wrong operationally when an organisation seeks to comply with data protection/privacy laws. And to write it in a way that speaks to our readers, that assumes they are not lawyers or IT geeks – though we certainly welcome lawyers and IT geeks as readers. We think they'll find value too.

We have included good practices based on our experiences and observations. We do not intend to be either prescriptive or all-encompassing. Every situation is different. Organisations should evaluate how our suggested good practices should be tailored to their unique circumstances, including organisational context and culture.

This book is meant for everyone who has an interest in data protection and privacy, either as an employee of an organisation or as an individual or member of the general public.




Data protection officers, especially, will benefit from the real-life anecdotes we cite, including cases of failure to comply with data protection laws that result in regulatory action. The subsequent penalties, even where the case is settled between the organisation and the regulator, provide salutary lessons. On top of the penalties, organisations incur considerable management time and expense – the diversion of resources from "getting on with business" – as part of the regulatory investigation, even where a complaint turns out to be frivolous.

Individuals who handle personal data and other confidential information in their day-to-day operations, such as real estate agents, financial advisers, healthcare workers, salespersons, freelancers or those working in service industries, will find this book useful.

Individuals who provide or disclose their personal data to organisations will become more aware of what they should or should not do in different circumstances.

### Structure of this book

We have looked at operational compliance with data protection/privacy laws through several broad categories, particularly with reference to

the information life cycle of collection, usage, disclosure, storage and retention, and disposal or destruction of personal data. The principles under each of these stages of the information life cycle are broad and generic enough to be applicable to most jurisdictions:

- **Section A: Governance & Information Asset Management.** These chapters (1 to 7) deal with some broad matters that apply generally to data protection and privacy.

- **Section B: Collection of Personal Data** (chapters 8 to 27). The over-riding principle is that the collection of personal data should be lawful, limited with consent. The principle of consent includes organisations notifying individuals at the time of collection of the purposes for collecting their personal data. It gives individuals the choice of consenting to organisations collecting their personal data or withholding their consent – an organisation must not coerce or force consent. The principle also gives individuals the right, having given their consent, to later withdraw it if they wish to do so. The organisation cannot change the purposes for which it will use personal data unless it gets fresh consent from the individual.

- **Section C: Usage of Personal Data** (chapters 28 to 39). This section deals with the usage or processing of personal data, which is limited by the purpose notified to the individual and the consent the individual gives subsequently. (There are some instances where the law allows collection, use or disclosure of personal data without consent. These are beyond the scope of this book.) Elements of usage or processing of personal data include a requirement for usage to be fair.

- **Section D: Data Accuracy & Integrity.** Organisations may store personal data about individuals, but must ensure its accuracy and integrity. The rights of an individual to have access to their personal data and to correct error and omissions, as well as the organisation's obligation regarding accuracy of personal data, are the subject of chapters 40 to 48.

- **Section E: Physical & Environmental Security.** All personal data in the care of organisations should be protected and this includes both securing it physically and ensuring a secure environment. Physical and environmental security are covered in chapters 49 to 53.

- **Section F: Security, Storage, Retention & Disposal of Personal Data.** Organisations must protect personal data too and must not retain it for longer than is necessary for the relevant use. We cover protection of personal data and retention – or, more accurately, the requirement for an organisation to cease to retain personal data – in chapters 54 to 75.

- **Section G: Disclosure of Personal Data.** Chapters 76 to 88 deal with disclosure of personal data. Organisations may disclose personal data only as permitted in the consent given by individuals after the organisation has notified them of the purposes for which their personal data will be disclosed and the individual has consented to those purposes.

- **Section H: New Areas, Developments and Technological Concerns.** Finally, chapters 89 to 99 cover new developments and technology concerns relevant to the GDPR, as well as new business segments that may be prone to potential privacy breaches such as start-ups and individuals working in the gig economy (or sharing economy).

### How to use this book

We expect that some of our readers might read this book from front to back. But more often we expect our readers will want to dip into it and read the chapters of most interest to them at any particular time. We have thus written it so that the individual chapters are "free-standing" and without cross-references. We have presented some information more than once to underpin this approach and hope that those who read it from front to back will forgive us for a small amount of repetition.

# Glossary

This book was written in Singapore. We have sought to use terminology that is not specific to Singapore, however, although our generic language is based on the data protection legislation in Singapore. Here are some explanations and equivalents. If your jurisdiction is not listed, words used have an equivalent meaning there.

**"Data protection law"** includes:

- Personal Data Protection Act 2012 – Singapore
- Personal Data Protection Act 2010 – Malaysia
- Data Privacy Act of 2012 – the Philippines
- Personal Data (Privacy) Ordinance (Cap. 486) – Hong Kong
- Privacy Act 1988 – Australia
- Privacy Act 1933 – New Zealand
- Data Protection Act 1998 – United Kingdom
- Data Protection Act 1988 – Ireland
- General Data Protection Regulation (GDPR) – European Union

**"Regulator"** includes:

- Personal Data Protection Commission (PDPC) – Singapore
- Personal Data Protection Department (PDPD) – Malaysia
- National Privacy Commission – the Philippines
- Office of the Privacy Commissioner for Personal Data, Hong Kong – Hong Kong
- Office of the Australian Information Commissioner – Australia
- Privacy Commissioner – New Zealand

- UK Information Commissioner's Office – United Kingdom
- Data Protection Commissioner – Ireland
- The data protection authority for the country of an organisation's main establishment and, if different, the "concerned authority" where an individual complainant resides – European Union

**"Organisation"** includes:

- Companies, unincorporated associations, firms and individuals conducting business (as used in Singapore and Australia)
- Data controller (as used in EU, UK and Ireland)
- Data user (as used in Hong Kong and Malaysia)
- Personal information controller (as used in the Philippines)
- Agency (as used in New Zealand)

**"Personal data"** is synonymous with personal information.

**"Individual"** is synonymous with data subject.

**"Data intermediary"** is synonymous with data processor.

“Data is the pollution problem of the information age, and protecting privacy is the environmental challenge.”

Bruce Schneier

SECTION A:

# Governance & Information Asset Management

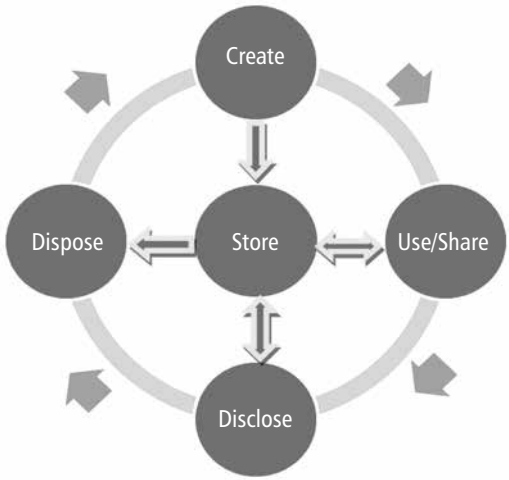
# 01 Data protection: don't forget that it is also physical

"Data protection" – when you see or hear these two words, what are the first thoughts that come to your mind? To most of us who are raised in today's Information Age and are being bombarded with multimedia-rich information content every day, we will not be too far off the mark when we say "data protection" includes:

- Secure databases with multi-layers of access controls, including passwords and multi-factor authentication
- Secure networks with firewalls and concentric rings of protection
- Data encryption
- Data loss/leakage prevention and
- Intrusion prevention and intrusion detection systems

Ironically, even though a lot of data today is in digitised or electronic forms, we still handle a massive amount of paper documents containing personal, confidential, private or sensitive information. The reasons vary. Many agreements are still in paper form, either for legal reasons or to cater to the parties' preferences. Official documents, such as land titles, marriage certificates and educational certificates, need to be in paper form with watermarks, authorised signatures and seals of the issuing authorities. Other documents, official and unofficial, such as interview or other meeting notes and assessments, are still sometimes more conveniently created and kept in paper form.

The personal data in these paper documents also have to be protected, so "data protection" must include elements that are relevant to paper documents as well – for example, keeping them under lock and key.




### The document life cycle

For both business and regulatory compliance reasons, an organisation must protect paper documents containing personal, confidential or sensitive information against unauthorised access, use, disclosure, duplication, modification, disposal or loss.

To establish effective control measures an organisation needs to first understand the *document life cycle* – that is, what happens from the point a document is created or generated to the point it is disposed of or destroyed. This includes understanding how the document is handled at each stage, for what reason and by whom.

The document life cycle:

- provides the organisation with useful insights on the weaknesses and vulnerabilities in protecting documents in the entire "data protection" chain, and then
- enables the organisation to develop and implement appropriate preventive or mitigating controls to address these areas of weaknesses and vulnerabilities in order to protect the documents.

### Journeying through the document life cycle

Here is a typical approach to determining a document life cycle:

- First, an organisation must compile a list of documents (including forms) that are required to support its various business processes.

With this *document inventory*, the organisation's objective is to get a clear view of all of its documents that are to be protected.

- Second, the organisation must assess each document in terms of its confidentiality and sensitivity. This is done so that the appropriate level of security protection can be assigned to the document.

  In other words, each document has to be classified according to a predetermined *document classification scheme*. Examples of document classification include "Confidential", "Internal Use Only" and "Public".
- Third, it is important for an organisation to have clear visibility of which department or employees within the organisation are responsible for handling the document at each stage of the life cycle and business process.

  Therefore, the organisation must construct a *document flow diagram*. This traces the movement of the document through its life cycle based on the organisation's business processes.
- Finally, based on the document flow diagram, the organisation must perform an *onsite audit* to assess the adequacy of existing document protection measures. It must then address identified weaknesses and vulnerabilities to minimise the organisation's risk exposures.

The onsite audit should focus specifically on:

- **Create** – where and how the documents are first created or generated, including completing paper forms
- **Store** – where and how the documents are stored or archived
- **Use/Share**
  - where and how the documents are used and shared within the organisation – high-risk areas include the handing/taking over points between departments or between employees
  - how documents in the possession of individual staff are controlled and safeguarded, including if and how individual staff can duplicate or copy them
- **Disclose** – identifying the "outside" individuals and organisations to whom the organisation discloses documents and how this is done
- **Dispose** – how the organisation disposes of or destroys the documents when it has no further use for them

### Benefits of the document life cycle

By having a systematic process of managing the document life cycle, organisations gain better assurance and confidence that they have addressed and mitigated the risks and vulnerabilities associated with the unauthorised access, collection, use, disclosure, copying, modification and disposal of personal, confidential, private or sensitive information.

**CHECKLIST OF GOOD PRACTICES**

In managing their documents containing personal data and other confidential information, organisations should:

- Understand the purpose and benefits of documenting the document life cycle.
- Put in place systematic processes to:
  - produce a *document inventory* and to ensure it is kept up to date
  - implement an agreed *document classification scheme*
  - produce *document flow diagrams* and ensure they are kept up to date and
  - carry out regular *onsite audits* to address any identified vulnerabilities and weaknesses

# 02 Investigated by a regulator? Will it find only good… or some bad?

When we work with our clients we have a constant refrain covering two things about data protection and privacy processes:

- concentrate on your operational compliance or you will get into trouble – and concentrate on it continuously with regular audits because it is not a "set and forget" task – and
- have an effective complaints resolution process in place to minimise the risk of any complaints to the regulator – audit its effectiveness regularly too and learn from complaints received.

An adverse outcome of a regulatory investigation – a finding that the organisation has failed to comply with the data protection law – can obviously have unfavourable consequences, including a fine. But even a "clean" outcome has a downside: investigations are distractions that use up time and management resources better spent on business operations.

Here is one case where an organisation took the time to get everything right at the outset. And another case where it did not.

### Case #1: Good processes pay off

An individual complained to the regulator[1] that they had received – and incurred charges related to – text messages from a subscription service after entering their mobile phone number into a website for a chance to win free flights. The individual complained that they had no knowledge of opting-in to receive text messages from the organisation.

[1] See https://www.dataprotection.ie/docs/Case-Studies-2008/939.htm, case study 7.

The regulator established that:

- when the individual entered their mobile phone number the organisation had sent them a text message that included a PIN number and the individual then entered the PIN number into the website to verify the subscription and
- the website indicated that the service was a subscription service and outlined the cost and frequency of the subscription element and
- the website gave clear instructions on how to unsubscribe from the service.

Therefore the individual had not received unsolicited marketing text messages as claimed, but had legitimately received subscription service text messages after opting-in to a service on the organisation's website. The regulator was also satisfied that the organisation had put in place appropriate procedures to ensure that numbers entered on the website were validly entered. Receiving a text message and actively opting-in removed any doubt about the validity of the consent.

The regulator commented that this case study is a clear reminder that individuals need to pay greater attention to information that organisations make available to them, particularly on websites. There were no grounds for upholding the individual's complaint.

The organisation might have been complimented on taking the time to develop and implement a carefully thought-through process that complied with the requirements of the data protection law.

### Case #2: Operational errors have unintended consequences

An individual provided their payment card details and email address to an organisation for the purpose of purchasing tickets for a particular concert. More than 12 months later the organisation sent them emails regarding the cancellation of another concert, for which they had not purchased a ticket.

The individual was concerned that the organisation had retained their personal data for such a long time and asked the organisation to remove their personal data from its database. At the same time, they complained to the regulator.[2] Here is what happened.

[2] See https://www.dataprotection.ie/docs/Case-Studies-2008/939.htm, case study 13.

- **Complaint resolved:** The organisation informed the regulator that it sent "performer alert emails" to customers who had previously bought tickets. These were only sent in respect of "similar products or services" in which it thought previous customers would have an interest. In each message, the organisation gave individuals an easy and free way of opting-out from receiving future messages.

  The organisation said that the emails about the cancelled concert had resulted from an operational error and that it had rectified its internal processes so that such an error would not recur. It wrote to the complainant to confirm that it had deleted all of their personal data from its records in accordance with their request.
- **Further consequences:** Problem solved and investigation closed, right? Wrong. Regulatory investigations are generally rather thorough. They may well uncover data protection/privacy issues in addition to the subject of the complaint they are investigating.

  That is exactly what happened to turn an operational email error into a much wider-ranging investigation and series of actions to be taken by the organisation. The regulator:
  - was concerned about the length of time the organisation retained personal data such as payment card details and said it should be reduced from 16 months to 12 months, with the personal data being deleted if there was no activity on the individual's account during that time and
  - said it would be more appropriate for individuals to opt-in to have their details retained rather than the existing practice of requiring them to uncheck a box when they purchased a ticket

  In addition, the regulator was concerned that the organisation might not have appropriate procedures in place for deleting personal data when it was no longer required for the purpose for which it was collected. It therefore obtained a copy of the organisation's data retention policy. This led to the regulator highlighting issues in relation to the privacy policy statement on the organisation's website.

  One issue was that the privacy policy statement referred to UK data protection legislation and made no reference to the Irish data protection legislation, whereas the organisation was registered in

both England and Ireland. The regulator said that a data protection notice relevant to Ireland should be published on its website. The organisation said the omission was an oversight on its part and remedied it.

- **Regulator's overall comments:** At the end of the investigation, the regulator said that it was satisfied that the organisation took its data protection responsibilities seriously. The regulator was "encouraged" by the cooperative manner in which the organisation addressed the issues and implemented the regulator's recommendations.

So, the outcome of the investigation might have been worse. But that was doubtless cold comfort to the organisation for a distraction that could have been avoided.

**CHECKLIST OF GOOD PRACTICES**

- Organisations should:
  - concentrate continuously on operational compliance with data protection laws and regularly audit it, particularly to avoid unintended consequences
  - have an effective complaints resolution process
- Individuals should pay attention to information provided to them by organisations, to make sure that their personal data is not retained beyond a reasonable period and they have an option to withdraw consent

# 28 Anonymising personal data – but is the individual really not identifiable?

*At an unidentified beach resort somewhere, two friends are lazing by the beach and debating the affairs of the world. The conversation soon turns to the concept of anonymity…*

A: Why do people want to be anonymous?

B: So that others will not know their true identities.

A: Whatever for?

B: So they can hide under a cloak of secrecy to say and do things that society or the government might not approve of them saying or doing.

A: Such as?

B: You may have heard of the "Anonymous" group of "hacktivists" who hack into government, religious and corporate websites, defacing them or posting vitriolic anti-establishment or protest content. By doing so, they hope to expose cover-ups, scandals or corruption in government and corporations in the name of justice or in their fight for the rights of the disadvantaged. None of the members of the "Anonymous" group ever uses any name. If they appear in public, such as when they make a public statement about their position on some issue, they wear a mask so that they can't be identified.

Or you may have read comments posted by individuals on social media platforms using a pseudonym – a fictitious name or an alias, for example – rather than their real names. They feel more liberated to air their views freely without fear of being tracked down by the authorities, lobby groups or other people who oppose their views.

A: Are you saying that being anonymous is different from using a pseudonym?

B: Yes. When an individual is anonymous they can't be identified by name. So if they do two or more different things there's no way of knowing that the same individual did them.

When someone uses a pseudonym they are using a false name. They still can't be identified by name. But if the same person does two or more different things under the same pseudonym it's known that the same individual did those things.

A: So, using a pseudonym is, strictly speaking, not anonymity but pseudonymity. But they are both ways in which an individual can hide their identity.

B: You are absolutely right. If I were to place the two concepts on a scale, I would say that pseudonymity is less strong in concealing the true identity of an individual as compared to anonymity.

A: So far, you have cited examples of the negative side of anonymity. Are there positive examples too?

B: Plenty. Say a rich person wants to donate a large sum of money to a certain charity. They don't want their true identity to be known in case there is publicity. It may infringe on their personal privacy, for example, because they are suddenly newsworthy and stories are written with details about their life or because they receive a spate of letters and phone calls seeking donations. Or simply because other people, including their friends, congratulate them about their

generosity when they would prefer not to talk about their donation. So they donate the money anonymously, so that not even the recipient charity knows their identity.

In research, there are many instances where the researcher anonymises the raw data of the sampled individuals so that they become non-identifiable. This is intended to ensure that sensitive personal data of individuals, such as health and medical data, are not disclosed. After all, in most research studies, the researcher is interested in trends, patterns and profiles derived from aggregated data. The identity of the individuals in the research sample doesn't matter.

A: If, as you say, researchers are interested in aggregated data only, then why don't they just leave out the unique identifiers of the individuals, such as their full name, home address and identity card number when they collect the personal data?

B: Ah, that's a good question. And the answer depends at least partly on the type of research and also on whether the personal data was collected solely for the research or whether it was collected for some other purposes and then later used for research.

For most research projects the researcher needs to have some unique identifiers of the individuals surveyed for two reasons. First, for the research to be accepted as valid the researcher may for practical reasons need to be able to verify that the data comes from real people. Secondly, when researchers are analysing and compiling their survey results they may need to clarify with the individuals concerned any ambiguity or discrepancy in their survey responses.

For some research projects the researcher doesn't need to have any unique identifiers for the individuals surveyed. This happens most often when the research is merely observational. For example, in a survey of public transport usage the researcher may simply need to observe and count the number of individuals, divided into categories of men, women and children, boarding certain buses and trains at specific times of the day and night.

A: OK. That's interesting. What did you mean when you mentioned that an organisation might collect personal data for a particular purpose and then later use it for research?

B: Well, say for example, that a voluntary welfare organisation, a charity, provides counselling and support in connection with an addiction, such as gambling addiction. For that purpose, it collects a wide range of personal data from individuals about themselves and their families and family circumstances.

Under the data protection law, the organisation must dispose of this personal data when it is no longer necessary for a legal or business purpose. Or the organisation may anonymise it and then can continue to keep it. The organisation might want to use it for research purposes or for similar purposes such as planning future service delivery or assessing the effectiveness of the organisation's counselling services.

To anonymise it effectively, the organisation must remove and dispose of all the personal data that might identify an individual and then it may keep the remainder. The organisation might assign a unique identifier to individuals for convenience when it refers to them. But for the data to be anonymised for the purposes of the data protection law the organisation must not keep the "key" to re-identifying any individuals.

A: You've lost me. What do you mean?

B: Well, John Lim of such and such address may be identified as "Man #1" and David Lee of some other address may be identified as "Man #2" and so on. Imagine a spreadsheet with the real names and addresses in two columns and "Man #1", "Man #2" in another column. To anonymise this personal data, the organisation must get rid of the two columns of names and addresses, retaining no copy, so that it is not possible to work out the identity of "Man #1", "Man #2", etc.

And this is just a fairly simple example that I've given. Depending on the circumstances, there may be more personal data that will need

to be taken away so that re-identification is not possible, such as the individual's mobile phone number and their identity card number. This can all be really tricky. I'm just giving you an idea of the way it works. To avoid unpleasant surprises, such as not complying with the data protection law, anonymisation of personal data collected for a specific purpose usually needs some expert assistance.

A: Right. I get it. But how can one be sure that once the data is anonymised, there is no means to re-identify it and link it back to the original individuals?

B: Well, most research organisations are governed by strict policies and codes of practice. These require them to remove the unique identifiers from the datasets once the research study is completed. They have to overcome any "just in case" thoughts of researchers who want to keep the unique identifiers just in case they might need them in the future.

And of course there is also the data protection law. If an individual finds out that an organisation has kept the means of identifying them for longer than the organisation needs their personal data for business or legal purposes they can complain to the regulator. The penalties for an organisation failing to comply with the data protection law can be stiff.

A: So much for research organisations. As an individual, how can I be sure that my anonymity is protected if I choose to be anonymous on certain occasions or under certain circumstances? For example, what if I want to remain anonymous when I contribute to an online forum that is discussing controversial and sensitive issues?

B: Well, usually you need to use some identifier on online forums, so you'll use a false name or alias that you think doesn't identify you. It'll be a case of pseudonymity, rather than anonymity.

Unfortunately, even if you can't be identified by your pseudonym it is impossible to be absolutely sure that your personal identity will never be found out, especially in today's highly connected and

networked world. This is because your mobile devices and other gadgets are sure giveaways of your location.

What I'm talking about here are mobile phone networks that can pinpoint your location through the signals emitting from your mobile phone. If you use public WiFi networks they also keep track of your location. Then there is the GPS (Global Positioning System) function in your phone or tablet. Some devices and gadgets (such as payment cards) use NFC (Near Field Communication) or RFID (Radio Frequency Identification).

If any of these methods show that you are usually in the same location from, say, 10:00 p.m. every day to 7:30 a.m. the following day, your home address is known. Ah, you say, but it's a condo so no one can know which of several individuals is me. Easy. Someone who wanted more information could sit outside the condo and wait until they see your mobile phone moving. Then they'll have you car registration number. They could follow you to your office and then know where you work. They could come into your office and ask the receptionist for your name or they could find it out through car registration records.

A: This is getting scary. Maybe I should be careful and turn off the location-identifying functions on my devices where possible and get rid of those devices and gadgets where I can't turn it off.

B: That sounds pretty inconvenient to me. And it won't necessarily keep your identity hidden. This is because when you surf the Internet, visit websites, communicate via emails or do online shopping, you leave behind loads of digital trails like your IP address, cookies downloaded on your computer, and the websites you have visited.

Service providers can use this information to match against their databases to identify you easily. I recall a police investigation where telephone companies – mobile phone carriers – were ordered by the Court to reveal the identities of a suspected group of drug traffickers who used their mobile phones to communicate with one another. And in several countries in 2015 the Courts ordered Internet Service Providers (ISPs) to reveal the identities of individuals who had

allegedly downloaded illegal copies of a movie called Dallas Buyers Club.

In a publication of the International Association of Privacy Professionals (IAPP) it was reported that knowing just three pieces of information about an individual – namely the birth date, zip/post code and gender – can identify the individual with a high degree of certainty by matching them against public records.

A: Wow, that's scary! We can't go around ignorantly thinking that anonymity or pseudonymity will protect us from being identified. We have to be very careful in what we say or do from now on. Hey, why don't we blog about what we have discussed today, to share with a larger audience? Should we do it anonymously, pseudonymously or with our true identities?

B: Haha! That depends on the content and the audience.

*The two friends then enjoy the beautiful sunset, while sipping the exotic fruit punch. Another fruitful day!*

**CHECKLIST OF GOOD PRACTICES**

Organisations and individuals should be aware of how to deal with anonymised data:

- Personally identifiable information can be anonymised by removing the unique identifiers, through aggregation or generalisation, or by replacing the actual data values with other values.
- Do not assume that anonymity is safe. People can be re-identified through a few pieces of information about them and matched against public records.
- The Internet and portable smart devices make it easier to track the location and usage patterns of individuals, and service providers can link these back to their databases for re-identification.

# 29 Beware of secondary usage of personal data

I applied to the local utilities company to open an account for my apartment that had just been vacated by the previous tenant and was to be marketed to a new tenant. The application process was a cinch. All I needed to do was to visit the website of the utilities company and fill in the application form online. So I keyed in all the information I expected would be sought, such as my name, identity card number, address of the apartment, the billing address, my email address and my phone number. So far so good.

Then there was a field that asked for my ethnic group, which I was quite reluctant to provide. In my mind I was thinking: why would the opening of a utilities account require a knowledge of my ethnic group? But since time was running short – I had to have the power and water turned on in a few days' time – I submitted the form with the field for ethnic group duly completed.

The next day, I sent an email to the utilities company asking them to clarify why they need to know my ethnic group for the purpose of opening a utilities account. The reply from the utilities company came back after a week with a terse one-liner to say that the information was required by their principal for analysis and reporting purposes. Apparently the utilities company was collecting the data on ethnic group on behalf of another organisation and they did not know much of the details.

Not satisfied with this answer, I wrote directly to the principal for enlightenment. Two weeks later, someone from the principal replied to say that the data on ethnic group was relevant to their study of

electricity consumption. This got me even more intrigued as I could not understand the cause-effect relationship between ethnic group and electricity consumption. I had learned in school that electricity consumption is affected by the number and type of electrical appliances, and how long they are being switched on. I wouldn't have minded so much if the principal had asked for the floor area of my apartment, the number of air-conditioning units or the number of occupants.

### Beware of secondary usage of personal data

The reason I am sharing this experience of mine is that as individuals providing our personal data to organisations, we should at least be notified of the purpose for the collection, usage and disclosure of our personal data. The utilities company should not have collected personal data beyond what was required for the primary purpose of opening an account. Worse still, the utilities company was collecting and disclosing personal data to a third-party for another secondary purpose without express consent from the customers. It would still be unacceptable even if the principal of the utilities company could assure consumers that their personal data would be anonymised for research purposes.

### Sales or marketing as a secondary use of personal data

Collecting personal data for a primary purpose and then using or disclosing it for a secondary unrelated purpose is not uncommon. For example, it is very tempting for the sales or marketing department in an organisation to conveniently get personal data that has been collected by another department for a particular (primary) purpose and use the data for their prospecting purposes. Organisations must guard against such a practice and require their employees not to do so, in order to ensure that the organisation does not fail to comply with the data protection law.

**CHECKLIST OF GOOD PRACTICES**

Organisations collecting personal data of customers should adopt the following practices:

- Notify customers of the purpose of collecting, using and disclosing their personal data.
- Do not collect more personal data than is required for the primary purpose or use it for a secondary unstated or unrelated purpose.
- Do not use personal data that is collected for a non-marketing purpose to prospect for new customers.

# 70 Digitising may be efficient, but don't forget the hardcopy

It almost goes without saying that office space is expensive, especially well-located office space in cities. It equally goes without saying that most organisations reduce their overhead expenses as much as possible by limiting the office space they acquire. It then follows that they find ways and means to maximise its use.

Besides carving out space for people, furniture and equipment, office planners have to create storage areas for paper documents and files. One means of reducing physical storage space is to digitise the paper documents and store them in computer servers or magnetic media that take up a fraction of the space.

Besides the saving in storage space, digitisation brings about a number of efficiencies and benefits. For example:

- the same e-document can be shared with a number of users concurrently at any time and at any place
- it is easier to index and retrieve e-documents
- an organisation can implement secure access controls to e-documents and
- e-documents do not deteriorate over time.

### Far from paperless office environment

Organisations may dream of a paperless – or at least a "less-paper" – office environment. However, even with digitisation, many organisations still maintain lots of compactus filing systems and storage cabinets for paper documents. Why is this so?

In some instances and due to legal or statutory requirements,

original paper documents bearing original authorised signatures, seals or company stamps must be maintained. It makes no difference that digital versions have been created. Examples of such documents include certificates and licences and, in some cases, even contracts and more informal documents such as memoranda of understanding.

### What should organisations do?

Organisations are faced with having two systems to manage their valuable and confidential documents – one for paper documents and one for e-documents.

For e-documents, there are a number of proven document management systems in the market. Some of them even include an authentication function so that e-documents can be produced in court in lieu of producing an original (paper) document.

Managing paper documents is more challenging, particularly where an organisation adopts digitisation, as it involves a number of manual processes. Here are some tips:

- **Version control**

  The paper version of each document and any e-version of it must be consistent. This is obviously easy where the organisation creates the document electronically. Whenever there is a new version of a paper document, either created by the organisation (such as by having an individual complete a paper form) or received from a third-party, a digitised version should be created as soon as possible.

- **Indexing and cataloguing**

  Paper documents have to be indexed and catalogued in a file inventory so that the organisation knows at any time where these documents are kept.

  The file inventory also helps the organisation to retrieve any document efficiently when needed. This is important in enabling an organisation to comply with the access and correction requirements of the data protection law. It is usually necessary in enabling it to comply with its document retention policy, as required by the data protection law.

- **Access control**
  The organisation must develop and implement policies to classify documents (such as "Confidential", "Public") and to control access to personal data and other confidential information on a "need to know" basis among its employees.

  This too is an important element in enabling an organisation to comply with the data protection law.

- **Retention and storage**
  The paper documents have to be stored in a safe and secure place to enable an organisation to comply with requirements of the data protection law to protect personal data. The storage place should have appropriate environmental controls to prevent the deterioration of the paper.

  If the paper documents are stored offsite, such as in a warehouse, the organisation should first satisfy itself that the warehouse operator is capable of storing the documents safely and securely. The organisation should include requirements in its contract with the warehouse operator about safety and security of storage and audit, particularly where documents contain sensitive personal data or highly confidential information. The organisation should ensure that the warehouse operator abides by these stringent requirements, including by exercising any inspection or audit rights under the contract.

  The time period of storage should follow the organisation's document retention policy for each type of document.

- **Disposal and destruction**
  The paper documents that contain personal data have to be marked for secure disposal or destruction when the retention periods adopted for compliance with the data protection law are reached.

  The retention schedule for each such document has to be recorded in the file inventory to ensure efficient tracking of the life of the document.

**CHECKLIST OF GOOD PRACTICES**

In managing paper documents, organisations should adopt the following practices:

- Version control – consistency between the versions of paper documents and e-documents.
- Indexing and cataloguing – file inventory to help in organising and storing the paper documents and in retrieving them when needed.
- Access control – policy to spell out who can have access to what document.
- Retention and storage – safe and secure place for storing paper documents, preferably with environmental controls. Same requirements apply to paper documents that are stored offsite at warehouses.
- Disposal and destruction – secure disposal or destruction of the paper documents when the retention periods are reached.

# About the Authors

**Kevin Shepherdson, CIPM, CIPT, GRCP, CIPP/E, CIPP/A, FIP**

Kevin Shepherdson is the CEO and co-founder of Straits Interactive Pte Ltd, voted as one of the Top 25 Compliance Solutions Providers in the Asia Pacific by *Asia Pacific CIO Outlook* magazine. He provides and drives the vision, strategy and innovation of the company's Data Privacy & GRC (Governance, Risk Management & Compliance) platform offerings.

He is a fellow of the International Association of Privacy Professionals (FIP), a Certified Information Privacy Manager (CIPM), Certified Information Privacy Professional Asia/Europe (CIPP/A and CIPP/E) and Privacy Technologist (CIPT). He is also an official trainer for both IAPP's privacy and OCEG (Open Compliance & Ethics Group) GRC professional certification courses for the ASEAN region.

Kevin has consulted with more than 100 companies in the area of data protection and has trained a few thousand people on the GDPR and local data protection laws in Singapore, Malaysia, Indonesia and the Philippines.

A veteran in the IT industry, Kevin has worked for a number of multinationals in senior management positions, including Creative Technology, Sun Microsystems and Oracle Corporation. Throughout his corporate career, Kevin was a multiple award-winner of both worldwide and Asia-Pacific employee excellence awards, including marketing excellence, market intelligence and technology innovation. He is a sought-after speaker for data privacy and protection issues in the ASEAN region.

Kevin holds a MSc (Internet & Media) degree from Nanyang Technological University and a Bachelor of Arts & Social Sciences from

the National University of Singapore, and is a Certified GRC Professional as well as a certified Master Practitioner in Neuro-Linguistic Programming (NLP), Neuro-Semantics and Hypnotic Communication.

**William Hioe, CIPM, CIPT, CIPP/A, CIPP/E, FIP, GRCP**

William Hioe is a senior consultant with Straits Interactive. He holds a number of certifications from the International Association of Privacy Professionals – Fellow of Information Privacy (FIP), Certified Information Privacy Manager (CIPM), Certified Information Privacy Technologist (CIPT), and Certified Information Privacy Professional for Asia and Europe (CIPP/A and CIPP/E). He is also a certified Governance, Risk Management and Compliance Practitioner (GRCP) from the Open Compliance and Ethics Group (OCEG).

William has more than three decades of Information and Communications Technology (ICT) experience in the government and public sector. Currently, he is the managing director of Cynergie Consulting Pte Ltd, a company founded by him to offer consultancy and training services in strategic ICT planning, strategy development, policy formulation, enterprise architecting and process improvement. Prior to that he was senior director of strategic planning at the National Computer Board (NCB)/ Infocomm Development Authority of Singapore (IDA). Before that he was an assistant director in Systems & Computer Organisation at the Singapore Ministry of Defence.

During his career in the government and public sector, William has built up a wealth of knowledge and expertise in ICT planning, development, implementation and project management in such diverse areas as human resource management, financial management, logistics management, procurement management, decision support systems, wargaming, and command and control systems. At NCB/IDA he was involved in the visioning, strategising and development of national-level ICT masterplans. He was also responsible for ICT policy research and formulation in such areas as secure e-transactions, digital signature, anti-spam, data governance, and data privacy and protection. With Cynergie Consulting, he has consulted with governments in South-East Asia in the areas of ICT masterplanning, visioning and strategy development.

William graduated with a B.Sc.(Engg) in electrical and electronics

engineering from the University of London and a Masters in control engineering and operational research from the University of Cambridge. He is a certified enterprise architecture practitioner (TOGAF) from The Open Group.

**Lyn Boxall, B.Com, LL.B (Melbourne), LL.M (Monash), GAICD, GRCP, GRCA, CIPM, CIPP/A, CIPP/E, FIP**

Lyn Boxall is a lawyer with extensive private practice experience and international in-house experience. In March 2015, Lyn established Lyn Boxall LLC, practising Singapore law and specialising in data protection / privacy, information/cyber-security, payment systems, and governance, risk and compliance. Her scope of work has more recently expanded to cover the General Data Protection Regulation (GDPR) and the laws regarding data protection / privacy in various ASEAN countries in addition to Singapore.

Lyn is a fellow of the International Association of Privacy Professionals (FIP), a Certified Information Privacy Manager (CIPM) and a Certified Information Privacy Professional Asia/Europe (CIPP/A and CIPP/E). She is also a certified Governance, Risk Management and Compliance Practitioner and Auditor (GRCP and GRCA) from the Open Compliance and Ethics Group (OCEG) and a Graduate of the Australian Institute of Company Directors (GAICD),

Lyn's privacy experience goes back more than 20 years, when she was Chief Legal Officer for GE Capital for Australia/New Zealand in 1996 and was part of an international in-house team formed to embed the requirements of the 1995 EU Data Protection Directive into the company's global products and operations.

Lyn is an Advocate and Solicitor of The Supreme Court of Singapore, a Member of the New York Bar, a Solicitor of The High Court of England and Wales and a Barrister and Solicitor of The Supreme Court of Victoria and of the High Court of Australia. She is also a member of the Data Protection and Cybersecurity Committee of The Law Society of Singapore and a member of SG Tech and its Cybersecurity and AI & High-Performance Computing chapters. Finally, Lyn is the author of "Personal Data Protection" for *Halsbury's Laws of Singapore* (published by LexisNexis).