Resolvo Systems Pte Ltd
20 Ayer Rajah Crescent #08-02
Singapore 139964
Tel: 65-68732049
Fax: 65-68734905

Feedback

Public Consultation on proposed Advisory Guidelines in the PDPA

Prepared by: Wong Onn Chee
First Published Date: 15 March 2012
Version: 1.0
Published Date: 15 March 2012
Total Page Count: 10
Document Classification: Feedback
RSFB-15032012-001

Abbreviations

Abbreviations	Full Name
PDPC	Personal Data Protection Commission
PDPA	Personal Data Protection Act

Distribution List

Name	Organisation, Department

Revision History

Version	Author	Date	Sections Changed	Summary of changes
1	Wong Onn Chee	15.Mar.2012	Initial version	

Contact Information

Customer

Liaison Officer: Title: Office: Fax: E-mail:	**Signature Authority:** Title: Office: Fax: E-mail:
Billing Address:	

Resolvo

Services Manager: Title: Office: Fax: E-mail:	**Account Manager:** Wong Onn Chee Title: CTO Office: +65-68732049 Fax: +65-68734905 E-mail: onnchee@resolvo.com

Table of Contents

1. Executive Summary

We congratulate PDPC on the prompt publication of much sought after guidelines, which private sector has been looking forward to since the enactment of the Act.

After our review of the guidelines on key concepts and selected topics, we have two (2) comments on the key concepts, two (2) comments on the selected topics and one (1) general comment.

We appreciate your kind attention to review our comments and we look forward to your kind follow-up thereafter.

2. Comments

2.1 Comments on Key Concepts

The following table lists our comments pertaining to "PROPOSED ADVISORY GUIDELINES ON KEY CONCEPTS IN THE PERSONAL DATA PROTECTION ACT ".

Section	Clause	Comments
11	Consent Obligation	One question is still left unaddressed. For instance, a person may have given consent to a service provider when one signs up for the service. However, when one terminates the service, the question remains whether consent is now deemed removed, as the current practices around termination of services do not allow one to explicit withdraw consent. We suggest that PDPC clarifies that consent is deemed to be removed once the commercial relationship with the service provider is terminated. An explicit opt-out should not be required as it is reasonable to deem the termination of consent goes together with the termination of the service. An explicit opt-in can be sought at the point of termination, so that the service provider can continue to communicate with the person even after the termination.
16.5	Examples of data protection measures	We observe that the explicit recommended usage of data leakage protection (DLP) solutions is missing in the list. End-point DLP solutions had already been mandated by our government authorities such as MAS for financial institutions for several years now. Hence, one can deem such solutions as a "reasonable" measure to protect personal data. In addition, as more personal data is now accessible via web-based services, such web-based CRM, self-managed portals and etc, we suggest that PDPC also recommends that private organisations implement solutions that prevent personal data leakage from web/cloud-based services. Attached in Annex A are reported cases of personal data leaked from web portals of Singapore commercial organisations. Past studies had shown us that the concern of data leakage from cloud is one of the main obstacles stopping users from adopting public cloud services. This is also mentioned in the MCI's (formerly MICA) justification for such an Act. However, the list of recommended measures does not address cloud or web-based services. In general, from a "reasonableness" point of view or common sense, it is "reasonable" to ***use inbound protection solutions to block inbound attacks*** and to ***use outbound protection***

		solutions to block outbound leakages. To recommend inbound protection solutions to block outbound leakages is difficult to legally defend on grounds of "reasonableness" or even common sense, hence such recommendations can easily be challenged in our court of law. Hence, arising from the need for PDPC to demonstrate due care and due diligence in the recommendations, we suggest that PDPC highlights the need for outbound security solutions to more reasonably protect against leakage of personal data, as shown by MAS in their directives to our financial institutions. The existing list of measures is sorely inadequate, even when compared to recommended ("reasonable") measures from other government agencies.

2.2 Comments on Selected Topics

The following table lists our comments pertaining to "PPROPOSED ADVISORY GUIDELINES ON THE PERSONAL DATA PROTECTION ACT FOR SELECTED TOPICS ".

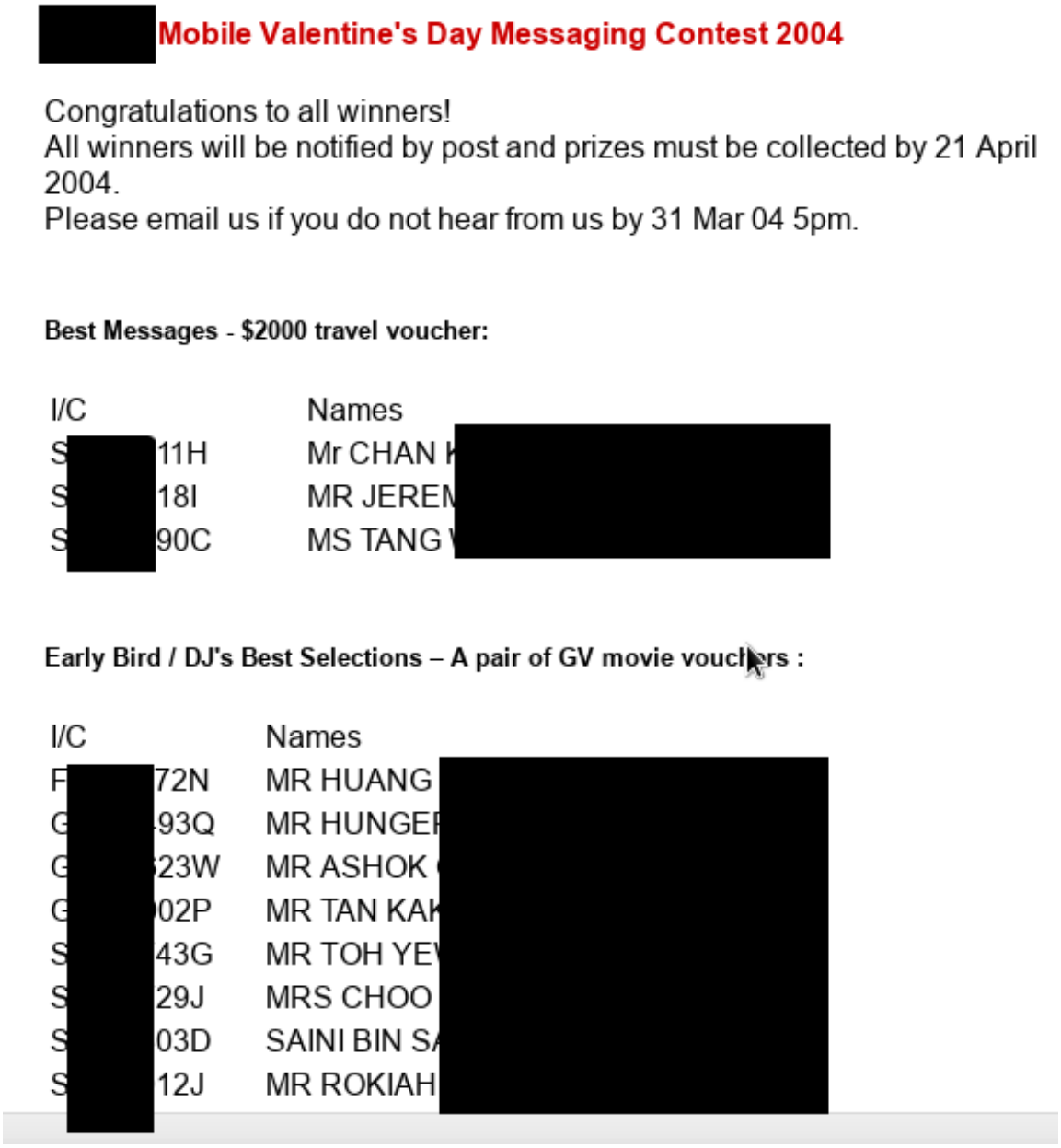
Section	Clause	Comments
6	NRIC Numbers	It is a common practice that security counters in commercial buildings require visitors to submit their NRIC numbers and names before being allowed entry to the buildings. We understand that such practice is helpful in contact tracing during times of pandemic outbreak. PDPC should publish explicit guidelines regarding such collection of NRIC numbers and names as such practices do fall under the ambit of the PDPA.
6.8	For example, organisations that use NRIC numbers as user names or membership numbers might be disclosing personal data to third parties without consent.	Our Singpass is based on NRIC. Similarly, some local Singapore banks are using NRIC as the UserID for their Internet banking services. What is PDPC's stand on such practices which contradict this guideline once the "sunrise" period is over?

2.3 Comments in general

2.3.1. PDPC should provide an online means of submitting complaints via PDPC main portal or a subsidiary portal. The submission mechanism should allow attachments, supporting the complaints.

Currently, there is no available means for the public to submit complaints even though the Act is already in effect. We understand that private organisations are given adequate time during the "sunrise" period of 18 months, but this does not mean the public can only submit complaints during this period.

3. Annex A: Leakages from web portals



[redacted] Mobile Valentine's Day Messaging Contest 2004

Congratulations to all winners!
All winners will be notified by post and prizes must be collected by 21 April 2004.
Please email us if you do not hear from us by 31 Mar 04 5pm.

Best Messages - $2000 travel voucher:

I/C	Names
S[redacted]11H	Mr CHAN [redacted]
S[redacted]18I	MR JEREM[redacted]
S[redacted]90C	MS TANG [redacted]

Early Bird / DJ's Best Selections – A pair of GV movie vouchers :

I/C	Names
F[redacted]72N	MR HUANG [redacted]
G[redacted]93Q	MR HUNGER[redacted]
G[redacted]23W	MR ASHOK [redacted]
G[redacted]02P	MR TAN KAK[redacted]
S[redacted]43G	MR TOH YE[redacted]
S[redacted]29J	MRS CHOO [redacted]
S[redacted]03D	SAINI BIN SA[redacted]
S[redacted]12J	MR ROKIAH [redacted]

Figure 1. Leakage of 100 subscribers' names and NRIC from local telco website

Updated: Singapore Airlines' website faced temporary glitch

Zafar Anjum | Feb. 22, 2012

In response to the news Krisflyer member gets 'online shock', Singapore Airlines (SIA) has explained to this publication that their website experienced a temporary issue which resulted in some unsavoury experience for some of its KrisFlyer members.

A Singapore-based user of Singapore Airlines' (SIA) membership programme, Krisflyer, had got 'online shock' when he logged onto his Krisflyer account last week. Raymond Liow wrote on Tuesday (21 February) in the Forum of the daily, *The Straits Times*, that when he logged onto his account on the airlines' website, he could read the full profile of another member.

"Our website experienced a temporary issue on the evening of 17 February, which resulted in some KrisFlyer members being shown pages from previous sessions of other members," Singapore Airlines vice president public affairs Nicholas Ionides told *Computerworld Singapore*.

"No unauthorised transactions took place," he clarified. "We sincerely apologise for this serious malfunction and acknowledge that it should not have occurred."

"The root cause was determined and the issue was resolved within four hours," he said.

"We take customer data privacy very seriously and assure our customers that steps have been taken to ensure that such an incident will not happen again," he added.

Figure 2. Leakage of KrisFlyer members from SIA website.

March 3, 2009

Glitch spills UBS clients' info

Wealthy customers saw details of others' online accounts, but bank says number affected is small

A TECHNICAL glitch at Swiss bank UBS gave its wealthy customers in Singapore and Hong Kong a shock last week when they logged on to their online accounts.

The private-banking clients found confidential details of other clients' bank statements and account information instead of their own. Clients' online accounts, though, do not indicate their names.

When contacted, a UBS spokesman confirmed the incident and said the bank was taking it very seriously.

Asked how many clients were affected, all she said was that 'some limited account information concerning a small number of UBS wealth-management clients was accessible by a very limited number of other system users'. She added that fewer than five accessed the information.

She told my paper the glitch occurred 'as a result of an inadvertent technical error following an information-technology system upgrade over the weekend of Feb 21'.

The bank immediately took steps to rectify the issue. UBS reviewed the circumstances leading to the incident and has implemented measures to prevent a similar occurrence in the future.

Figure 3. Leakage of clients bank account information from UBS Internet banking portal.