

# COMMUNIQUE

## SPECIAL AWARD ENTRIES ISSUE: DISPUTE RESOLUTION, COMPLIANCE AND ENFORCEMENT

### MESSAGE FROM THE SECRETARIAT

#### INSIDE THIS ISSUE:

**A PRACTICAL GUIDE ON COMPLIANCE WITH PERSONAL DATA LAW IN HONG KONG** 2-3

**SENSITISATION ACTIVITIES TO PROMOTE AWARENESS ON DATA PROTECTION ACT** 3

**ENFORCEMENT ACTIONS AGAINST DATA TRADERS** 4

**JOINT INVESTIGATION OF THE ASHLEY MADISON** 5

**FIRST PRIVATE SECTOR AUDIT** 6

#### SPECIAL POINTS OF INTEREST:

- Entries from Australia, Canada and USA, EU, Hong Kong, Ireland, Israel, Mauritius, Mexico, Philippines, Spain, and UK.

#### Dispute resolution, compliance and enforcement entries

The second category in the ICDPPC Global Privacy and Data Protection Awards is 'Dispute resolution, compliance and enforcement'. It builds upon the focus that the Conference has placed on enforcement cooperation in several resolutions in recent years.

This triple category reflects the multi-faceted roles that Data Protection Authorities perform which always covers at least one of the following roles and often encompass all three:

- Compliance: promoting compliance by data controllers or actually checking that they are complying.
- Dispute resolution: mediating or investigating and resolving issues where it appears to an individual that the law has been breached.
- Enforcement: taking many forms, enforcement involves taking formal action in relation to non-compliance with the law.



For most DPAs individual cases of dispute resolution and enforcement are carried out privately with public action typically only in a selection of cases, usually after the matter is completed and on the public record.

However, the private, confidential or

secret nature of aspects of some dispute resolution, compliance and enforcement has not prevented authorities from being able to give a public airing of selected successful initiatives or innovations. Indeed, we were pleased to receive 16 entries in this category.

The entries range over a variety of interventions, cases, techniques, tools and stages of dispute resolution, compliance and enforcement, such as:

- Compliance assistance: e.g. guidance to companies, public conference to follow up on major breach, creating communities of interest to support DPOs.
- Cases: case studies of complexity or involving cross-border cooperation.
- Techniques: e.g. investigation guidance to DPA staff, reviewing routine government practices that impact individuals, efforts to reward good practice.
- Tools: e.g. simplifying reporting by individuals of nuisance calls or filing of appeals by individuals, tools to assess impacts of laws.
- Stages: e.g. lodging complaints, investigation, criminal proceedings, filing of reviews or appeals, audits.

The range of entries demonstrates an impressive array of innovations and diligence amongst DPAs. Clearly privacy authorities are not simply sitting back and waiting for citizens to knock on their doors to lodge a complaint. They are promoting compliance amongst data controllers, acting in proactive ways to address systemic issues and tackle complex problems and assisting citizens to use the remedies provided in law.

I am sure that there are many good ideas amongst the entries from 2016 that will inspire other authorities to new endeavours in 2017.

*Blair Stewart – ICDPPC Secretariat*


## SPECIAL AWARDS ENTRIES ISSUE: DISPUTE RESOLUTION, COMPLIANCE AND ENFORCEMENT

This is the second of 4 special issues of the ICDPPC Secretariat newsletter outlining more than 90 entries to the inaugural ICDPPC Global Privacy and Data Protection Awards. This issue focuses on dispute resolution, compliance and enforcement. The others will variously feature education and advocacy and the use of online tools.

In each special issue you can read summaries of initiatives taken by member authorities that have been entered into competition. The ICDPPC Executive Committee Chair will be judging the entries over the coming months with the results being available in time for this year's annual meeting in Hong Kong in September.

You too can be involved as we are making arrangements to enable staff at member authorities to cast online votes for the 'people's choice awards'. Details of how to cast votes will be released in June so watch this space! Use these special newsletters to identify your favourite entries.



<b>Category 2</b> <b>Dispute resolution, compliance and enforcement</b>	<b>During 2016 or 2017 has your DPA:</b>
	<ul style="list-style-type: none"> <li>• Re-engineered or substantially improved your complaints processes?</li> <li>• Taken substantial new initiatives to promote compliance?</li> <li>• Enhanced your capacity for specialised investigation?</li> <li>• Made strides in cross-border enforcement?</li> <li>• Through your own initiatives scored a major enforcement success?</li> </ul>
	Or done something else interesting, effective or innovative in dispute resolution, compliance or enforcement? If the answer is yes: you should enter the ICDPPC awards ...
<b>Open to ICDPPC member authorities</b> <b>Deadline: 21 April 2017</b>	

## AWARD ENTRIES: DISPUTE RESOLUTION, COMPLIANCE AND ENFORCEMENT

### B1: Procedures Manual: Dispute Resolution and Investigations (New Zealand)

[non-competitive entry]



Office of the Privacy Commissioner

### Procedures Manual: Dispute Resolution and Investigations

21 November 2016

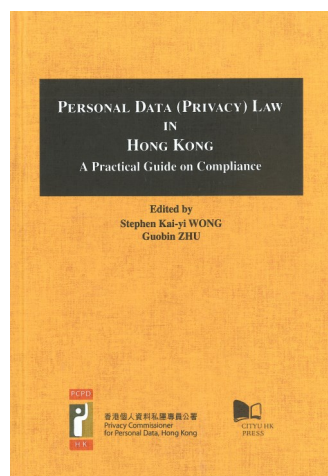
### Procedures Manual: Dispute Resolution and Investigations

In November 2016 the Office of the Privacy Commissioner adopted an internal Procedures Manual to guide staff work in dispute resolution and investigations. The objective is to help to:

- ensure that our work is lawful
- provide certainty and consistency in our administrative processes

- preserve institutional memory by recording the knowledge and experience accumulated over two decades
- reinforce and support investigations staff in exercising statutory discretion

### B2: A comprehensive guidebook entitled "Personal Data (Privacy) Law in Hong Kong – a Practical Guide on Compliance" (Hong Kong)



### A comprehensive guidebook entitled "Personal Data (Privacy) Law in Hong Kong –

*Hong Kong's practical guide on compliance is written with a view to explaining the conceptual, legal and practical frameworks of personal data privacy protection.*

**AWARD ENTRIES: DISPUTE RESOLUTION, COMPLIANCE AND ENFORCEMENT (CONTD.)**

**a Practical Guide on Compliance\***

The book is written with a view to explaining the conceptual, legal and practical frameworks of personal data privacy protection in Hong Kong, in the hope that readers, whether professionals or otherwise, will find it user-friendly to delve into the most relevant statutory provisions for their need or interest in the topics.

**B3: Sensitisation activities to promote awareness on the legal provisions of the Data Protection Act (Mauritius)**

The Data Protection Office engaged in continuous sensitisation activities to promote awareness on the legal provisions of the Data Protection Act and application of data protection principles in real-life scenarios. The office adopted a customer centric approach by moving towards people. In its mission to remedy the infringements occurring through the mishandling of personal information of our citizens, this office conducted enquiries and investigations with a view to establishing whether a breach has taken place or not under the Data Protection Act.



**B4: Digital tool for citizens to report nuisance calls and messages (UK)**



For citizens to report nuisance calls and messages to the UK Information Commissioner's Office (ICO), so that we can take action against those responsible.

**B5: System of Access, Rectification, Cancellation and Opposition of Personal Data of the State of Mexico (SARCOEM) (Infoem, Mexico)**

Sarcoem is a computer system that allows ARCO rights to be exercised to authorities of the State of Mexico and Municipalities by



Internet, to file an appeal against (review), verifying compliance and management to the profiles of various users.

**B6: First ever data privacy summit in the Philippines (Philippines)**



Privacy.Gov.PH – Government at the Forefront of Protecting the Filipino in the Digital World is the Philippines' first data privacy summit, held last December 5-6 at Novotel Manila. With over 250 attendees from government agencies and civil groups, it provided a venue for state institutions to familiarize themselves with the fundamentals of data privacy, the Data Privacy Act, and its IRR.

**B7: Complex investigation into the unlawful acquisition and use of personal data (UK)**

About the ICO / News and events / News and blogs /

**ICO investigation reveals how charities have been exploiting supporters**

Date: 06 December 2016  
Type: News

The Royal Society for the Prevention of Cruelty to Animals (RSPCA) and British Heart Foundation (BHF) secretly screened millions of their donors so they could target them for more money, a comprehensive ICO investigation has found.

The ICO said so-called "wealth screening" was one of three different ways both charities breached the Data Protection Act by failing to handle donors' personal data consistent with the legislation.

Complex investigation into the unlawful acquisition and use of personal data by 24 major UK charitable organisations. The investigation uncovered widespread unlawful use of donor and supporter personal data, with charities sharing it with

*The ICO investigation uncovered unlawful use of donor and supporter personal data, with charities sharing it with commercial third parties in order to undertake detailed investigation into donor income and finances.*



**AWARD ENTRIES: DISPUTE RESOLUTION, COMPLIANCE AND ENFORCEMENT (CONTD.)**

commercial third parties in order to undertake detailed investigation into donor income and finances. The charities used the personal data provided by supporters to uncover additional personal data and use it to target donors.

**B8: Data Protection self-assessment for SMEs (UK)**



For organisations, particularly small and medium sized enterprises, to quickly and easily assess their compliance with the Data Protection Act in a range of areas, and get targeted guidance on what they can do to improve.

**B9: ILITA's enforcement actions against data traders (Israel)**



**ILITA's enforcement actions against data traders**

In 2005 the Israeli population registry was stolen. ILITA conducted a criminal investigation that ended with 5 people convicted, two of which were sentenced to jail. In order to prevent further use of the data, in a complex forensic investigation, which took place in 2016, ILITA found data traders that obtained the illegal information, and terminated their activities. ILITA identified the clients who bought the data, gave them instructions and fined "disobedient" clients.

**B10: Crossing the Line: The Indiscriminate Disclosure of Attempted Suicide Information to U.S. Border Officials via CPIC (OIPC Ontario, Canada)**

An OIPC investigation revealed that Ontario police services were disclosing information



about suicide attempts to U.S. agencies under an international data-sharing agreement. Subsequent court action and settlement discussions led to privacy-protective changes to national computer systems (Canadian Police Information Centre (CPIC)), the removal of a majority of such Toronto police generated information from CPIC, the suppression of all but a few such entries from U.S. access and fairer CPIC entry and removal procedures.

**B11: The First Philippine Data Protection Officers' Assembly – DPO1 (Philippines)**



Serving as an initiative on compliance and enforcement as well as on education and advocacy, the National Privacy Commission (NPC) has organized **DPO1: The First Philippine Data Protection Officers' Assembly** for government on April 5, 2017. In just over a year following its establishment, the NPC was able to convene representatives from 295 government agencies through DPO1 and secure their compliance to designate data protection officers (DPOs). The NPC also launched its official website during the event.

**B12: Data Protection by Design Award (Catalan, Spain)**

APDCAT has launched a competition to find

*An OIPC investigation revealed that Ontario police services were disclosing information about suicide attempts to U.S. agencies under an international data-sharing agreement*

**AWARD ENTRIES: DISPUTE RESOLUTION, COMPLIANCE AND ENFORCEMENT (CONTD.)**



an app or technological solution developed anywhere that best showcases “applications or systems that improve the implementation of security measures, facilitate compliance with legal obligations in the field of data protection, strengthen people’s control over their own information and, in general, make the management of privacy easier.”

**B13: The joint investigation of the Ashley Madison Breach (Australia, Canada and USA)**



Conference members FTC, the Office of the Privacy Commissioner of Canada and the Office of the Australian Information Commissioner carried out a joint investigation of the data breach involving AshleyMadison.com, operated by ruby Corporation, f/k/a Avid Life Media, ruby Life Inc., and ADL Media Inc. The data breach affected more than 36 million consumers and included sexual preferences, account information, email addresses, security questions and answers, and in some cases billing information. The authorities cooperated under the APEC Cross-border Privacy Enforcement Arrangement (CPEA). To facilitate cooperation with its Canadian and Australian partners, the FTC relied on key provisions of the U.S. SAFE WEB Act that allow the FTC to share information with foreign counterparts to combat deceptive and unfair practices that cross national borders.

This collaborative approach was both efficient and effective. The partnership allowed the 3 authorities to take advantage

of differences in legislation, and even time zone differences (on occasion literally working 24 hours a day) to address this global privacy risk as a global team. By pooling resources, the 3 authorities were able to work quickly, gathering information both separately and jointly, including through a joint site visit, and avoiding duplication of effort. This joint enforcement approach led to a more holistic outcome, addressing more issues than any one authority would have alone, in the increasingly overlapping spectrum of privacy and consumer protection. The result was greater impact – both on the activities of ruby Corporation, and in terms of clarifying standards and expectations globally – in particular, with respect to security safeguards.

**B14: Necessity Toolkit (EDPS, European Union)**



**Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit (Necessity Toolkit)**

The toolkit aims to help the EU legislators to better assess the necessity of new legislative measures which limit the right to data protection and other fundamental rights, such as the right to privacy. It provides a practical step-by-step checklist, exemplifying the criteria for applying the necessity principle.

**B15: Access Rights and Responsibilities Guide (Ireland)**

Access requests account for the greatest number of complaints to the Irish DPC every year, accounting for 56% of all complaints

*Data Protection by design award introduced by APDCAT to showcase applications or systems that improve security measures, comply with data protection and strengthens user’s controls over their information.*



# ICDPPC

International Conference of Data  
Protection & Privacy Commissioners

ICDPPC

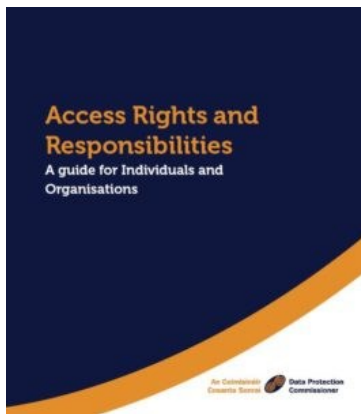
Email: [ExCoSecretariat@icdppc.org](mailto:ExCoSecretariat@icdppc.org)

Follow us on twitter [@ICDPPCsec](https://twitter.com/ICDPPCsec)

SHARE THE  
NEWS

Please share the  
newsletter with  
other staff.

## AWARD ENTRIES: DISPUTE RESOLUTION, COMPLIANCE AND ENFORCEMENT (CONTD.)



received. We decided that a renewed awareness raising campaign was needed, so that access rights and responsibilities would be highlighted in advance of GDPR. The PDF guide that we published, along with the infographic 'check list' for individuals and organisations has been praised for its clear use of language, and its comprehensible format.

### B16: First private sector audit (British Columbia, Canada)

This initiative was the first private sector audit undertaken by the Office of the Information and Privacy Commissioner (OIPC). It followed a complaint to our Office about a medical clinic in the Lower Mainland. Beginning in June 2016, auditors examined the organisation's privacy management program and its use of video and audio surveillance. The key finding was that the clinic is not authorized to collect personal information through its video and audio surveillance system.

*First private sector audit management program and its use of video and audio surveillance. The key finding was that the clinic is not authorized to collect personal information through its video and audio surveillance system.*

