RESOLUTION TO ADDRESS THE ROLE OF HUMAN ERROR IN PERSONAL DATA BREACHES

41st International Conference of Data Protection and Privacy Commissioners
October 2019, Tirana, Albania

SPONSOR:

- Office of the Australian Information Commissioner, Australia

CO-SPONSORS:

- Autoriteit Persoonsgegevens, The Netherlands;
- Comissão Nacional de Protecção de Dados, Portugal;
- Commission Nationale de l'Informatique et des Libertés, France;
- Data Protection Commission, Ireland;
- Information Commissioner's Office, United Kingdom;
- National Institute for Transparency, Access to Information and Personal Data Protection, Mexico;
- National Privacy Commission, The Philippines;
- Office of the Privacy Commissioner, New Zealand;
- Office of the Privacy Commissioner of Canada, Canada

The 41st International Conference of Data Protection and Privacy Commissioners:

NOTING that, in order to protect the privacy of individuals and to build trust in the data economy, a global response from data protection and privacy authorities and organisations is required due to the growth in the number, size and severity of personal data breaches, the commonality of their causes, the international nature of their consequences and the harm that can result from them;

ACKNOWLEDGING that the implementation of personal data breach notification schemes in some member jurisdictions has led to a significant increase in the reporting of personal data breaches and that has provided valuable insights into their causes, and allows for a better understanding of how they might be avoided and the identification of potential prevention strategies;

HIGHLIGHTING that notifications of personal data breaches and regulatory action in some member jurisdictions as well as national and international studies show that personal data breaches often involve human error, specifically, employees unintentionally disclosing personal data to unauthorised recipients or individuals being deceived into compromising user credentials that allow access to information and systems ('human error');

RECOGNISING that a principle common to privacy and data protection laws around the world is that personal data should be protected by appropriate security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure;

AFFIRMING that the predominance of the role of human error in personal data breaches emphasises the importance of building workplace cultures where privacy and security are organisational priorities, including through the periodic implementation of training, education and awareness programs, building privacy into the design, operation and management of systems and practices, and the implementation of technological solutions;

NOTING that the International Conference of Data Protection and Privacy Commissioners has previously identified the need to work towards global policy, standards and models and to ensure greater levels of regulatory cooperation to enhance the efficient prevention, detection, deterrence and remedy of privacy and data protection issues and to ensure consistency and predictability in the system of oversight in the data economy;

MINDFUL of the ongoing work of the Organisation for Economic Co-operation and Development (OECD) to ensure that digital security and privacy protection fosters the development of the digital economy, and to improve the evidence base for security and privacy policy making, including comparability in personal data breach notification reporting;

NOTING that the International Conference of Data Protection and Privacy Commissioners Census from 2017 showed that personal data breach notification schemes vary across member jurisdictions and include not having a personal data breach notification system, a voluntary personal data breach notification system and mandatory personal data breach notification requirements that apply generally and to particular sectors;[1]

HIGHLIGHTING that the collection, classification, analysis and publication of statistics on personal data breaches notified to data protection and privacy authorities, including their causes, is essential for the development of both a global policy and a response to the causes of personal data breaches;

RECALLING that the 31st International Conference of Data Protection and Privacy Commissioners in 2009 adopted the International Standards on the Protection of Personal Data and Privacy ('The Madrid Resolution') which included principles directed to the protection of personal data through the implementation of appropriate technical and organisational measures (Principle 20 – Security measures) and proactive measures, including

[1] International Conference of Data Protection and Privacy Commissioners Data Protection Metrics Working Group, *Counting on Commissioners: High level results of the ICDPPC Census 2017* (2017) https://icdppc.org/wp-content/uploads/2017/09/ICDPPC-Census-Report-1.pdf.

periodic implementation of training, education and awareness programs and audits by independent parties (Principle 22 – Proactive Measures);

RECALLING that the 32nd International Conference of Data Protection and Privacy Commissioners in 2010 resolved to encourage the adoption of Privacy by Design's Foundational Principles as guidance to establishing privacy as an organisation's default mode of operation;

THE 41st INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS resolves to call upon:

1) THOSE ICDPPC MEMBERS that collect, analyse and publish statistics on the personal data breaches notified to them under a voluntary or mandatory personal data breach notification scheme to:

   (i) classify and report on the causes of personal data breaches, and consider including classifications for those that are the result of human error; and

   (ii) continue to consider any recommendations made by expert bodies such as the OECD and the ICDPPC Data Protection Metrics Working Group on the measurement of personal data breaches.

2) ALL ICDPPC MEMBERS to promote appropriate security safeguards to prevent human error that can result in personal data breaches, which may include the following:

   (i) Building workplace cultures where privacy and personal data security are organisational priorities, including through the periodic implementation of training, education and awareness programs for employees on their privacy and security obligations and the detection and reporting of threats to the security of personal data;

   (ii) Establishing robust and effective data protection and privacy practices, procedures and systems, including by:

      a. building privacy into the design, operation and management of systems and practices, and investing in the improvement of the overall security posture in line with known security risks; and

      b. at a user level, implementing technologies to complement user education in mitigating against the risk of compromised credentials and unintentionally disclosing personal data to unauthorised recipients;

   (iii) Evaluating privacy practices, procedures and systems to ensure continued effectiveness, including by implementing a program of proactive review, including system monitoring and auditing.

3) ALL ICDPPC MEMBERS to liaise with relevant international and regional networks to promote this Resolution.

4) ORGANISATIONS (INCLUDING GOVERNMENT AND BUSINESS) to understand and recognise that personal data breaches often involve human error and act to implement appropriate security safeguards, which may include those outlined in clause (2) above.

EXPLANATORY NOTE

This Resolution is a further step towards a global ICDPPC policy on the prevention of personal data breaches, by focusing on the security safeguards that are appropriate to take against the cause of many personal data breaches – human error.

The Resolution is timely given that the large increase in notifications in ICDPPC member jurisdictions with mandatory data breach notification schemes is confirming what has been known for some time – that many personal data breaches are caused or triggered by human error.[2]

The first call to action seeks to build the evidence base provided by data breach notification. A 2017 survey of statistical practices in relation to breach notification undertaken with the cooperation of ICDPPC Data Protection Metrics Working Group showed there is little commonality in the way that those surveyed classified personal data breaches notified to them, and suggested that there was a good scope for work to assist authorities to develop common practices for classifying the nature of breaches.[3]

The Organisation for Economic Co-operation and Development (OECD) has identified similar issues as part of its ongoing work to improve the evidence base for security and privacy policy making. The OECD's work in this area has included the development of a questionnaire, with the support of the ICDPPC, to inform a feasibility study on what data privacy and data protection authorities should collect and report to enhance comparability in personal data breach notification. The questionnaire includes consideration of the classification of types of data breaches. In particular, whether data should be classified according to 'high level classifications' or more specific 'incident type' sub-categories.[4]

The call to action is directed only to those members that collect, analyse and publish statistics on personal data breaches notified to them, acknowledging that notification systems vary across member jurisdictions, with some member jurisdictions having no notification system or a practice of reporting statistics on notified personal data breaches.

The second call to action is directed to all ICDPPC members, individually. It recognises the predominance of human error and asks ICDPPC members to not only promote to organisations the implementation of effective ICT security measures, but also measures to

[2] Identification of human error as the cause of many personal data breaches pre-dates the implementation of mandatory data breach notification schemes, and has been reported as a known cause of personal data breaches by member jurisdictions that have voluntary or no data breach notification schemes, as well as in reports by private sector and research organisations.

[3] Blair Stewart, *Improving the measurement of digital security incidents (Privacy authority perspectives): Taking stock and priorities for action* (18 April 2017) https://icdppc.org/wp-content/uploads/2017/04/Breach-notification-statistics-survey-report-18-April-2017.pdf.

[4] See, for example, OECD Working Party on Security and Privacy in the Digital Economy (WPSDE), *Promoting Comparability in Personal Data Breach Notification Reporting: Findings from an OECD Survey of Privacy Enforcement Authorities* (13-14 November 2018) DSTI/CDEP/SPDE(2018)13; OECD WPSPDE, *OECD Workshop 'Improving the Measurement of Digital Security Incidents and Risk Management': Draft Summary and Main Points* (30-31 October 2017, Paris) http://www.oecd.org.

address human error to ensure the ongoing effectiveness of ICT measures and to address the human factor.

The call to action endorses a non-exhaustive list of safeguards and approaches that are well-known to ICDPPC members,[5] and that are commonly acknowledged to be appropriate security safeguards in certain circumstances against such risks as loss or unauthorised access, destruction, use, modification or disclosure of personal data.[6]

The third call to action is directed to all ICDPPC members and seeks to ensure that the Resolution is promoted through relevant international and regional networks.

The fourth call to action is directed to organisations (both government and business). It seeks to highlight the role of human error in personal data breaches and the security safeguards that may be appropriate to take against it.

While none of the security safeguards set out in the Resolution will be new to ICDPPC members, their inclusion signals a further step towards a global policy and a response to the known causes of personal data breaches.

[5] See, for example, 31st International Conference of Data Protection and Privacy Commissioners, *International Standards on the Protection of Personal Data and Privacy* ('The Madrid Resolution'), Principle 20 – Security measures and Principle 22 – Proactive Measures.

[6] The Security Safeguards Principle is a core privacy principle set out in the 1980 *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* as well as the 2013 revised *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. The Principle states: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.