PROMOTING COMPARABILITY OF PERSONAL DATA BREACH NOTIFICATION REPORTING

Suguru Iwaya, Policy Analyst, Digital Economy Policy Division, STI, OECD

BETTER POLICIES FOR BETTER LIVES

Project's background

- Based on the Ministerial Declaration on the Digital Economy in 2016
- Aims at evidence base for security and privacy policy making through compatible DBN reporting
- Survey questionnaire was circulated with the support from the GPA, APPA and EDPB from June 2019 to February 2020

Survey from June 2019 to February 2020

- The survey provides a wide range of information:
  A. General questions and authority profile
  B. Authority's funding and resources
  C. Personal data breach notification reporting law, jurisdiction and exemptions
  D. Personal data breach annual reporting
  E. Number of personal data breach notifications received
  F. Personal data breach notification by sector
  G. The nature and type of the personal data breach incident
  H. The types of personal data affected
  I. Monetary fines and other penalties
  J. Measures taken to prevent or mitigate risk and impact evaluation
  K. Use of PDBN data

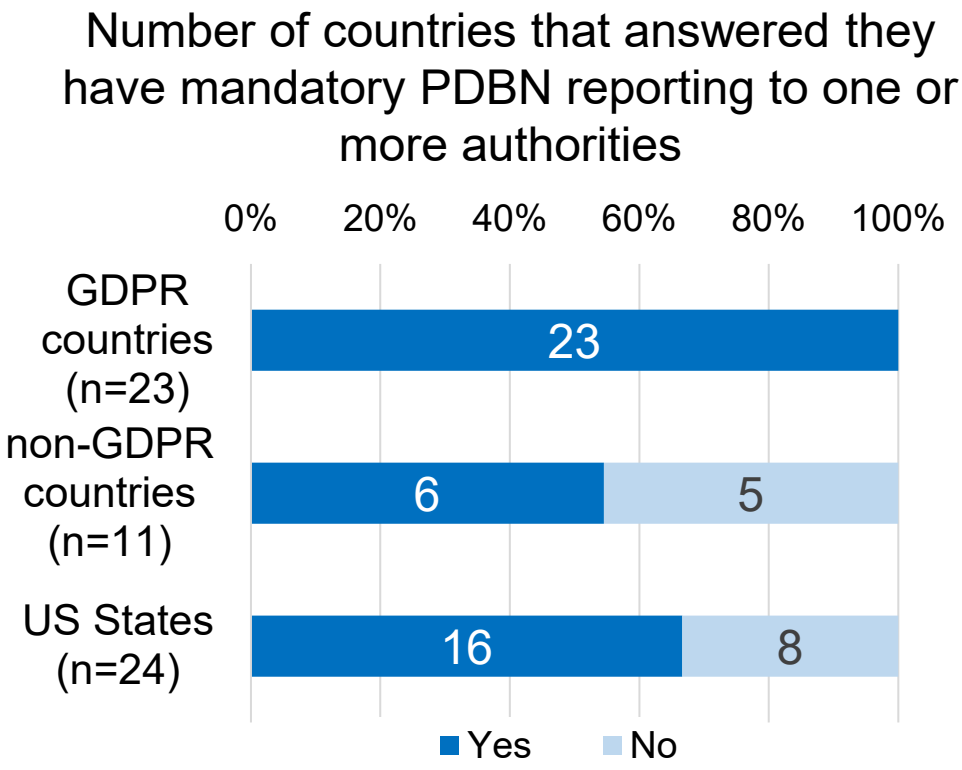
- Total of 35 countries that participated in the survey:
  – 32 OECD members (including 24 States reporting for the United States) and 3 non-members

What is data breach notification (DBN) ?

- Data breach
  - The general term ‘data breach’ refers to security incidents that impact on **non-personal data** as well as on **personal data**.
  - A ‘personal data breach’ can be described broadly as being a breach of security that leads to the unintended or unauthorised destruction, loss, alteration, disclosure of, or access to personal data.
- Personal Data breach notification
  - The regulatory requirements that require organisations to notify **the authority** and/or to **the affected individuals** following a personal data breach.
  - These requirements are **mandatory** or **voluntary**.
  - The **window** though which the authority and individuals can obtain information on data breaches.

Trend towards mandatory PDBN reporting

- Trend towards mandatory personal data breach notification to the authority.
- In some jurisdictions mandatory PDBN reporting apply differently depending on the sector
- Thresholds to notify are generally based on a risk-based approach
- There are variations in mandatory PDBN reporting to data subjects



Internationally comparable data metrics

Total number of data breaches reported to the authority

Nature of causes

- Malicious or non-malicious
- Internal or external
- Human error

Specific causes

- Loss of IT equipment
- Mailing
- Hacking
- Technical error
- Theft
- Improper disposal of documents
- Unauthorised access

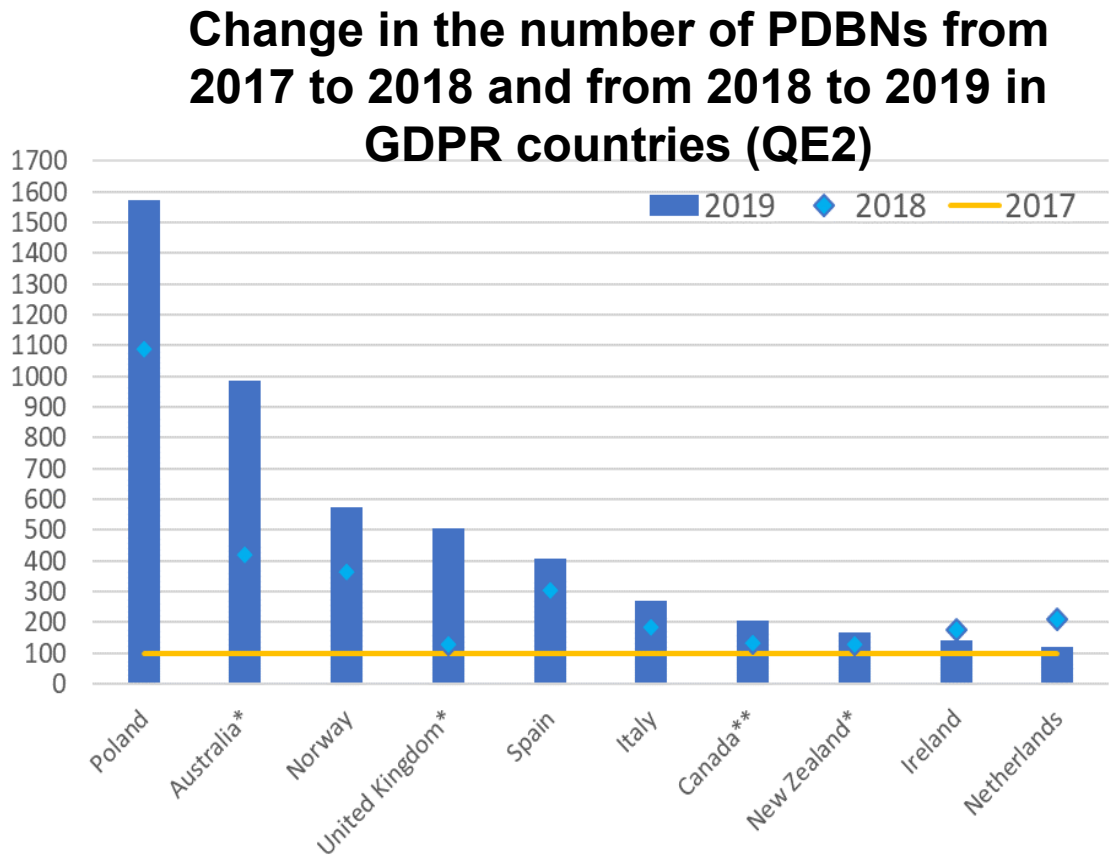
Types of data breached

- Personal credential data
- Sensitive data
- Financial data

Information on encryption of data breached

Total number of data breaches reported to the authority

- Number of PDBNs generally increased from 2017 to 2019.
- Significant increase can probably be attributed to introduction of mandatory PDBN.



* Numbers of PDBNs in 2017 are normalised to 100. Numbers of PDBNs in 2018 and 2019 are compared against this normalised value. To avoid overrepresentation of changes from small numbers, data less than 50 was eliminated from the calculation.

Recent trends of the total number of DBs

- Both increase and decrease in the number of PDBNs were observed.
  - e.g. DBNs reported in 2020 increased by 10% (Irish Data Protection Commission, 2021)
  - e.g. DBNs reported in 2020 decreased by 26% (UK ICO, n.d.)
- Impacts of mega breaches are increasing.
  - e.g. while the number of publicly disclosed breaches shrank by 48% in 2020, the number of records increased by 141% compared to 2019 (RiskBased Security, 2021)
- Other complementary indicators such as number of DBNs that meet the reporting threshold and number of the affected data subjects have gained importance.

Nature of causes

- Internationally comparable data items on nature of causes of DBs reflect the high-level trend of DBs
  - Malicious or non-malicious
  - Internal or external
  - Human error
- High-level trend continues after the survey period
  - e.g. Common causes of DBs: ‘email error’,followed by ’other’, ‘website error’, ‘hacking’ (Privacy Commissioner New Zealand, 2020)
  - e.g. are malicious attack (52% of breaches), system glitch (25%), and human error (23%) (Ponemon Institute and IBM Security, 2020).
  - e.g. From November 2019 to October 2020, the top actions that caused data breaches were ‘hacking’, ‘social’, ‘error’, and ‘malware’ (Verizon, 2021).

Specific causes

- Internationally comparable data items on specific causes
  - Loss of IT equipment
  - Mailing
  - Hacking
  - Technical error
  - Theft
  - Improper disposal of documents
  - Unauthorised access
- Specific causes may need to be complemented by the explanation on the current threat environment.
  - the inclusion of “unauthorized disclosure” to reflect misdelivery and misconfiguration
  - An explanation to “theft” to clarify that it involves the theft of credentials through social engineering or reuse of stolen credentials for phishing

Types of data breached

- Internationally comparable data items on the types of data breached
  - Personal credential data
  - Sensitive data
  - Financial data
- The comparable data items capture the threat environment
  - e.g. “Personally Identifiable Information” is the top that 80% of breaches involved (Ponemon Institute, 2020); Top 2 were “Names”(46%) and Email (32%) in 2020 (Risk Based Security, 2021)
  - e.g. Medical data, financial data steadily increased since 2018 (Risk Based Security, 2021)
- “unknown” is enhancing the presence in the types of data breached