APEC
Asia-Pacific
Economic Cooperation

Advancing Free Trade
for Asia-Pacific Prosperity

2021 APEC Virtual Forum on Improving Cross-Border Effectiveness of Personal Data Breach Notification Systems

APEC Digital Economy Steering Group

February 2022

APEC

Asia-Pacific
Economic Cooperation

2021 APEC Virtual Forum on Improving Cross-Border Effectiveness of Personal Data Breach Notification Systems

Republic of Korea | 8 September 2021

APEC Digital Economy Steering Group

February 2022

APEC Project: DESG 01 2020A

Produced by
Jung-soo Byun and Beomsoo Kim
Project Overseer

Personal Information Protection Commission
209 Sejong-daero, Jongno-gu, Seoul 03171,
Republic of Korea

Barun ICT Research Center, Yonsei University
New Millennium Hall 417, 50 Yonsei-ro, Seodaemun-gu, Seoul 03722,
Republic of Korea

For
Asia-Pacific Economic Cooperation Secretariat
35 Heng Mui Keng Terrace
Singapore 119616
Tel: (65) 68919 600
Fax: (65) 68919 690
Email: info@apec.org
Website: www.apec.org

© 2021 APEC Secretariat

APEC#222-CT-04.1

TABLE OF CONTENTS

ABSTRACT

The Personal Information Protection Commission (PIPC) and Yonsei University's Barun ICT Research Center jointly held the 2021 APEC Virtual Forum on Wednesday, 8 September with the umbrella theme of "Improving Cross-Border Effectiveness of Personal Data Breach Notification Systems." As the need to create a secure environment for the use of personal information in online transactions increases, this APEC Forum aimed to offer a venue to listen to and discuss with representatives from six APEC member economies. The key theme of this Forum was the “Data Breach Notification.” This is a policy that aims to reduce secondary damage by ensuring that when sensitive personal information has been breached, subjects are notified and provided detailed instructions on how to respond and remedy the situation.

With COVID-19, online transactions have become more widespread, and the international movement of personal data is growing evermore significant. Thus, the need to expand the personal data breach notification is growing to become more prominent. As the hosting economy of the 2021 APEC Virtual Forum, the Republic of Korea hopes this Forum was a valuable place to share meaningful content and insights into data breach notification systems.

I. BACKGROUND

The digital economy is enabling the cross-border use of products and services. Accordingly, the Asia-Pacific economy needs to establish an environment for safe use of personal data for active participation in the digital economy. The objective of this project is to share an understanding of and opinions on the current situation of each personal data breach notification of the Asia-Pacific economies. It aims to open a Forum to identify the necessity, direction, and basic principles of the personal data breach notification system to invigorate the digital economy of APEC member economies.

Trust in data management is important for the sustainable development of the digital economy. The APEC Privacy Framework 2015 promoted the necessity of security safeguards against the risk of data breach in Principle 7 (Security Safeguards). This project aims to supplement the previous APEC initiative and reinforce the competencies of member economies so that the Asia-Pacific economy can use personal data safely and fairly at home and abroad. As a result, APEC economies are expected to provide users with an environment for safe use of personal data, and therefore contribute to the development of the digital economy.

This project consisted of an online Forum for APEC economies on “Improving Cross-Border Effectiveness of Personal Data Breach Notification Systems.” It was held on Wednesday, 8

September 2021, from 12:00PM to 15:00PM (Korea Standard Time, GMT +9) via ZOOM.

Through the participation of APEC member economies, this Forum contributes to reinforcing the personal data capacity of its APEC members, as well as improving knowledge of personal data breach notification systems and methods in different economies by doing the following:

> 1) Improving understanding of problems related to personal data conflicts in digital trade, including cross-border enforcement issues
>
> 2) Facilitating awareness of personal data breach notification and discussing systems and policies that can prevent secondary damage to users in case of international problems
>
> 3) Strengthening the structure of the digital economy through the sharing of personal data breach notification systems, policies, and processes of solving problems

Of the 12 economies that attended the Forum including the United States, Chinese Taipei, the Philippines, Japan, Indonesia and Peru, the six representative economies that presented are as follows: The Republic of Korea, Singapore, Chile, Canada, Australia, and Hong Kong, China. To indicate this forum's gender ratio, the number of female participants is 38 (54.3%), including 2 female speakers, and the number of male participants 32 (45.7%) including 6 male speakers. This Forum is the international conference on the subject of the data breach notification act. The objective of this project is to discuss the current situations and policies of APEC member economies in regard to personal data breach notification systems in an effort to globally share responses to personal data breaches in the digital environment. The various types of stakeholders for data breach, and personal data protection experts from firms, private sectors, and civil society participated in the Forum.

This Forum is expected to contribute greatly to the promotion and advancement of data breach notification acts worldwide as economies that have implemented data breach notification and economies that are preparing for the implementation of it can actively participate.

II. SUMMARY OF THE DISCUSSION

2.1. Current Status of APEC Economies' Personal Data Breach and Notification Systems I

2.1.1. Singapore's Data Breach Notification

1. Personal Data Protection Act in Singapore

The data breach notification system in Singapore was first introduced to Personal Data Protection Commission (PDPC) in February 2021. Singapore's Personal Data Protection Act was also amended in February and has governed the collection and disclosure of personal data by private organizations in Singapore. The Personal Data Protection Commission set the baseline standard for data protection in the private sector. In addition to PDPC, Singapore also implemented other obligations under laws including those that cover specific sectors. PDPC also covers Data Protection Provisions and 'Do Not Call' Provisions which enable individuals to opt out of receiving specified messages, such as unsolicited marketing messages in the form of text messages or voice calls sent to Singapore telephone numbers.

2. Mandatory Data Breach Notification in Singapore

Under the mandatory data breach notification in Singapore, organizations are required to notify PDPC and provide access to cases of data breach to make them notifiable. A notifiable breach is a breach that is likely to result in significant harm to the affected individuals or has met the threshold of a significant scale of more than or equal to 500. Organizations are also required to notify the affected individuals if they assess that the data breach is likely to result in significant harm to that individual. However, if technological protections are in place or remedial actions had been taken to render such breaches to be relatively harmless to individuals, organizations can choose not to notify the affected individuals.

3. Data Breach Notification Timeline

After a breach is known, the organization should assess if it is notifiable within 30 days. This is to allow time for them to conduct an internal investigation to determine the scale and harm of that breach. When the organization determines that the breach is of a significant scale or harm, it must report to PDPC within 3 calendar days. If the organization is going to notify individuals, it should notify PDPC before or at the same time as its notification to the affected individuals, if not ahead of time.

4. Rising Number of Data Breach Notification Cases

With the mandatory data breach notification coming into force, PDPC has experienced at least three times the increase in the number of DBN (data breach notification) cases, compared to the same period last year. In June this year, PDPC exceeded the number of the DBN cases that they received in the year of 2019 and 2020.

5. Common Causes of IT-related Data Breaches

About half of the data breaches resulted from cyber or IT-related causes and attacks. The five commonly observed gaps in IT system management and processes resulting in such breaches include malware & phishing attacks, configuration issues, coding issues, inadequate implementation of security controls & assignment of responsibility, and unsecure account & passwords management.

6. Filing a DBN Case on PDPC Website: Self-Assessment Questionnaire

To provide guidance and to make it easy and intuitive for organizations, PDPC constantly enhances its DBN guide map and tools. They have recently included a self-assessment questionnaire to help users navigate the requirements easily. This questionnaire was designed to assist organizations to determine if the data breach incident is a notifiable breach. The questions serve as a guide for the organizations to assess if the data breach incident has met the threshold of a significant scale or harm. After answering the questions in the assessment tool, organizations will be advised if the breach is notifiable based on their responses to the questions. PDPC also provides necessary links to their online data breach notification portal that might be applicable.

7. Data Breach Notification Form

According to the PDPC's DBN form, PDPC first understands that when data breaches occur, organizations could be in contravention of multiple sectorial regulations. PDPC works with sector regulators including the Monetary Authority of Singapore and Ministry of Health in Singapore to enable them to be notified in real time simultaneously. They also notify the Cyber Security Agency if the data breach is found to be related to a cyber incident. This enables efficient cross-agency cooperation to ensure a quick flow of data between them so that they can all react in a timely manner. Secondly, PDPC also understands that there are different kinds of information that they collect, which is relevant to the different nature of data breaches. To prevent the form from being too long to answer and too daunting for organizations in distress to fill out, they have implemented dynamic features so that only the specific details related to the nature of that particular breach are collected for assessment. PDPC is also constantly working to enhance its form. In order to include more features that will streamline organizations' reporting processes even further, they are also continually working with more sector regulators. They also expand their network of notifications to ensure that they can effectively tackle these breaches in their respective space as well.

To take a closer look at how their data breach notification form works, at the beginning of the form, organizations have to indicate the sector that the data breach is related. Once selected, the information on the form will be sent to the relevant sector regulator immediately. For example, if an organization chooses that a data breach case is related to the financial sector, it will be sent to PDPC and onwards to MAS (Monetary Authority of Singapore) regulated entity at the same time. Likewise, if an organization chooses the health sector, the information will be sent to PDPC and to the Ministry of Health at the same time. Once an organization has selected the related sector, they have to move on to select the cause or suspected cause of the incident. If it has selected the cause of the data breach incident to be a cyber incident, for example, then it will move forward to the page with several questions relevant to the cyber incident. This is to ensure that only the relevant information is being captured by PDPC and not to overload the data protection officers or organizations to face a form that is too long and complicated.

8. Managing Data Breach Notification Cases

When DBN cases are received, PDPC case officers communicate with the organizations to ensure that all necessary information is received. When the necessary responses are collected from the organizations, they make an assessment to determine if it is a Prima Facie case against the organization or any contravention of the act. If the case officers refer the case to be investigated, the investigation team exercises their legal power to compel the organization to produce the necessary information needed for the investigation to determine if the organization had contravened any act or obligation. If necessary, enforcement action is taken against the organization.

9. Active Enforcement Framework

The actions that PDPC can take if cases are found to be in contravention of PDPA include suspension or discontinuation, voluntary undertaking, expedited breach decision, and full investigation process. Suspension or discontinuation is for cases where the impact is assessed to be low. The voluntary undertaking is to allow organizations with demonstrable accountability practices and effective remedy plans in order to implement their remedy plans within a specific time. Expedited breach decision is for the organization that has provided an upfront voluntary admission of reliability, providing PDPC with the relevant facts of the incident and complying with the directions set by PDPC. However, if all of these three measures fail, PDPC will launch into the full investigation process.

10. Full Investigations Decisions

There are several kinds of decisions that PDPC may take after the full investigation process. It includes no breach, warning, directions, financial penalty, and directions & financial penalty. To elaborate more on directions & financial penalty, under the PDPA, PDPC can direct organizations to take collective actions to remedy for the contravention of the PDPA to prevent or reduce the harm to the affected individuals. PDPC may also require the organizations to pay a financial penalty for any intentional or negligent contravention of the provisions. The maximum penalty prescribed under the PDPA is either one million or ten percent of the organization's annual turnover in Singapore.

11. Publication of Enforcement Decisions

PDPC provides the enforcement decisions published on their website. These decisions provide valuable insight and lessons for the organizations so that they can implement preventive measures for similar occurrences. This also can serve as a reminder to individuals and organizations of their respective rights and obligations under the PDPA. In the longer term, PDPC aims to promote accountability among organizations to build and strengthen consumer trust and confidence.

2.1.2. Australia's Notifiable Data Breaches Scheme

1. The Office of the Australian Information Commissioner (OAIC)

The OAIC is an independent statutory body within the Australian Attorney-General's portfolio. Their purpose is to promote and uphold privacy and information access rights by:

- protecting the public's right of access to documents under the Australian *Freedom of Information Act 1982*, and

- ensuring organizations and Australian Government agencies follow the Australian *Privacy Act 1988* when handling personal information.

2. The Privacy Act in Australia

The Privacy Act deals with information privacy and provides protections for the collection and handling of personal information. It seeks to prevent individuals from being subject to arbitrary interferences with their personal information and protect them from harm that may stem from the misuse of their information. It also facilitates the free flow of information, including across borders, by ensuring that the protection of the privacy of individuals is balanced with the interests of organizations in carrying out their functions.

The Act applies to most Australian Government agencies and a range of organizations. There are some exemptions such as state and territory government agencies, and businesses with an annual turnover of $3 million or less.

3. Notifiable Data Breaches Scheme Framework

One of the main focus areas for the OAIC is ensuring the security of personal information and the Notifiable Data Breaches (NDB) scheme is now a well-established mechanism for achieving this.

The NDB scheme was introduced in February 2018, making it one of the major changes to the Privacy Act in recent years. Under the scheme, organizations that are covered by the Privacy Act must notify affected individuals and the OAIC when they experience a data breach that is likely to result in serious harm to individuals whose personal information is involved.

The key objective is to protect individuals by allowing them to act quickly to prevent the risk of serious harm when their personal information is compromised. This might mean giving them the opportunity to quickly change passwords or to cancel credit cards, to monitor their accounts more closely, and be on a higher alert for scams. The scheme also motivates organizations to improve their security standards for personal information and to be accountable for privacy. In doing this, it works to build trust in personal information handling across the private and public sectors.

Another benefit that arises from the NDB scheme is the information that the OAIC receives. They have increased visibility about the risks and threats currently facing personal information.

This allows the OAIC to better inform policymakers, regulators, law enforcement, and researchers about trends in the handling of personal information.

4. What Is an Eligible Data Breach?

Under the Privacy Act, an eligible data breach occurs when:

- there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an organization or agency holds
- this is likely to result in serious harm to one or more individuals, and
- the organization or agency hasn't been able to prevent the likely risk of serious harm with remedial action

The scheme provides organizations with the opportunity to take positive steps to address a data breach in a timely manner, and thus avoid the need to notify. A data breach is no longer considered to be an eligible data breach if the organization takes steps that prevent the likely risk of serious harm eventuating. For example, if personal information is lost, the remedial action is adequate if it prevents that information from being accessed or disclosed without authorization.

5. Trends in Data Breach Notifications in Australia

The OAIC publishes detailed statistics about notifications received under the NDB scheme to help organizations and the public understand current trends and risks. They report on the industry sectors that notify the most breaches, the sources of data breaches, areas for improved practice, and data breach response best practices. These reports can be found on the OAIC website and provide organizations with clear information on the causes of data breaches so that they can assess and improve their security posture and processes to minimize the risk of a data breach from occurring.

6. Notifiable Data Breaches Report: January to June 2021

Since the start of the NDB scheme, around 60% of data breaches notified to the OAIC have been caused by malicious or criminal attacks, the majority of which have been caused by cyber security incidents such as phishing, ransomware, and hacking.

Data breaches caused by human error have accounted for about a third of the notifications the OAIC has received. Some common examples of human error include staff of organizations sending personal information to the wrong recipient via email or failing to use the blind carbon copy or BCC function when sending group emails. The OAIC increasingly sees this human element is a factor in malicious or criminal attacks such as those that involve an element of social engineering.

Most data breaches notified to the OAIC affected 5,000 individuals or fewer. In their latest report, 65% of the data breaches affected 100 individuals or fewer, and 44% affected between 1 and 10 individuals.

Across the life of the scheme, the OAIC has received notifications from almost all sectors of the Australian economy. There are a handful of sectors that have routinely appeared in the top 5 sectors by notifications. Health service providers have notified the most data breaches to the OAIC, followed by the finance sector. The OAIC is working with the health and finance sectors to inform them of the types of matters being notified. They have also developed a joint action plan with other Australian Government agencies to help the health sector contain and manage data breaches.

7. Emerging Themes and Challenges

The themes and challenges that have emerged from the NDB scheme include the assessment of suspected data breaches, evolving technical threats, the growth of data on the dark web, and managing the human factor.

Under the Privacy Act, organizations must conduct an assessment of a suspected data breach if there are reasonable grounds to suspect that there may have been an eligible data breach. It is necessary even if there are insufficient reasonable grounds to believe that an eligible data breach has actually occurred. However, there are cases where organizations don’t understand their information environment and this leads to them being constrained when it comes to conducting a timely and thorough assessment and investigation of a suspected data breach. For example, according to the OAIC’s latest statistics report, some organizations are not reporting data breaches caused by ransomware because they say that they possess a ‘lack of evidence’ that data has been accessed or exploited. Organizations must understand the personal information they hold and where it is located to be able to undertake a meaningful assessment of a data breach.

Another issue the OAIC focused on in the latest report is the evolving cyber security threat environment. According to the report, 43% of data breaches notified to the OAIC in the first half of this year resulted from a cyber-security incident. Of note, ransomware incidents increased by 24%. Organizations need to put in place measures that guard against common threats such as ransomware, phishing, and impersonation fraud and these measures need to be robust, especially as the growth of data on the dark web has meant that malicious actors increasingly hold sufficient personal information to circumvent baseline controls.

There is no strict definition of serious harm in the legislation. It may include serious physical harm, psychological, emotional, financial, or reputational harm. Therefore, organizations must assess the risk of serious harm holistically. They have to take into account the likelihood of the harm that could result for individuals whose personal information was part of the data breach, and the potential consequences of the harm.

8. Guiding Regulatory Action

In Australia, the NDB scheme has been a useful mechanism for pushing organizations that handle personal information to a more proactive stance when it comes to data breaches. Most organizations generally engage with the scheme and take steps to remedy breaches and mitigate harm.

The OAIC interacts heavily with organizations that notify data breaches to ensure that they fully comply with the requirements and implement new practices, processes, and technologies to reduce the risk of a data breach reoccurring.

The OAIC has been administering the NDB scheme for over 3 and a half years and has provided education advice and reports on the known causes of notifiable data breaches. They take the position that the scheme is now in a mature phase and expect that organizations will report breaches in line with the legislative requirements. They also expect that organizations will take proactive steps to improve the security of personal information they hold.

2.2. Current Status of APEC Economies' Personal Data Breach and Notification Systems II

2.2.1. Personal Data Breach Notification in Republic of Korea: Status Quo and Challenges

1. Personal Data Breach Notification Regulations in Korea

Korea has a Personal Information Protection Act, enforced by the Personal Information Protection Commission (PIPC). This commission covers both the public sector and private sector. In the past, Korea had multiple laws governing the IT sector, and financial and banking sector, but from the year 2020, the PIPC oversees all issues in public and private sectors. The commission works with the Ministry of the Interior and Safety, financial services commission, other ministries in the government, and private sector organizations, including global and domestic corporations.

2. Key Components of Data Breach Notification

The Personal Data Breach Notifications (PDBN) in Korea focuses on mandatory notifications to individuals and privacy enforcement authorities. Korea believes that notification to individuals is an important component to personal data privacy of Korean citizens. Because the enforcement authorities enforce the act with a legal framework, and promote compliance with data controllers, there are limits to protecting the individual's privacy. To overcome such limitations, Korea believes that individuals can act and participate to improve personal privacy. When Korea was working on this PDBN regulations about 16 years ago, they benchmarked the PDBN regulations of many states in the US. Korea developed a framework and identified key components in data breach notifications. With this, Korea developed the Korean PDBN regulation framework and systems and improved on the PBDN regulations.

One of the key components that Korea identified was the breach recognition and origin: when, why, and how the breach happened. For example, Singapore, Australia, and many other economies focus on these spectrums. Additionally, Korea also focuses on the scope of PDBN, whether it is the public sector or private sector. While certain economies focus either more on government sectors or private sectors, or sector-specific PDBN, Korea focuses on both public and private sectors. Another component is the mandatory or voluntary notification. Certain economies including Korea adopt mandatory notification, but other economies have voluntary notification systems. These have pros and cons, and different cultures and heritage lead to different effectiveness of these regulations.

Korea also must consider the triggers for notifications: data size, type, and risk of harm analysis. Australia implemented the “risk of harm” trigger, and on analysis of those, Korea has seen impact, making these regulations effective. Korea focuses more on the quantifiable criteria for the trigger: size of the data breach, and the potential harm and sensitivity of data. Another important component in the PDBN framework is time frame of notification to individuals and privacy enforcement authorities. This includes the questions of whether Korea needs to inform immediately to individuals, or if Korea needs time to investigate, and so on. The Korean Personal Information Protection Act specifies content of notification, which is the data that needs to be delivered to the individuals and the authorities, and the methods of notifications, which might include email, webpage, mobile messages, and fax. Following this, data controllers often come up with plans to respond to the emergencies and conduct risk management and crisis management approaches.

3. The Current Status of Data Breach Notification

On a closer look at Korea's PDBN, Korea focuses more on the quantitative criteria triggers. For the time frame, data controllers must notify individuals and authorities within 5 days of discovery. The trigger point is over 1000 data subjects' data records. In the telecom sector, Korea believes that a swifter response is necessary, so Korea enforces notification within 24 hours to authorities and individuals. Korea needs to continue to monitor whether these criteria are effective. Regarding the content of the notification message, Korea requires data controllers to inform the individuals of the following: 1. List of breached personal data/information items, 2. When and how personal data/information have been breached, 3. Information about what a data subject can do to minimize damage from the data breach, 4. A personal data/information manager's immediate actions for data protection and procedure for damage recovery, 5. The department and person in charge of receiving reporting and contact if damage is inflicted on a data subject. Sometimes, there is a need for investigation, but Korea requires that these investigations must be done swiftly, and the corresponding investigation can be done by the commission. In addition, PIPC and KISA also offer personal information breach response manuals to data controllers.

4. Number of Incidents and Affected Individuals

Korea has had PDBN as a mandatory requirement since 2011, across public and private sectors. In recent years, Korea has seen more data breach cases in the private sector, believed to be due to the diligence of regulatory bodies. By having lower trigger points for data breach notification, Korea sees more cases reported in the year 2018, 2019, and 2020. In the year 2014, Korea went through major credit card company data breach cases and that affected a huge number of individuals whose records were breached. The causes of these personal data breaches are either internal or intentional, and Korea is seeing increasing cases of external and intentional hacking or crime-related incidents. However, at the same time, Korea also monitored a substantial number of internal data breaches due to human error.

5. Individual’s Action to Protect

Korea also runs a survey every year on what individuals do about data breaches. Among the Korean survey respondents, 54% of the individuals take matters into their own hands: changing passwords, firewalls, antivirus software, and so on. However, according to the survey, 32% of respondents still take no action after receiving these PDBNs.

2.2.2. Significance of Personal Data Protection in the Growth of Chile’s Digital Economy

1. The Current Status of Chile

Before the advent of COVID-19 pandemic, Chile conducted a survey about the digital economy in the economy and they saw large gaps with other economies in the OECD. However, due to the pandemic and the restrictions imposed on mobility, Chile was the economy that increased the digitization effort the most when compared to all OECD economies. Although the base of comparison was lower at the beginning, 62% of Chile’s small-medium enterprises (SME) increased the use of digital technologies because of the pandemic, and 90% believe it will be a permanent change. There is a great process of digitalization currently taking place in the economy, and it correlates with the legislations that are currently in Congress.

In 2019, the Ministry of Economy offered approximately 20,000 instances of SME digitalization. During the pandemic, in 2020, the figure grew 11 times to 230,000 instances of SME digitalization, and this year the figure grew to approximately 400,000.

Chile has also been deploying fiber optic networks. In 2020, Chile was a leader among OECD economies in the establishment of new fiber optic connections. Chile is also leading the construction of the first transoceanic cable between Latin America and the Asia-Pacific region. Beginning construction next year, this is an investment of about half a billion dollars and will cover 12,360 kilometers. Chile was also the first economy in the region to enact its 5G spectrum. Once it is in operation, this public policy initiative is expected to contribute 0.2% to GDP in the first year, and 0.5% annually.

2. COVID-19 and Digitization Efforts

Chile has also been discovering lately that they have optimal conditions for space observation.

Chile currently hosts 70% of the world's observation capacity. Through the establishment of the data observatory foundation, the large data sets created by these observation centers are now available and have spurred the local development of algorithms and technologies that process this bounty. Additionally, Chile also has a good position to download satellite data from world stations. Chile has created partnerships to exploit these unique opportunities, on how to leverage astronomy as a vehicle for fostering data science.

This has led Chile to think differently in terms of regulation since there are always threats of overregulating or underregulating. If the government overregulates, perhaps they do not have the capacity to stimulate innovation fast enough, and if the government underregulates, perhaps they are not building the industries that they need. Thus, Chile is approaching this differently, and they are designing the first regulatory sandbox for artificial intelligence. Chile is seeking to spur innovation and digitalization in different parts of the economy regarding artificial intelligence with the collaboration of the private sector, the academy, and the different economic stakeholders. To sum up, the pandemic has forced an increase in digitization efforts of all the economy, and this is forcing the government to think differently on how to approach these regulatory processes.

3. Future Directions in Chile

Chile will be one of the first economies in South America to have a domestic policy for artificial intelligence. The representative speaker believes the president will have announced those changes by the end of the month. This could mean a growth of at least 1% in their GDP because artificial intelligence is transferrable to all the industries Chile has in their economy.

Chile has entered into a digital economy partnership agreement with Singapore and New Zealand to allow Chilean SMEs to better leverage opportunities that result from digital trade. This allows them to exchange practices and internationalize the services that they provide through digital means. One of the key lessons that most SMEs are currently learning when they are undergoing their digitalization efforts is that the digital economy has no boundaries, so they can try to export services and increase the number of connections and services delivered to the Asia-Pacific region thanks to these types of partnerships.

However, Chile knows that any type of growth in the digital economy is accompanied by new challenges. Chile still does not have an agency, but today the president of the republic announced that they are going to have their first data protection agency. This agency is expected to oversee the protection of data subject rights to strengthen the rights of individuals and improve enforcement under deliberation. Chile is also improving their digital security; they are currently creating another bill in Congress to create a cybersecurity agency.

Cybersecurity and cybercrime legislation are currently under deliberation. These are the two things that are quite important: the largest gap that Chile has with developed economies comes in terms of whether they recognize the threats of cybersecurity, and how to protect consumers, data subjects and citizens within data breaches. This is something that Chile expects to learn as they had discussed in the first part of this Forum, and there were many ideas that can help them to prove the legislation process currently being undertaken.

2.3. Good Practices of Personal Data Breach Notification with APEC Member Economies

2.3.1. Handling Data Breach in Hong Kong, China

1. What is a Data Breach?

In Hong Kong, China, data breach is generally considered a suspected breach of security of personal data held by a data user by exposing the data to the risk of unauthorized or accidental access, processing, erasure, loss or use. Unlike Singapore, Australia, or Republic of Korea, it is not a mandatory requirement in Hong Kong, China for data users to inform the local data protection authority, namely the Office of the Privacy Commissioner for Personal Data, Hong Kong, China ("PCPD"), about data breach incidents. Notwithstanding this, PCPD advocates that it is a good practice to establish a good data breach handling policy and practice, because it will not only be useful to contain the damage caused by a breach, but it also shows the data user's responsible and accountable attitude to tackle the problem and in giving a clear action plan to be followed in case of a data breach.

Some of the common causes of data breaches that PCPD has come across in the past years include loss of physical documents or portable storage devices, hacking and inadvertent disclosure through emails. With PCPD's promotional efforts, there has been an increase of data breach notifications lodged with PCPD, which hit a record high in 2019. This suggests that lodging data breach notifications with the local data protection authority is now a more common practice for data users, and there is heightened awareness of personal data protection among data users. In recent years, PCPD has witnessed the heightened level of security of data users' computer systems and networks, and the stepping up of data protection training provided to the staff.

2. How Does PCPD Handle Data Breach in Hong Kong, China?

PCPD plays a role as both an educator and investigator. Insofar as data breach handling is concerned, PCPD advises data users to collect all essential information to assess the impact on data subjects, including: when and where did the breach take place, how was the breach detected and by whom, what was the cause(s) of the data breach, what kind and extent of the personal data was involved, how many data subjects were affected. PCPD asks data users to contact the interested parties, especially IT experts, for assistance because most of the breaches involve computer systems and network security issues. PCPD recommends data users adopt some containment measures to avoid any further leaks of data. In the case of a system failure, they should stop the system or revert the configuration to an earlier version. PCPD encourages data users to keep all the evidence and notify the data subjects and PCPD of the data breach. PCPD has a designated data breach notification form accompanied by "information notes", which provide some practical guidance to data users such as how to fill in the form and how to provide a notification to the PCPD. Data users are asked to fill in information including: what the breach is about, what types of personal data are involved, the number of affected data subjects, what the risk of harm is and what containment actions data users should take.

3. Workflow of Data Breach Handling in Hong Kong, China

Upon receiving a data breach notification, PCPD would decide whether a compliance check should be conducted. PCPD can also initiate a compliance check or investigation in the absence of a data breach notification if there are sufficient grounds to believe that the data practice may contravene the requirements under the Personal Data (Privacy) Ordinance (the "Ordinance"), the personal data protection law of Hong Kong, China. If there is prima facie evidence of contravention that a significant number of data subjects are affected, or sensitive personal data is involved, PCPD may initiate an investigation with a view to understanding the data breach thoroughly. During the process, PCPD alerts data users of any apparent inconsistency with the requirements of the Ordinance, and either advises them to take remedy actions to prevent the breaches or provide undertaking to prevent further breaches. If PCPD concludes that the data user contravened the requirements under the Ordinance, PCPD may issue an enforcement notice to direct the data user to take remedial actions. Failure to comply with the enforcement notice is a criminal offence, which could lead to referral to the police for investigations. PCPD may also compile and publish an investigation report after completing the investigation if they consider it in the public interest to do so.

4. Real Cases of Data Breach Handling in Hong Kong, China

An international airline based in Hong Kong, China suffered from unauthorized access to personal data to their computer systems, affecting approximately 9.4 million passengers around the globe. PCPD took steps to investigate the matter, and it was revealed that the airline had failed to take reasonable or practical steps to protect the affected passengers' personal data against unauthorized access, due to their poor management. They had lax data governance without applying effective authentication to all remote access users. PCPD concluded that the airline had contravened the relevant requirements of the Ordinance and therefore issued an enforcement notice directing them to, among others, engage an independent data security expert to overhaul the systems that contain personal data, conduct effective vulnerability scans, devise a clear data retention policy, and engage an independent data security expert to conduct reviews / tests of the security of the airline's network at regular intervals.

2.3.2. Assessing Real Risk of Significant Harm from Privacy Breaches

1. Background of Tool Development

The Office of the Privacy Commissioner of Canada receives, reviews, and assesses breach reports, and works with organizations to ensure the breach responses are appropriate in order to protect privacy rights. This is done under two legislations: Personal Information Protection and Electronic Documents Act and the Privacy Act. Personal Information Protection and Electronic Documents Act applies to private sector organizations that collect, use, or dispose personal information in the course of any commercial activity. The Privacy Act is mostly equivalent to Personal Information Protection and Electronic Documents Act and applies to Federal Government institutions.

The private sector legislation was amended close to 3 years ago, making it mandatory for organizations to report to their office in breaches of security safeguards involving personal information under the control, where it is reasonable under the circumstances to believe the breach creates a Real Risk of Significant Harm (RROSH) to individuals. Significant Harm includes bodily harm, humiliation, damage to reputation or relationships, financial loss, identity theft, negative effects on the credit record, damage to or loss of property, as well as loss of employment, business, or professional opportunities. Factors that are relevant to determining whether a breach creates a real risk of significant harm include sensitivity of the personal information involved in the breach, and the probability the personal information has been/is/will be misused. A tool to assess RROSH is necessary for several reasons. Primarily, it is the first step to consider if the organizations' responses to breaches are appropriate and if the organizations' notifications to individuals describe appropriate steps that individuals can take to reduce the risk of harm from the breaches. Additionally, it brings efficiency; last year the Office received close to 800 private sector breach reports. Adding reports from Federal Government institutions, the number of reports received is 1000 per year. Also, as organizations better understand the breach reporting requirements, that number seems to be steadily increasing. Furthermore, it provides them with data to inform decisions on where to target their resources. The Office will be able to agree in advance on levels at which breaches should be considered for further compliance activities. It also streamlines staff training on conducting RROSH assessments and it should make the Office's annual breach record inspections faster to complete. The RROSH Tool standardizes Canada's approach to how they assess RROSH. It will not replace the Office's judgement, but it supplements it. The tool is currently moving through the approval and implementation stages

2. Demonstration of the RROSH Tool

When using the tool on their desktop, an investigator will see a wizard or a survey with a series of questions. As the investigator enters answers, a breach assessment logic operates real-time in the background. The logic decides what questions to ask of the investigator from the available set of questions in the tool. It also calculates risk scores at the end of the process. When answering the questions, the investigator can see a blue shaded box above the questions. This box allows users to understand the import of their answers and the rationale behind the questions. They promote understanding of the risk assessment process. Ultimately, the tool compares those scores to thresholds that suggests if and how the breach represents RROSH to individuals. The demonstration will show the question wizard with the questions the user will see, the means of significant harm and categories of personal information the tool considers, and how the tool displays the RROSH results. The scenario for this demonstration is an unintentional breach such as misdirected correspondence or mail. It will ask extra questions to calculate the probability of misuse.

2.3.3. Promoting Comparability of Personal Data Breach Notification Reporting

1. Background of the Project

The OECD project started in response to the OECD Ministerial Declaration on the Digital

Economy in 2016, calling for a new metrics for the digital economy. The project of personal data breach notification aims at the metrics for interoperable data on personal data breaches that privacy enforcement authorities are collecting. The OECD conducted a survey to privacy enforcement authorities from June 2019 to February 2020, in order to test the proposed set of interoperable data items. During this process, the OECD received support of the GPA (Global Privacy Assembly), APPA (Asia Pacific Privacy Authorities), and EDPB (European Data Protection Board).

2. Survey Questionnaire

The survey questionnaire covered a wide range of information from authorities' profiles to regular duty requirements to statistical figures to types of data the authorities are collecting and how authorities use the collected data. Despite the lengthy and complex questionnaire, in total, 35 economies answered the survey, consisting of 32 OCED member economies and 3 non-member economies. The survey results are summarized in an analytical report, which the OECD will publish in Q4 of this year.

3. Trend Toward Mandatory Personal Data Breach Notification

The OECD found a trend towards a mandatory personal data breach notification to the authorities. As of February 2020, all the European economies and more than half of non-European economies introduced mandatory data breach notification to the authorities. However, there are also variations in the implementation. In some economies, it applies to private and public sectors differently. For example, there are exemptions in the private sectors by annual turnover of funds. Also, variations exist in thresholds. Generally, thresholds of notifications reflect a risk-based approach, but there are variations in the factors considered to weigh the risks such as likelihood of harm to data subjects, number of the affected data subjects, and types of data breached. There are also variations related to data breach notifications to data subjects. Some economies have the same triggers and time frames to notify both data subjects and the authority, while others have different triggers and time frames to notify them.

4. Internationally Comparable Data Metrics

Their survey found common data metrics that privacy enforcement authorities are using in their operation. The main part of the data metrics the OECD identified includes: total number of data breaches reported to the authority, nature of causes which Indicates general trends in data breach notifications, specific causes, types of data breached, and information on encryption of data breached which shows more detailed trends of data breach notifications.

4-1. Recent Trends in the Total Number of Data Breach Notifications

First, the OECD survey found a general increase in the total number of data breach notifications from 2017 to 2019. Second, the graph represented changes in the number of data breach notifications reported to the authorities in 10 economies that answered for all consecutive years in the survey. There is also a significant increase in particular European economies. These increases in the number of data breach notifications can probably be attributed to the introduction of mandatory personal data breach notifications to the authority. However, looking at some of the recent figures, there may be a mixed trend after the survey period. Third, both increases and decreases of the total number of data breach notifications were observed in 2020 in a number of reports. There are anecdotal causes of the decline in the number of data breach notifications. For example, in the case of over-reporting, breached organizations reported the data breaches that did not meet the notification thresholds in order to stand on the safer side after the introduction of mandatory data breach notification. Anecdotally, as time passes, the over-reporting disappears. Anecdotal causes of the decline also include a temporal decline in the processing activities due to office shutdown. When one report analyzed that organizations with more workforce working remotely took longer days to identify and contain data breaches, it counts as potential lack of cooperation between the security team and legal team. Fourth, there is an increase in the size and impact of data breaches. Mega breaches not only involve a massive number of data subjects, but also influence across the borders. For example, the data breach of Marriott in 2018 involved 339 million guest records in 31 European Economic Areas. Fifth, while the number of publicly disclosed breaches shrunk by 48% in 2020, the number of records lost increased by 141%, indicating the increase in the average number of records lost by data breaches.

4-2. Nature of Causes of Data Breaches

Common data items for nature of causes: malicious or non-malicious, internal or external, and human errors. These data items capture the general trend that data breaches are caused by human errors or malicious attempts either by internal or external actors. These trends were observed in a number of reports both by authorities and private sector organizations before the pandemic, but the observed trend is continuing during the COVID-19 pandemic. For example, according to the report by Verizon, the top actions that caused data breaches from November 2019 to October 2020 were hacking, social, error, and malware.

4-3. Specific Causes of Data Breaches

Common items for specific causes: loss of IT equipment, mailing, hacking, technical error, theft, improper disposal of documents, and unauthorized access. It may be useful to add “unauthorized disclosure” to reflect recent trends of data breaches. This is because human error, such as misdelivery of messages and misconfiguration of cloud storage, are reported as major causes of data breaches in several reports. Also, it may be useful to add explanations to identified data items, to better capture the recent trends of data breaches. For example, according to Interpol, there was an increase in the domains registered with the pandemic related terms such as “COVID” and “vaccination,” which were frequently used in fake websites and emails to lead victims to open malicious attachments or clicking phishing links. Thus, it may be useful to add explanations to the data item “theft,” to clarify that it involves the theft of credentials and financial data through social engineering.

4-4. Types of Data Breached

The common data items for types of data breached include personal credential data, sensitive data, and financial data. One type of data that could be added: “unknown.” According to the report by Riskbased security in 2021, “unknown” data is when a data breach was confirmed but it was not able to identify what kind of data was breached. Their report states that the category of “unknown” has tripled since 2018.

III. CONCLUSION

As the size of data grows and the scope of its use increases, the forums in which personal data is collected and utilized are increasing rapidly. Whenever we use our smartphones, we are providing data to someone else. Online services are moving beyond international borders, and COVID-19 has further promoted the movement of data between economies. In other words - even if you are physically in Korea, your personal data might be stored and used in another economy without you knowing. To protect personal data, each economy has been preparing for a legal system regarding personal data protection.

The scope and frequency of individuals using international services are increasing, but the personal data protection laws vary significantly among economies. Thus there is a clear limit to protecting personal data that has been transferred overseas solely with the power of the government. This is because it is difficult for the government to control personal data that has already been transferred to other economies when protection systems vary internationally. For example, when Korean companies engage in business activities in other economies, they may suffer from different personal data protection systems. They would have to provide different services according to the regulations and legal systems for each economy whenever they try to expand their businesses abroad. Preparing and responding to different services from economy to economy is bound to be a significant management burden for companies, as well as socially and economically inefficient.

This Forum makes it possible to share international responses in the medium- and long-term as a solidarity among personal data-related experts are formed and personal data breach notification systems of different economies are discussed. This Forum provides to further promote participation in the digital market by making the digital environment more consumer friendly. This Forum contributes to reinforcing the personal data capacity of APEC member economies and improving knowledge of personal data breach notification systems and methods in different economies.

1) Improving understanding of problems related to personal data conflicts in digital trade, including cross border enforcement issues

2) Making people aware of the personal data breach notification system and discussing systems and policies that can prevent secondary damages to users in case of international problems

3) Strengthening the digital economy structure through sharing of personal data breach notification systems, policies, and processes of solving problems as well as the participation

of APEC member economies.

Furthermore, this project promotes the leadership, voice, and agency, which are pillars of women's economic empowerment. Both male and female speakers and participants attended the APEC Virtual Forum, the programs of the Forum included female speakers. Also, both male and female experts in related areas such as policy makers, personal data experts, NGOs, and academics of APEC member economies was invited. This project proposal strongly encourages to go beyond the underrepresented gender's participation and bring gender discussions into projects to actively contribute to women's empowerment in economic activities in the region.

IV. FUTURE DIRECTION

We propose further discussions on the issue of an “effective global personal data policy system.” Effective regulations and systems cannot be developed only with the opinions of a small number of experts. It should be based on exchanges, communication, and participation of diverse opinions. In order to increase our social competitiveness in the era of AI and big data, where data collection and utilization have become more important than ever, a more comprehensive and international approach to the personal information system is needed. More effective, rational, domestic, and international legal systems can be created when experts and citizens from various economies gather to freely share their experiences and opinions on whether each policy is effective, whether there are new methods of policies, whether it should be strengthened or relaxed, and more. Personal data cannot be protected by only one economy.

All of us are continuing to provide and receive personal data from someone, and through this process, we facilitate our social lives. It would be very helpful if each of us knew how the personal data we provide is used, how it is protected, and how to minimize damage if it is breached. To spread awareness of personal data and privacy, the final report of the Forum will be open to the public, and anyone who is interested in personal data protection can access it.

After the APEC Forum, the results of discussions can be used by policy makers of APEC member economies to respond to personal data breaches. As AI and Big Data technology are utilized, personal data breach is unavoidable, and continued review and preparations of an international personal data breach notification is needed. Next, the APEC Virtual Forum is expected to be followed by various relevant activities, academic forums, and public attention to further discuss personal data issues of APEC economies and suggest feasible solutions.