The 12th

Asia Privacy Bridge Forum 2023

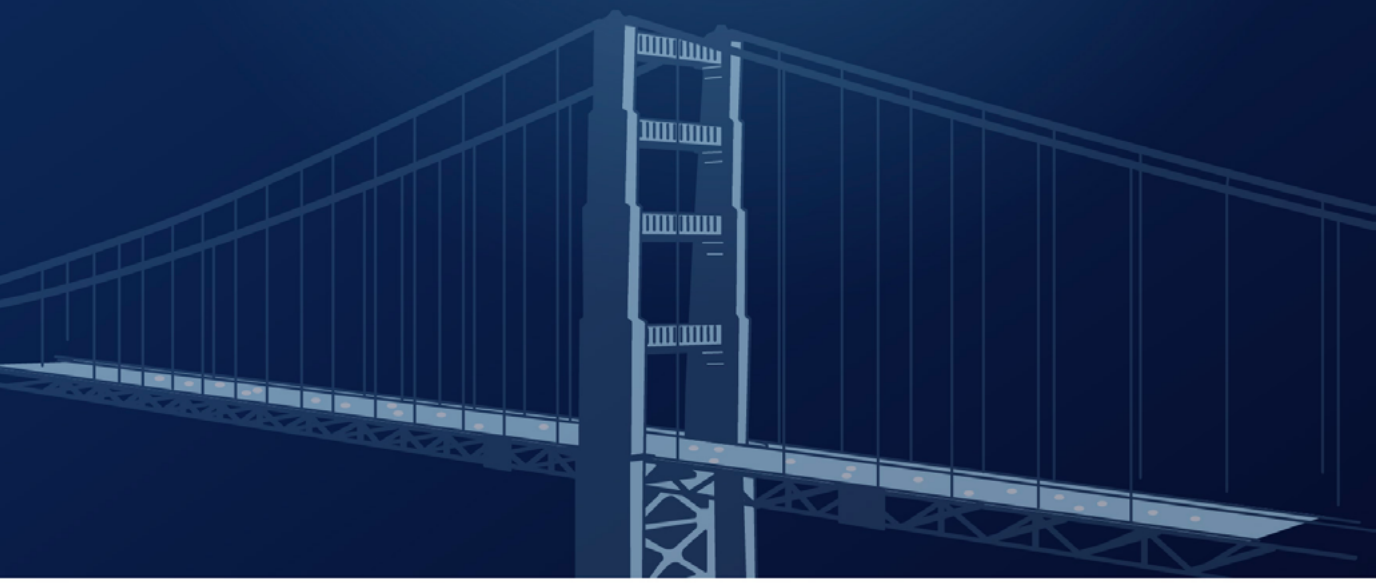
Data Access and Trust in AI Era

Oct 12 (Thu) 09:00 ~ 17:00

Auditorium 3,
Science and Technology Convention Center
한국과학기술회관 중회의실3

Oct 13 (Fri) 10:00 ~ 14:00

#703 New Millennium Hall, Yonsei University
연세대학교 새천년관 703호 [Closed meeting, Invited only]



Ministry of Science and ICT · Personal Information Protection Commission · KISA · ISACA Korea Chapter · 한국CPO포럼 · FROM100 · Graduate School of Information Yonsei University · Barun ICT Research Center · Yonsei University Innovative Talent Development Program for Personal Information Protection

Table of Contents

October 12th, Thursday
Science and Technology Convention Center

Table of Contents

October 13th, Friday
New Millennium Hall, Yonsei University

Session 1

Regional Efforts
for Free Data Flow

1. Country / Case Reports
2. Hiroshi Miyashita (Professor, Chuo University, Japan)
   "Data Free Flow with Trust – Human Rights and Trade"

Session 2

Data Breach Notification
across Borders

1. Country / Case Reports
2. Janssen Esguerra (IT officer I, National Privacy Commission, Philippines)
   "Data Breach Notification across Borders"

Session 3

APB Future Planning

1. Jong-Chul Shin (Professor, Yonsei University Law School, Korea)
   "Past, Present, and Future of the Personal Information Protection Act in Korea"
2. Recommend Topics / Experts for Next Meeting
3. Policy Suggestion / Proposals

The 12th

Asia Privacy Bridge Forum 2023

Keynote

Steve Wood

Director & Founder, PrivacyX Consulting, UK
(Former Deputy Commissioner, ICO)

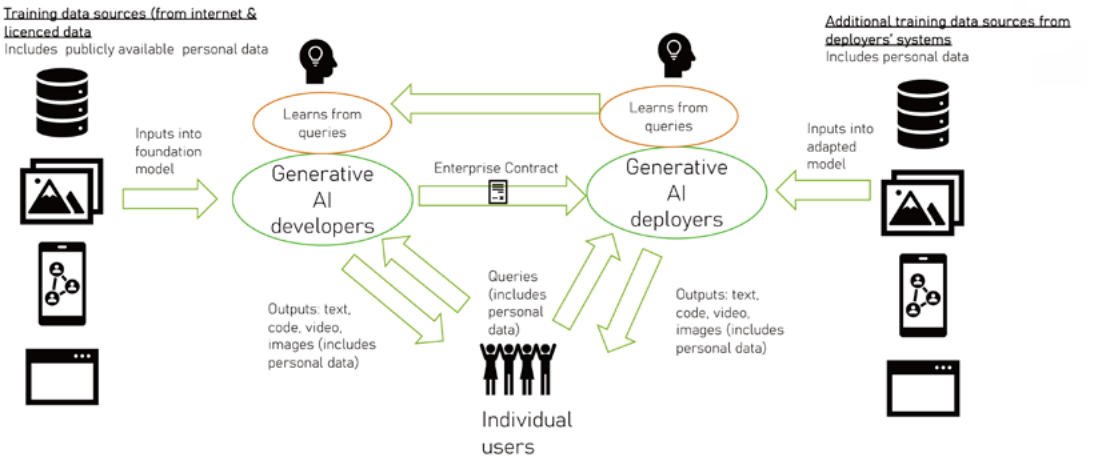
GENERATIVE AI AND COMPLIANCE WITH DATA PROTECTION AND PRIVACY LAWS: CURRENT INTERNATIONAL TRENDS & FUTURE CHALLENGES

Steve Wood, PrivacyX Consulting

Asia Privacy Bridge 12/13 October 2023

PrivacyX Consulting

GENERATIVE AI AND FOUNDATION MODELS: HOW THEY CAN USE PERSONAL DATA



GENERATIVE AI: DATA PROTECTION RISKS AND CHALLENGES

Transparency
- Explaining training data inputs
- Explaining learning from queries
- Explaining implications of Generative AI outputs, including automated decisions

Accountabilty
- Controller & processor roles
- Liability
- Data Governance
- Data Protection by Design
- Impact assessments

Data Rights
- Right of access
- Right of correction or deletion
- How do the rights interact with data in foundation models?
- Objection to automated decisions

Lawful basis
- Legitimate interests
- Necessity and proportionate
- Consent
- Contract

Children
- Consent for child users
- Transparency and awareness
- Impact of outputs

Fairness
- Bias risk
- Discrimination risk
- Dataset fairness
- Design fairness
- Outcome fairness
- Implementation fairness

DP principles
- Accuracy – hallucinated output, deepfakes
- Data minimisation – scale of training data
- Purpose limitation – re-use of personal data in models

Security
- Personal data leakage
- Identification risks
- Model inversion, data poisoning, prompt injection
- Automation of cyber attacks

1. Rejection or removal of personal data from training data before model is developed
2. Train models to reject queries for private or sensitive information about people
3. Allowing website operators can specifically disallow crawlers or block the crawler's IP address
4. Not training and learning from enterprise deployments of their foundation model and allow the deployment to control data retention
5. Opt-out for use of chat history data for individual users
6. Improved privacy notices and information about data training and classification process
7. New forms and procedures for data rights - including access and objection
8. Revised contracts and data protection agreements between developers and deployers
9. Guidance and tools to support safe deployments

ACTION TAKEN BY DATA PROTECTION AUTHORITIES

Enforcement orders and fines

- Italy Garante – prohibition to OpenAI, lifted after one month
- South Korea PIPC – administrative fine of 3.6 million KRW against OpenAI for failure to notify a data breach in relation to its payment procedure and issued a list of instances of non-compliance
- Japan PIPC – warning issued to OpenAI

Investigations on going into OpenAI

- Canada – Federal OPC, British Columbia, Quebec, and Alberta
- US Federal Trade Commission
- Brazil ANPD

Co-ordinated actions

- European Data Protection Board and Ibero-American Network of DPAs

Guidance

- New Zealand PC, UK ICO, Spain AEPD, France CNIL

ACTION TAKEN BY DATA PROTECTION AUTHORITIES – AREAS OF NON-COMPLIANCE

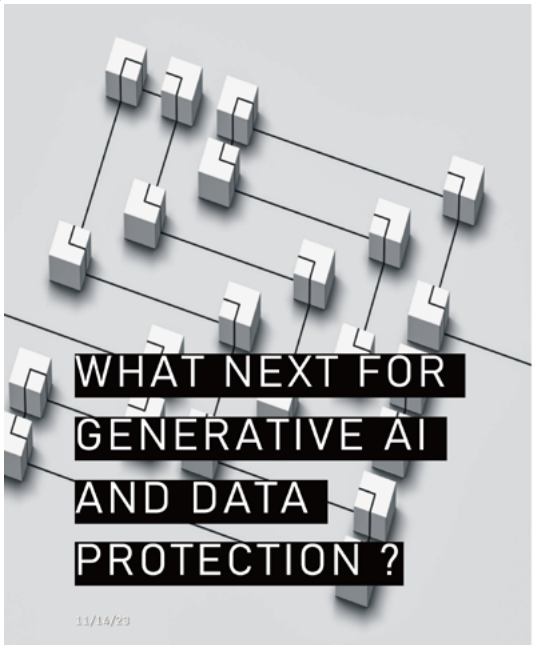
G7 DATA PROTECTION AUTHORITIES

Joint statement on generative AI June 2023

Key areas of concern:

- ✓ Legal authority for the processing of personal information
- ✓ Risks to children
- ✓ Security safeguards
- ✓ Mitigation and monitoring measures of generated output
- ✓ Transparency measures to promote openness and explainability
- ✓ Production of technical documentation across the development lifecycle to assess the compliance
- ✓ Technical and organizational measures to ensure individuals can exercise their rights
- ✓ Accountability measures to ensure appropriate levels of responsibility among actors in the AI supply chain
- ✓ Limiting collection of personal data to only that which is necessary to fulfil the specified task.

Steve Wood APB Conference 2023



- ❑ More detailed DP guidance and regulatory actions
- ❑ DP investigations across the AI supply chain, not just deployers
- ❑ DP investigations into specific use cases of generative AI e.g. in recruitment, banking
- ❑ Growth of DP regulatory sandboxes to provide advice on data protection by design
- ❑ Joined up investigations between DP regulators and other regulators (e.g. competition, financial services)
- ❑ Policy makers consider places that DP cannot regulate and how the gaps should be filled
- ❑ Role of the EU AI Act in regulating generative AI (under negotiation in 2023). Some data protection regulators may take on AI Act functions when it becomes law

Steve Wood APB Conference 2023 8

The 12th

Asia Privacy Bridge Forum 2023

Keynote

Marc Rotenberg

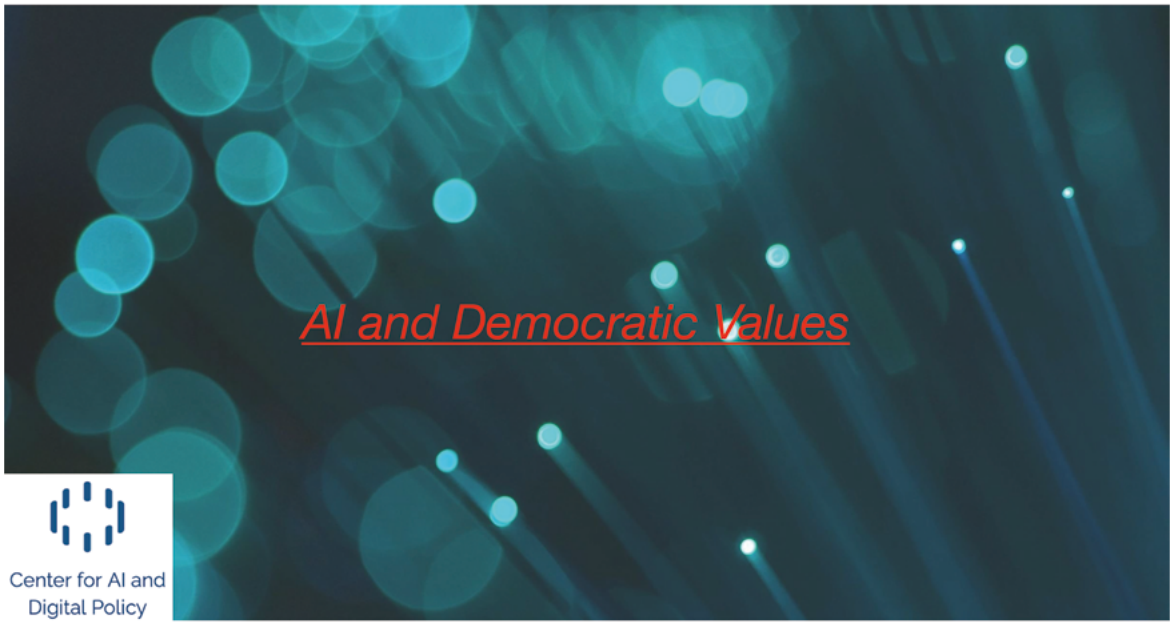
Executive Director, the Center for AI and Digital Policy, US


Center for AI and
Digital Policy


How are we to govern AI?


1) The report *Artificial Intelligence and Democratic Values*
2) Overview of Legal Frameworks for AI
3) Challenges of Machine Learning and the Protection of the Fundamental Rights
4) Developments in the US
5) A return to ethics
Center for AI and Digital Policy


CONGRATULATIONS TO KOREA
(1) *OECD AI Principles*
(2) *"Cryptography and Liberty"* (1999-2002)
(3) New initiatives - Digital Bill of Rights
Center for AI and Digital Policy

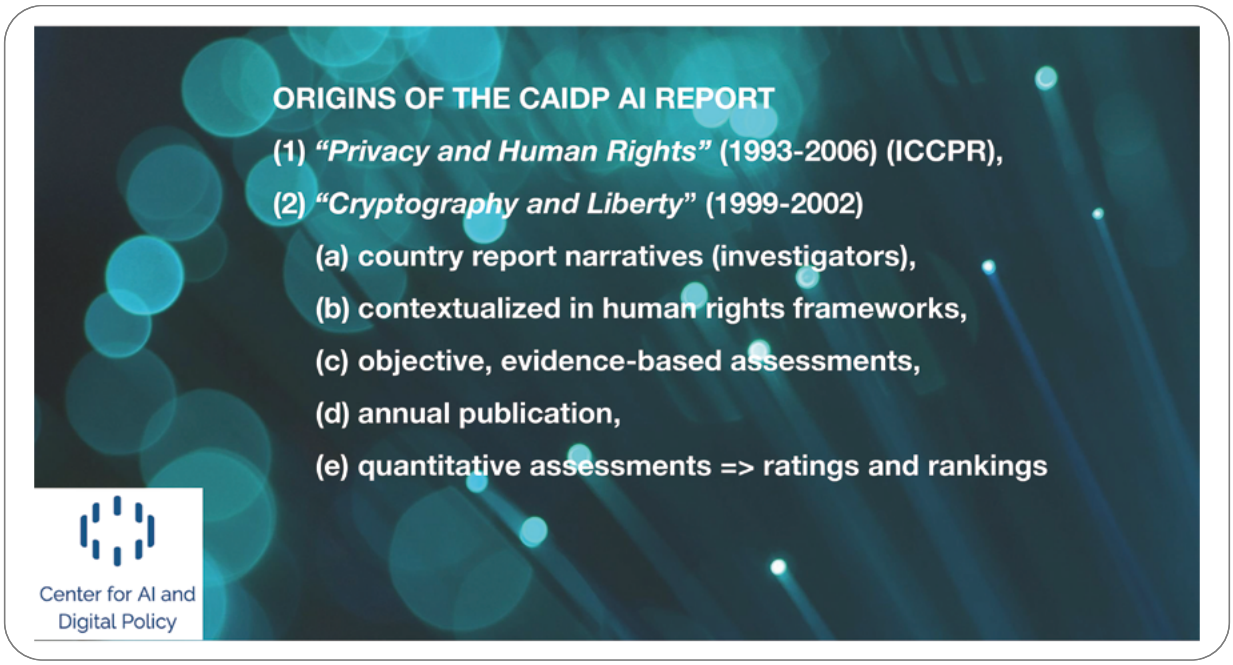

AI and Democratic Values
Center for AI and Digital Policy

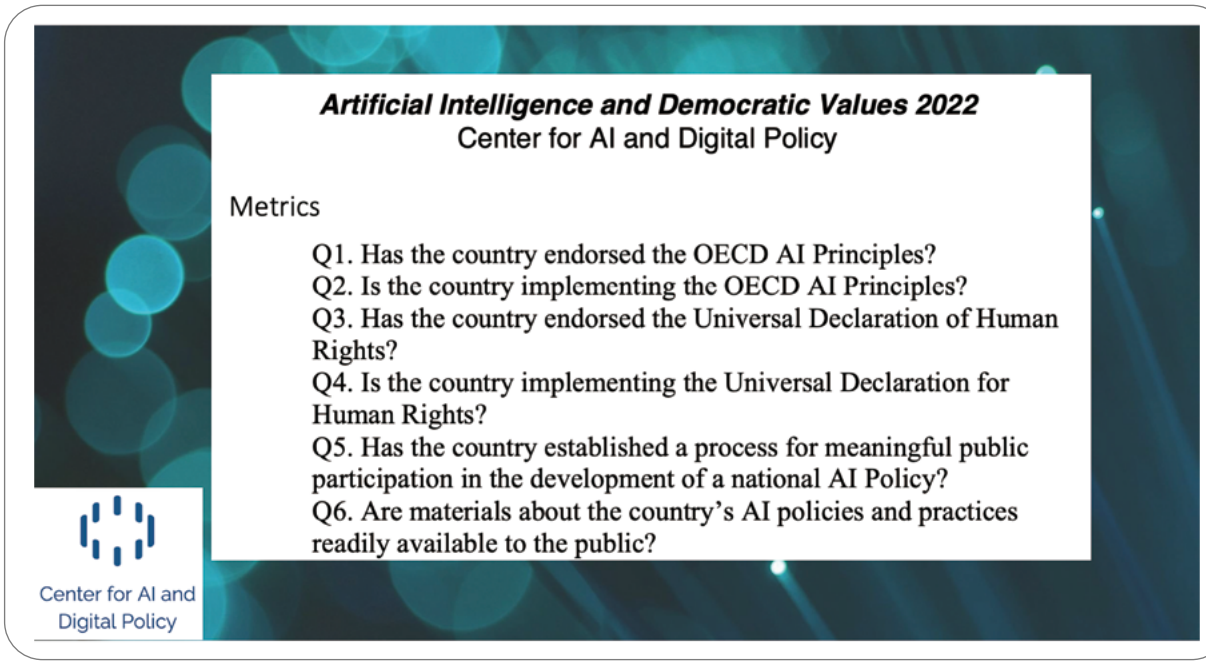

COMMUNICATIONS of the ACM
HOME
CURRENT ISSUE
NEWS
BLOGS
OPINION
RESEARCH
Home / Blogs / BLOG@CACM / Time to Assess National AI Policies / Full Text
BLOG@CACM
Time to Assess National AI Policies
By Marc Rotenberg
November 24, 2020
Comments
VIEW AS:
SHARE:
The artificial intelligence (AI) ethics field is booming. According to the Council of Europe, there are now more than 300 AI policy initiatives worldwide. Professional societies such as the ACM and the IEEE have drafted frameworks, as have private companies and national governments. Many of these guidelines set out similar goals: human-centric policies, fairness, transparency, and accountability. But little effort has been made to evaluate whether national governments have taken steps to implement AI policies.
The Center for AI and Digital Policy has undertaken the first comparative review of national AI policies. Our goal is to understand the commitments that governments have made, the AI initiatives they have launched, and the policies they have established to protect fundamental rights and to safeguard the public. Constructing the methodology for such a survey is not a simple task. A country can commit to "fairness" in AI decision-making, as many have, but to determine whether they are implementing the practice is a much harder task.
The AI Policy Sourcebook 2020
MARC ROTENBERG
Electronic Privacy Information Center
WASHINGTON DC
Center for AI and Digital Policy

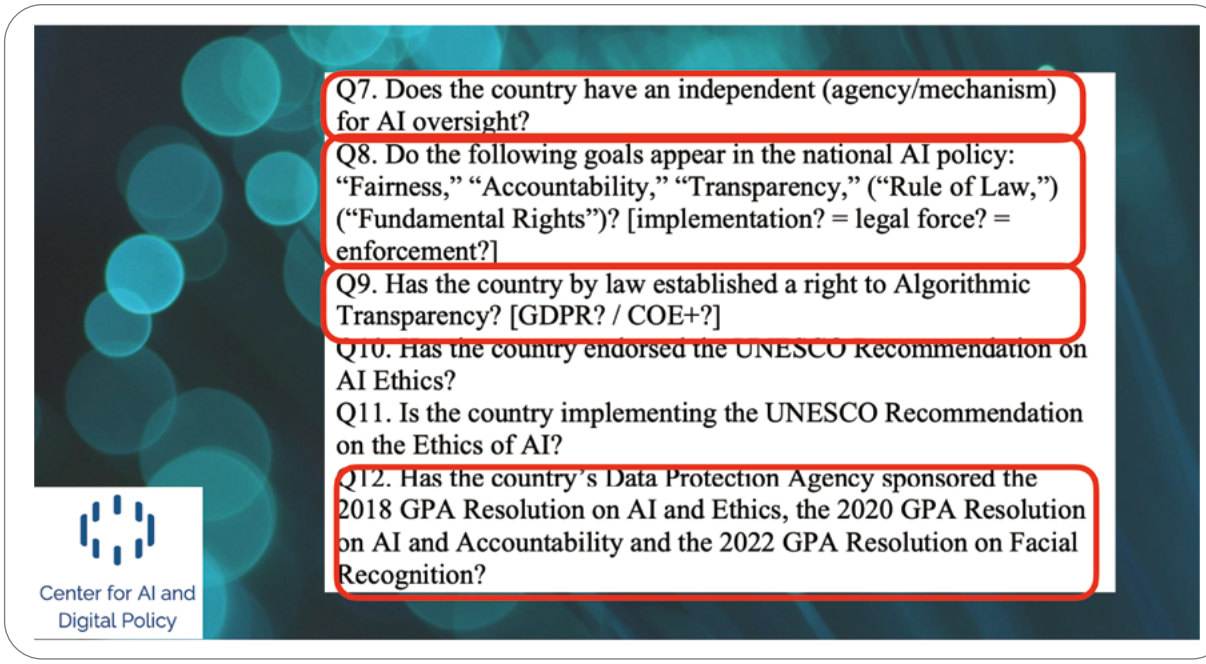

Center for AI and Digital Policy
ARTIFICIAL INTELLIGENCE AND DEMOCRATIC VALUES INDEX
APRIL, 2023
CENTER FOR AI AND DIGITAL POLICY
WASHINGTON, DC
CAIDP.ORG
Center for AI and Digital Policy

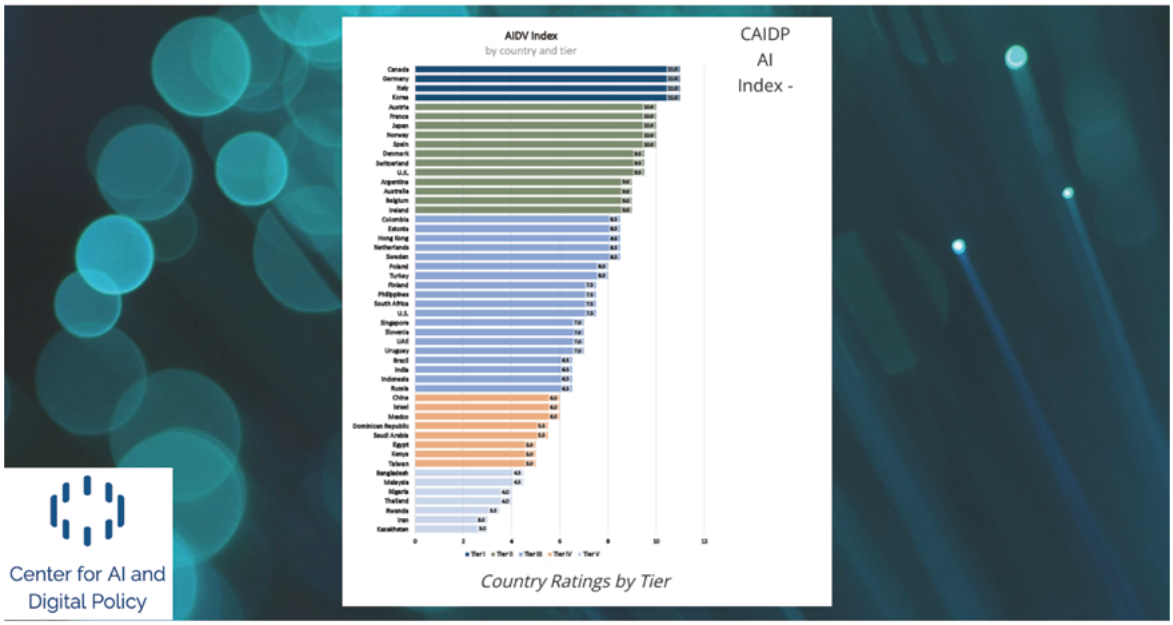

THE GOALS OF THE AI REPORT
(1) Document AI policies and practices of countries,
(2) Establish a methodology based on global norms,
(3) Provide basis for comparative evaluation, and
(4) Encourage countries to ensure that AI is trustworthy and human-centric
Center for AI and Digital Policy

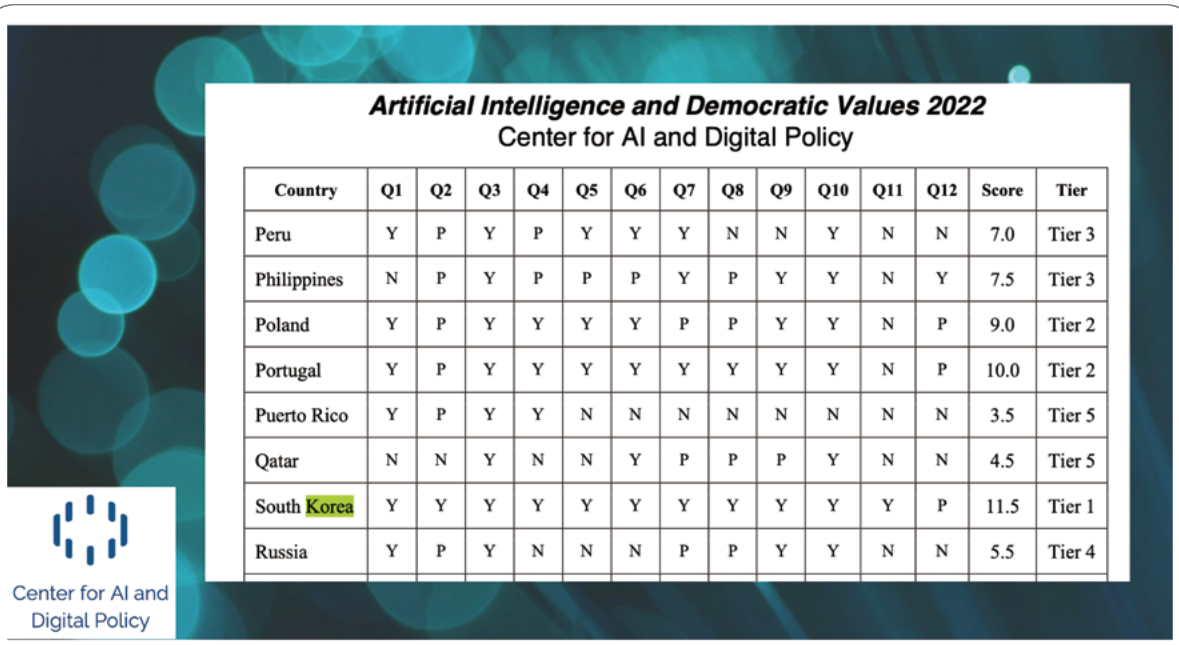

A FEW NOTES ON THE REPORT
• 300+ researchers in more than 60 countries
• Review of AI policies and practices in 50 countries
• Ratings across 12 metrics (e.g. OECD AI? UDHR?)
• Countries are rated and ranked and placed in 5 tiers
• Review also of AI policy developments at G7, G20, COE, EU, UNESCO
Center for AI and Digital Policy


ORIGINS OF THE CAIDP AI REPORT
(1) *"Privacy and Human Rights"* (1993-2006) (ICCPR),
(2) *"Cryptography and Liberty"* (1999-2002)
(a) country report narratives (investigators),
(b) contextualized in human rights frameworks,
(c) objective, evidence-based assessments,
(d) annual publication,
(e) quantitative assessments => ratings and rankings
Center for AI and Digital Policy


Artificial Intelligence and Democratic Values 2022
Center for AI and Digital Policy
Metrics
Q1. Has the country endorsed the OECD AI Principles?
Q2. Is the country implementing the OECD AI Principles?
Q3. Has the country endorsed the Universal Declaration of Human Rights?
Q4. Is the country implementing the Universal Declaration for Human Rights?
Q5. Has the country established a process for meaningful public participation in the development of a national AI Policy?
Q6. Are materials about the country's AI policies and practices readily available to the public?
Center for AI and Digital Policy


Q7. Does the country have an independent (agency/mechanism) for AI oversight?
Q8. Do the following goals appear in the national AI policy: "Fairness," "Accountability," "Transparency," ("Rule of Law,") ("Fundamental Rights")? [implementation? = legal force? = enforcement?]
Q9. Has the country by law established a right to Algorithmic Transparency? [GDPR? / COE+?]
Q10. Has the country endorsed the UNESCO Recommendation on AI Ethics?
Q11. Is the country implementing the UNESCO Recommendation on the Ethics of AI?
Q12. Has the country's Data Protection Agency sponsored the 2018 GPA Resolution on AI and Ethics, the 2020 GPA Resolution on AI and Accountability and the 2022 GPA Resolution on Facial Recognition?
Center for AI and Digital Policy

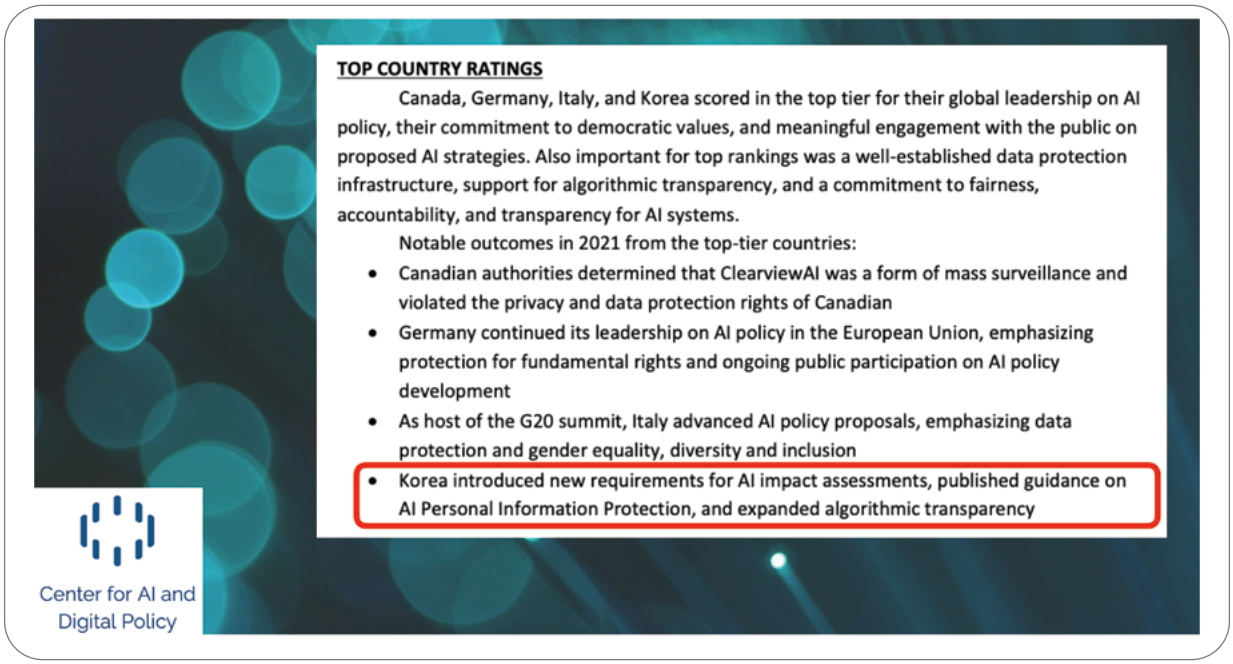




Artificial Intelligence and Democratic Values 2022

Center for AI and Digital Policy

Country	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Score	Tier
Peru	Y	P	Y	P	Y	Y	Y	N	N	Y	N	N	7.0	Tier 3
Philippines	N	P	Y	P	P	P	Y	P	Y	Y	N	Y	7.5	Tier 3
Poland	Y	P	Y	Y	Y	Y	P	P	Y	Y	N	P	9.0	Tier 2
Portugal	Y	P	Y	Y	Y	Y	Y	Y	Y	Y	N	P	10.0	Tier 2
Puerto Rico	Y	P	Y	Y	N	N	N	N	N	N	N	N	3.5	Tier 5
Qatar	N	N	Y	N	N	Y	P	P	P	Y	N	N	4.5	Tier 5
South Korea	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	P	11.5	Tier 1
Russia	Y	P	Y	N	N	N	P	P	Y	Y	N	N	5.5	Tier 4

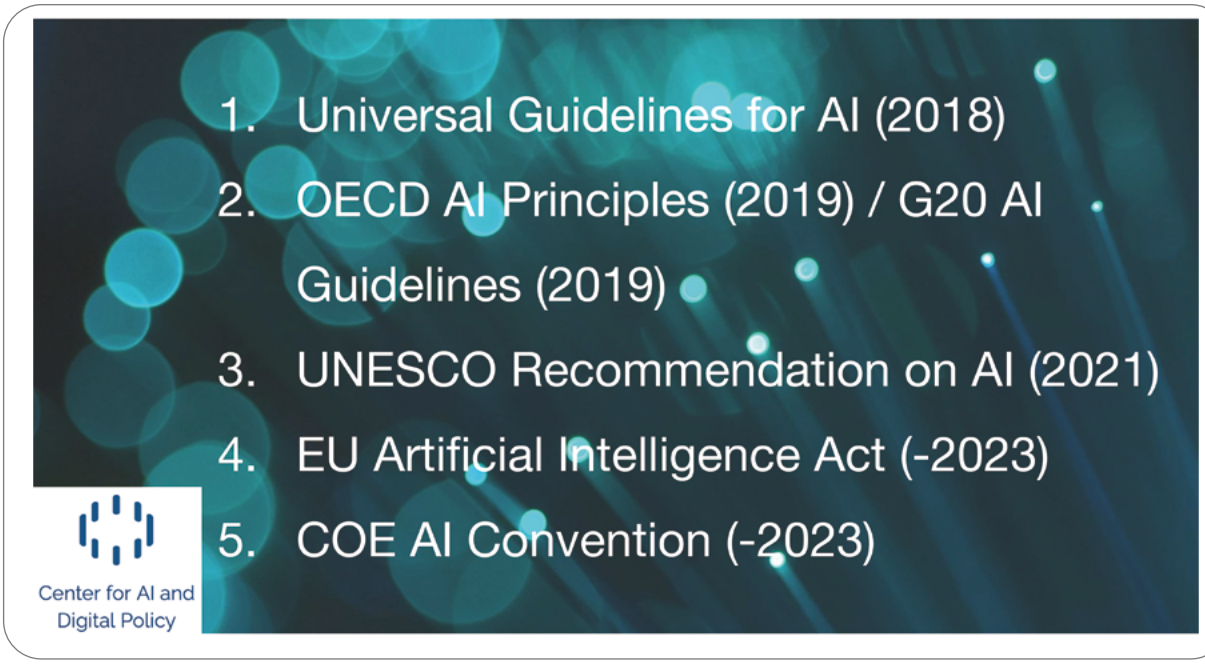

TOP COUNTRY RATINGS
Canada, Germany, Italy, and Korea scored in the top tier for their global leadership on AI policy, their commitment to democratic values, and meaningful engagement with the public on proposed AI strategies. Also important for top rankings was a well-established data protection infrastructure, support for algorithmic transparency, and a commitment to fairness, accountability, and transparency for AI systems.
Notable outcomes in 2021 from the top-tier countries:
• Canadian authorities determined that ClearviewAI was a form of mass surveillance and violated the privacy and data protection rights of Canadian
• Germany continued its leadership on AI policy in the European Union, emphasizing protection for fundamental rights and ongoing public participation on AI policy development
• As host of the G20 summit, Italy advanced AI policy proposals, emphasizing data protection and gender equality, diversity and inclusion
• Korea introduced new requirements for AI impact assessments, published guidance on AI Personal Information Protection, and expanded algorithmic transparency
Center for AI and Digital Policy


CAIDP - RECOMMENDATIONS (2021)
1. Countries must establish national policies for AI that implement democratic values
2. Countries must ensure public participation in AI policymaking and also create robust mechanisms for independent oversight of AI systems
3. Countries must guarantee fairness, accountability, and transparency in all AI systems
4. Countries must commit to these principles in the development, procurement, and implementation of AI systems for public services
5. Countries must halt the use of facial recognition for mass surveillance
Center for AI and Digital Policy

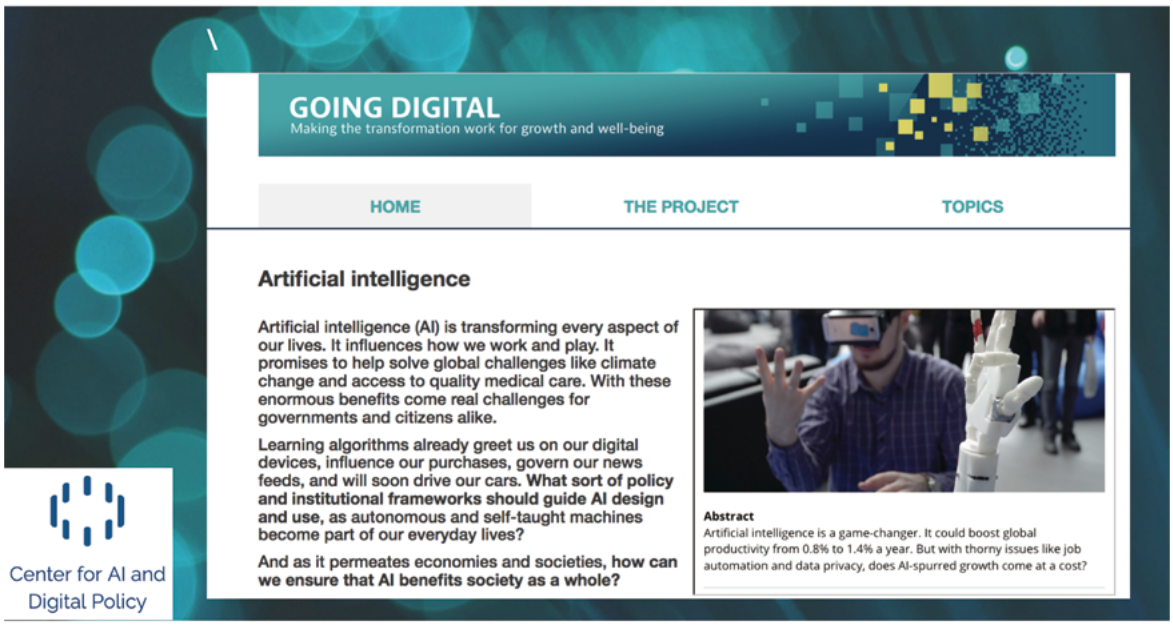

CAIDP - RECOMMENDATIONS (for 2022)
• Countries must curtail the deployment of lethal autonomous weapons
• Countries must begin implementation of the UNESCO AI Recommendation
• Countries must establish a comprehensive, legally binding convention for AI
Center for AI and Digital Policy


CAIDP - THE FINDINGS (2022)
• UNESCO AI Recommendation - social scoring and mass surveillance banned
Continued progress on implementation of OECD AI Principles
• G7 leaders embraced algorithmic transparency to combat AI bias
• US opens up policy process, embraces "democratic values"
• EU AI Act will make slow progress in 2022
• Council of Europe makes progress on AI treaty (CAHAI proposal)
• AI regulation in China leaves open big questions
• Growing global battle over deployment of facial recognition
• UN fails to reach agreement on lethal autonomous weapons
Center for AI and Digital Policy

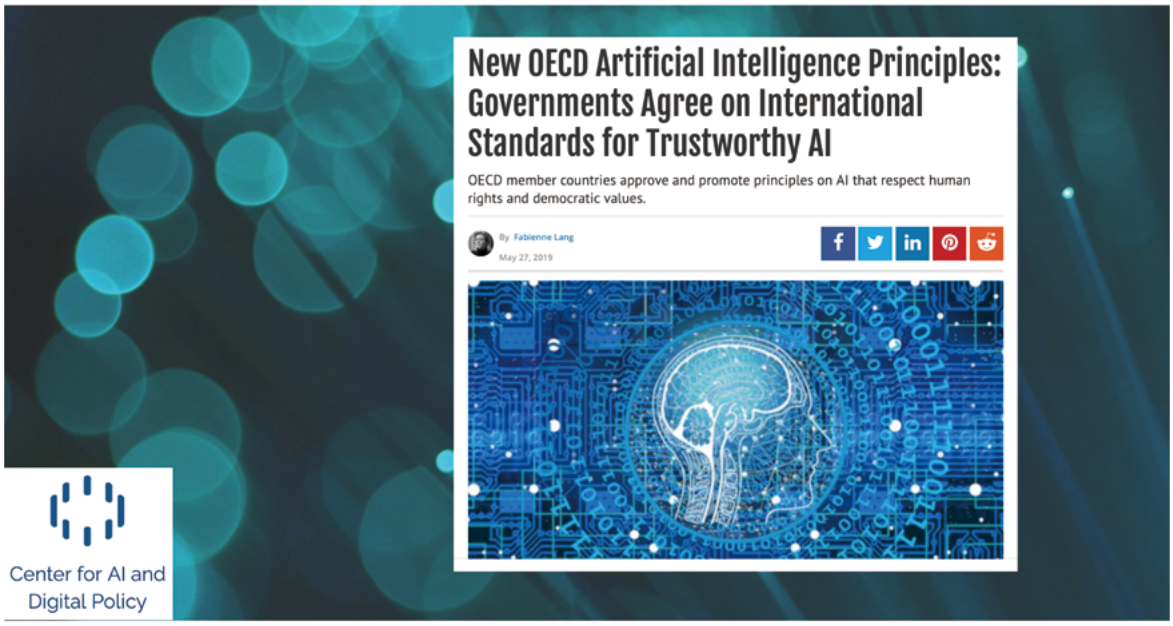

AI POLICY FRAMEWORKS
Center for AI and
Digital Policy


1. Universal Guidelines for AI (2018)
2. OECD AI Principles (2019) / G20 AI Guidelines (2019)
3. UNESCO Recommendation on AI (2021)
4. EU Artificial Intelligence Act (-2023)
5. COE AI Convention (-2023)
Center for AI and
Digital Policy

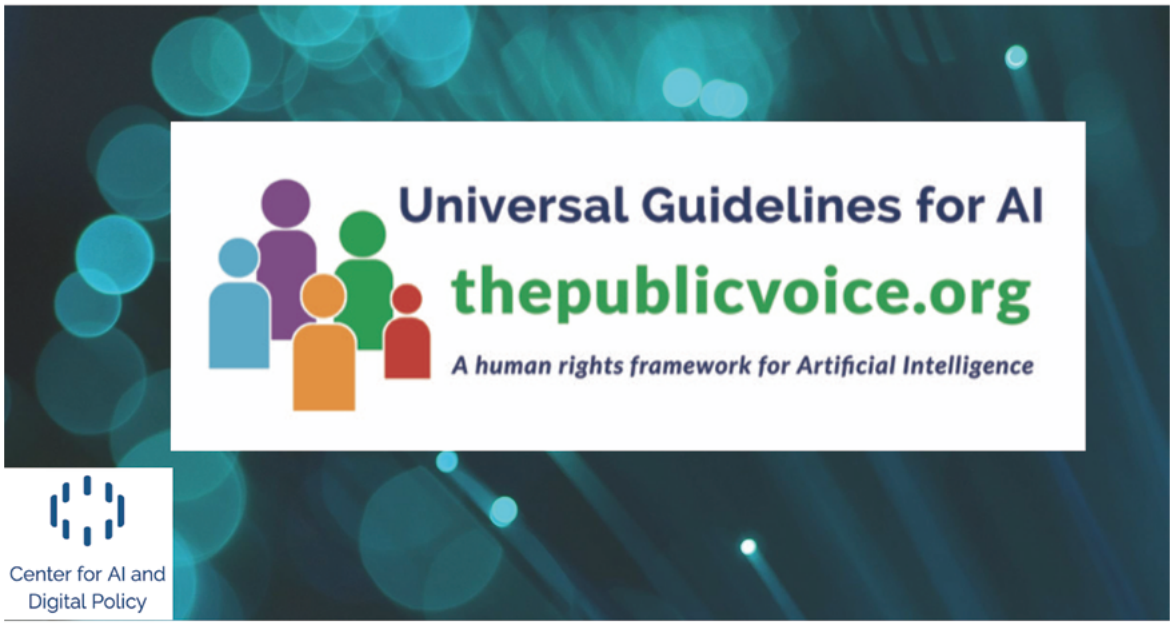
Center for AI and Digital Policy

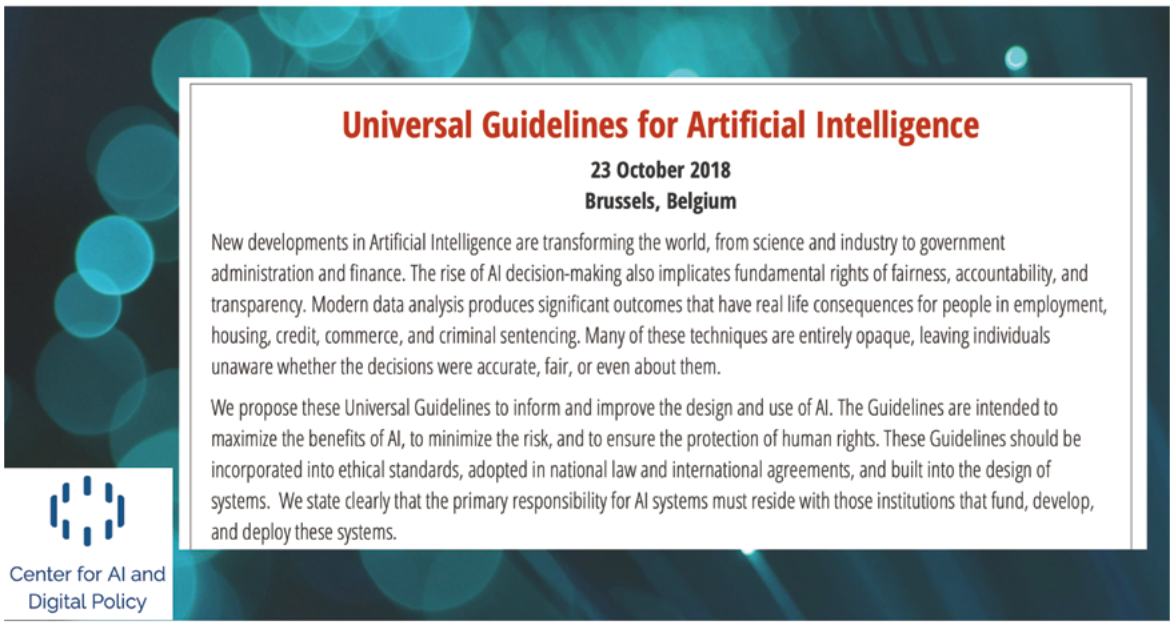


Center for AI and Digital Policy


New OECD Artificial Intelligence Principles: Governments Agree on International Standards for Trustworthy AI
OECD member countries approve and promote principles on AI that respect human rights and democratic values.
By Fabienne Lang
May 27, 2019
Center for AI and Digital Policy

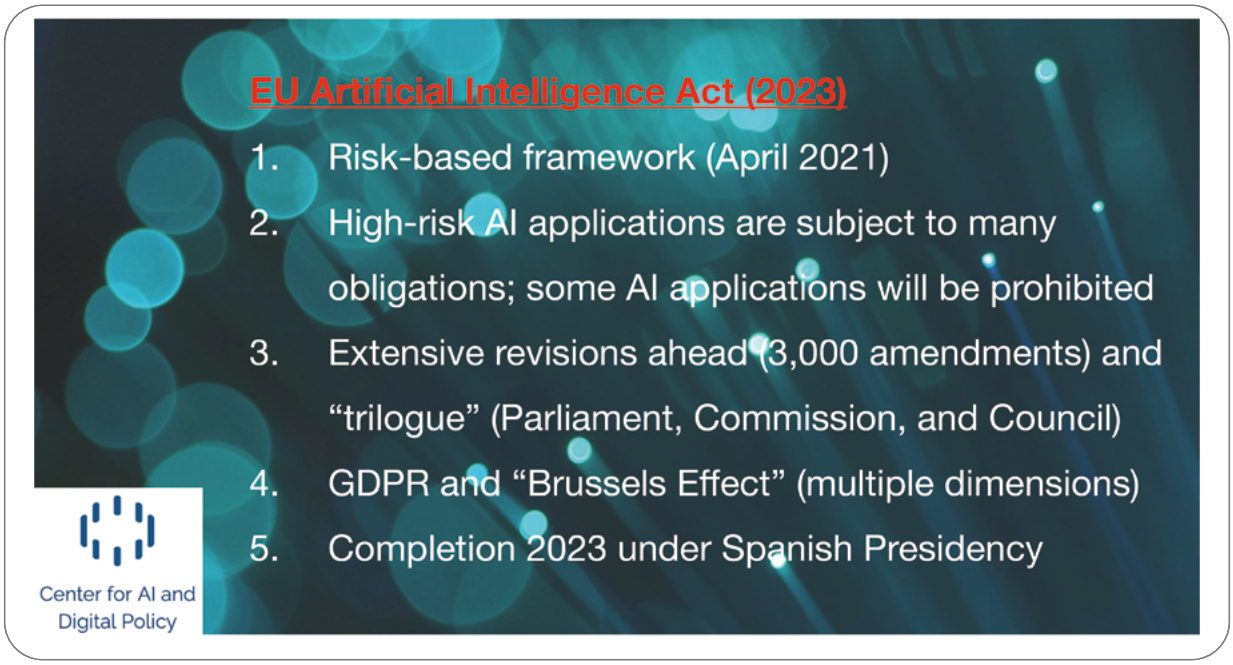

OECD AI Principles (2019)
1. General, non-binding principles for human-centric, trustworthy AI (key provision on contestability)
2. Builds on other OECD policy frameworks - privacy, computer security, risk assessment
3. Incorporated in G20 AI Guidelines, more than 50 countries (including Korea) endorsed
4. Ongoing assessment of implementation, OECD.AI
Center for AI and Digital Policy


Universal Guidelines for AI
thepublicvoice.org
A human rights framework for Artificial Intelligence
Center for AI and
Digital Policy


Universal Guidelines for Artificial Intelligence
23 October 2018
Brussels, Belgium
New developments in Artificial Intelligence are transforming the world, from science and industry to government administration and finance. The rise of AI decision-making also implicates fundamental rights of fairness, accountability, and transparency. Modern data analysis produces significant outcomes that have real life consequences for people in employment, housing, credit, commerce, and criminal sentencing. Many of these techniques are entirely opaque, leaving individuals unaware whether the decisions were accurate, fair, or even about them.
We propose these Universal Guidelines to inform and improve the design and use of AI. The Guidelines are intended to maximize the benefits of AI, to minimize the risk, and to ensure the protection of human rights. These Guidelines should be incorporated into ethical standards, adopted in national law and international agreements, and built into the design of systems. We state clearly that the primary responsibility for AI systems must reside with those institutions that fund, develop, and deploy these systems.
Center for AI and
Digital Policy

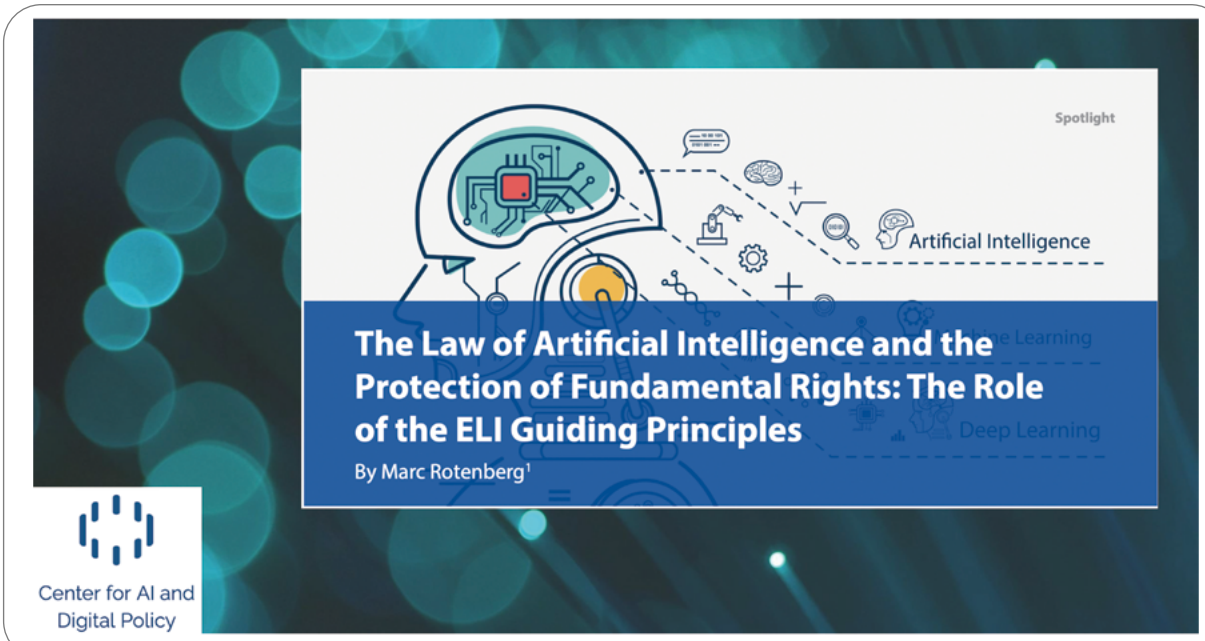

Universal Guidelines for Artificial Intelligence
1. Right to Transparency.
2. Right to Human Determination.
3. Identification Obligation.
4. Fairness Obligation.
5. Assessment and Accountability Obligation.
6. Accuracy, Reliability, and Validity Obligations.
7. Data Quality Obligation.
8. Public Safety Obligation.
9. Cybersecurity Obligation.
10. Prohibition on Secret Profiling.
11. Prohibition on Unitary Scoring.
12. Termination Obligation.
thepublicvoice.org/ai-universal-guidelines
Center for AI and Digital Policy

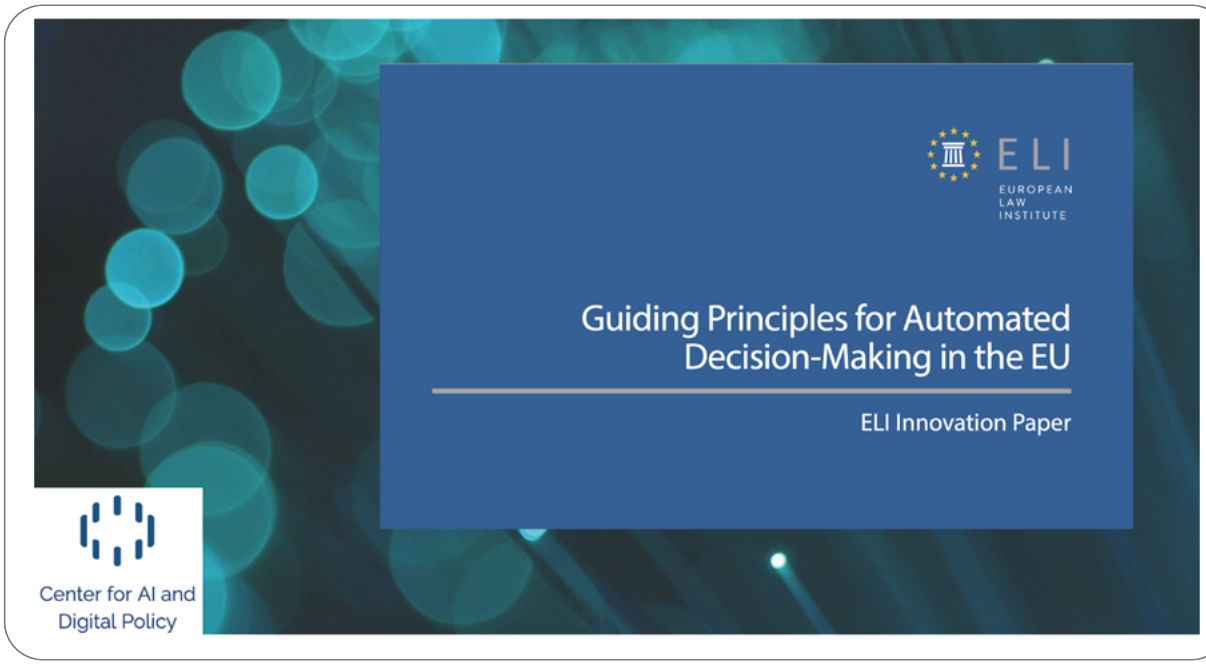

UNESCO Recommendation on AI Ethics (2021)
1. Protecting Data
2. Banning social scoring and mass surveillance
3. Monitoring and Evaluation (Ethical Impact Assessments and a Readiness Assessment Methodology)
4. Protecting the environment (fight against climate change)
=> Implementation will be critical
Center for AI and Digital Policy


EU Artificial Intelligence Act (2023)
1. Risk-based framework (April 2021)
2. High-risk AI applications are subject to many obligations; some AI applications will be prohibited
3. Extensive revisions ahead (3,000 amendments) and "trilogue" (Parliament, Commission, and Council)
4. GDPR and "Brussels Effect" (multiple dimensions)
5. Completion 2023 under Spanish Presidency
Center for AI and Digital Policy


Council of Europe Convention on AI (2023)
1. Reflects the COE commitment to democratic institutions, fundamental rights, and rule of law
2. A preliminary report from "CAHAI" (AI expert group) with proposed Legal Instruments completed in 2021.
3. Work now underway by COE Committee on AI. COE Council of Ministers to determine legal instrument
4. Open for ratification by non-member States
5. Similar to COE Privacy Convention ("108+") and COE Cybercrime Convention
Center for AI and Digital Policy


AI and Fundamental Rights
Center for AI and Digital Policy


Spotlight
Artificial Intelligence
Machine Learning
Deep Learning
The Law of Artificial Intelligence and the Protection of Fundamental Rights: The Role of the ELI Guiding Principles
By Marc Rotenberg[1]
Center for AI and Digital Policy


ELI
EUROPEAN
LAW
INSTITUTE
Guiding Principles for Automated Decision-Making in the EU
ELI Innovation Paper
Center for AI and Digital Policy


When do we prohibit AI?

The Challenge of Machine Learning

"In so far as a scientific statement speaks about reality, it must be falsifiable: and in so far as it is not falsifiable, it does not speak about reality."

- Karl Popper, The Logic of Scientific Discovery

Center for AI and Digital Policy

TOP GRANDMASTERS SPEAK ABOUT

ALPHAZERO VS STOCKFISH

Chess.com

EDITORIAL

Chess, a Drosophila of reasoning

The recent world chess championship saw Magnus Carlsen defend his title against Fabiano Caruana. But it was not a contest between the two strongest chess players on the planet, only the strongest humans. Soon after I lost my rematch against IBM's Deep Blue in 1997, the short window of human-machine chess competition slammed shut forever. Unlike humans, machines keep getting faster, and today a smartphone chess app can be stronger than Deep Blue. But as we see with the AlphaZero system (see pages 1118 and 1140), machine dominance has not ended the historical role of chess as a laboratory of cognition.

Much as the *Drosophila melanogaster* fruit fly became a model organism for geneticists, chess became a *Drosophila* of reasoning. In the late 19th century, Alfred Binet hoped that understanding why certain people excelled at chess would unlock secrets of human thought. Sixty years later, Alan Turing wondered if a chess-playing machine might illuminate, in the words of Norbert Wiener, "whether this sort of ability represents an essential difference between the potentialities of the machine and the mind."

Much as airplanes don't flap their wings like birds, machines don't generate chess braries of opening and endgame moves, AlphaZero starts out knowing only the rules of chess, with no embedded human strategies. In just a few hours, it plays more games against itself than have been recorded in human chess history. It teaches itself the best way to play, reevaluating such fundamental concepts as the relative values of the pieces. It quickly becomes strong enough to defeat the best chess-playing entities in the world, winning 28, drawing 72, and losing none in a victory over Stockfish.

I admit that I was pleased to see that AlphaZero had a dynamic, open style like my own. The conventional wisdom was that machines would approach perfection with endless dry maneuvering, usually leading to drawn games. But in my observation, AlphaZero prioritizes piece activity over material, preferring positions that to my eye looked risky and aggressive. Programs usually reflect priorities and prejudices of programmers, but because AlphaZero programs itself, I would say that its style reflects the truth. This superior understanding allowed it to outclass the world's top traditional program despite calculating far fewer positions per second. It's the embodiment of the cliché, "work smarter, not harder."

AlphaZero shows us that machines can be the experts, not merely expert tools. Ex-

"...machine dominance has not ended the historical role of chess as a laboratory of cognition."

Garry Kasparov *is the former world chess champion and the author of* Deep Thinking: Where Machine Intelligence Ends and Human Creativity Begins. *He is chairman of the Human Rights Foundation, New York, NY, USA. kasparov@hrf.org*

Center for AI and Digital Policy

CJEU PNR Decision Unplugs the 'Black Box'

Case C-817/19, Ligue des droits humains v. Conseil des Ministres [2022] ECLI:EU:C:2022:491.

*Marc Rotenberg**

Center for AI and Digital Policy

The criteria must 'target, specifically, individuals who might be reasonably suspected of involvement in terrorist offences or serious crime covered by that directive'

The PNR Directive 'precludes the use of artificial intelligence technology in self-learning systems ('machine learning'), capable of modifying without human intervention or review the assessment process.' (AG)

Ligue des droits humains (The PNR case), C-817/19 (June 2022)

'given the opacity which characterises the way in which artificial intelligence technology works, it might be impossible to understand the reason why a given program arrived at a positive match'.

- **PNR Directive Art. 6(3)(b)**
- **CFR, Arts. 7, 8, 21, 47**

algorithms 'must function transparently and that the result of their application must be traceable'

Center for AI and Digital Policy

Good AI

Rule-based Expert Systems
Explicit criteria
Fixed outcomes

Bad AI

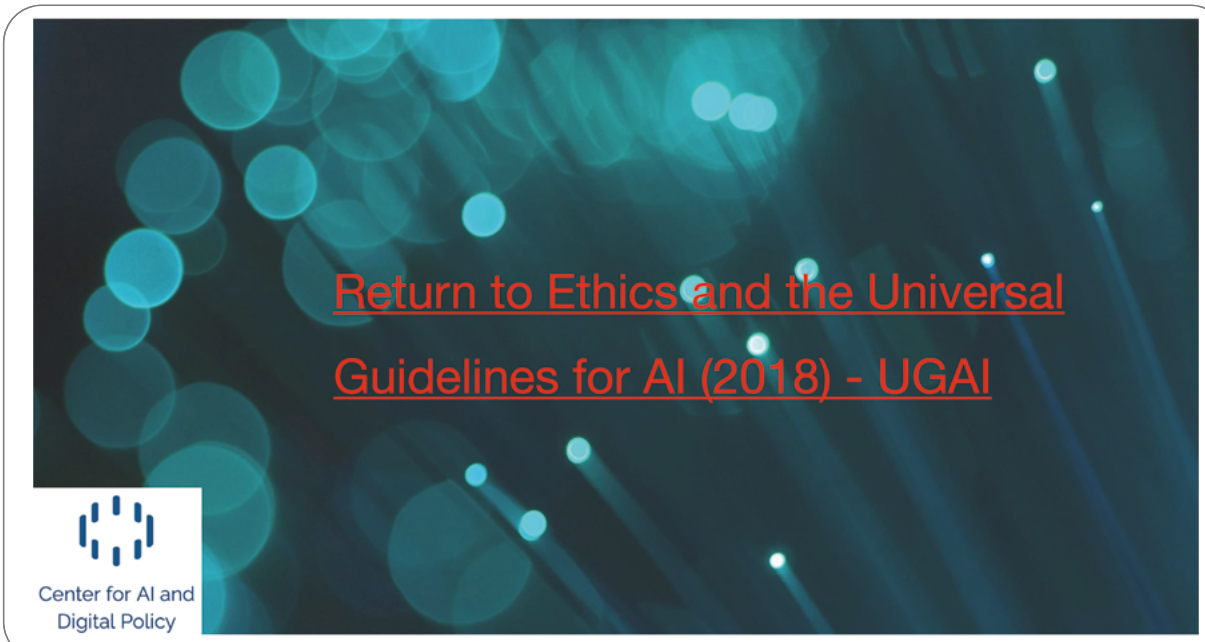
Machine Learning Systems
Reinforcement Learning
Statistical outcomes
Generative AI

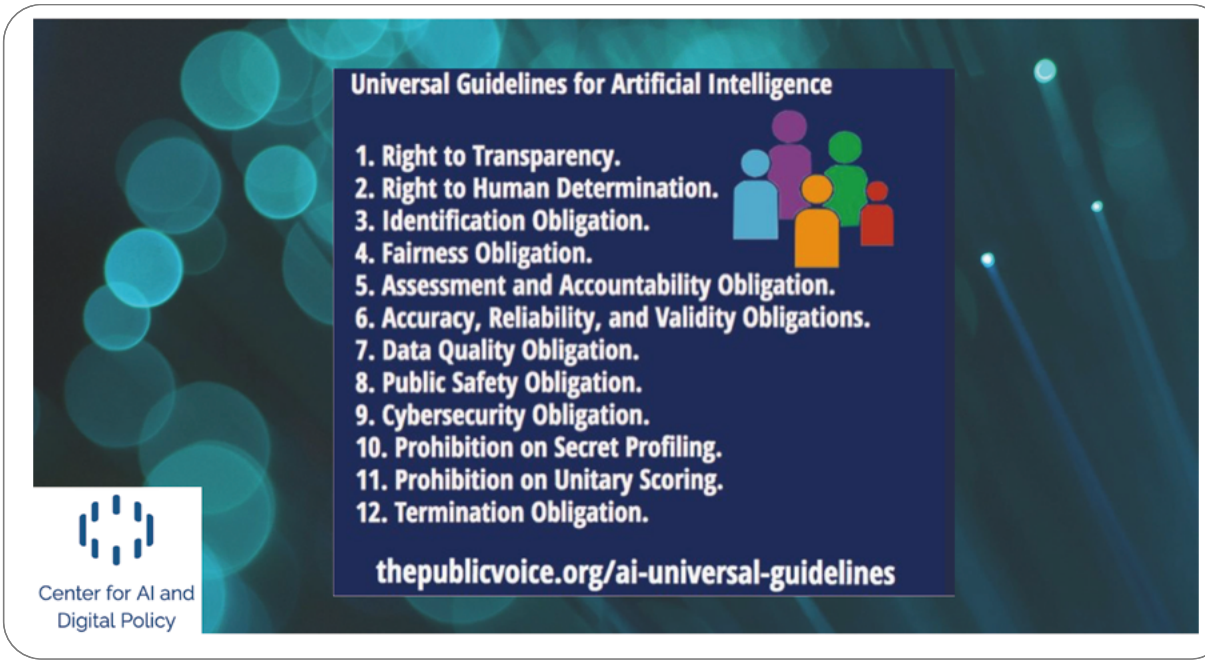
Center for AI and Digital Policy

AIProhibitions

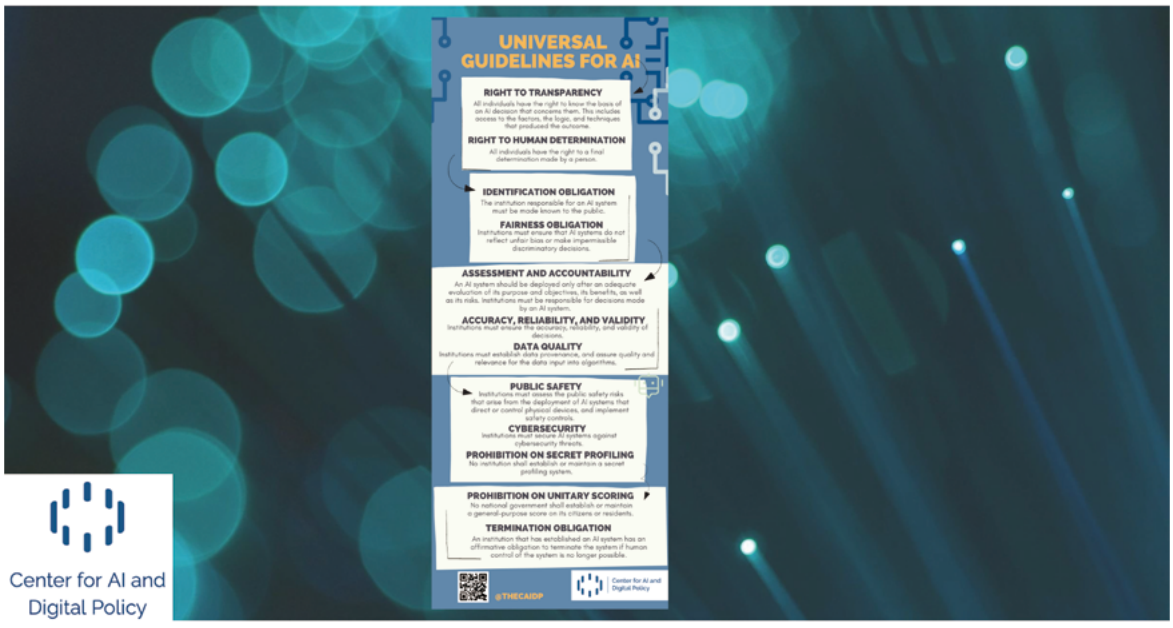
1. Fail to comply with international human rights standards (UN OHCHR)
2. Social Scoring (UNESCO 2021)
3. Mass Surveillance (UNESCO 2021)
4. Biometric categorization (?) (EU AIA)
5. Emotion recognition (?) (EU AIA)
6. Predictive policing (?) (EU AIA)
7. Generative AI and fundamental rights (??)

Center for AI and Digital Policy


Return to Ethics and the Universal Guidelines for AI (2018) - UGAI
Center for AI and Digital Policy


Universal Guidelines for Artificial Intelligence
1. Right to Transparency.
2. Right to Human Determination.
3. Identification Obligation.
4. Fairness Obligation.
5. Assessment and Accountability Obligation.
6. Accuracy, Reliability, and Validity Obligations.
7. Data Quality Obligation.
8. Public Safety Obligation.
9. Cybersecurity Obligation.
10. Prohibition on Secret Profiling.
11. Prohibition on Unitary Scoring.
12. Termination Obligation.
thepublicvoice.org/ai-universal-guidelines
Center for AI and Digital Policy


CONFERENCE
"THE UNIVERSAL GUIDELINES FOR AI AFTER 5 YEARS"
2018- 2023
HYBRID EVENT
50 INVITEES IN PERSON
2 KEYNOTES | 4 PANELS
OCTOBER 5TH
CENTER FOR AI AND DIGITAL POLICY
WASHINGTON D.C
Center for AI and Digital Policy
MORE INFO: CAIDP.ORG | @THECAIDP


UNIVERSAL GUIDELINES FOR AI
RIGHT TO TRANSPARENCY
All individuals have the right to know the basis of an AI decision that concerns them. This includes access to the factors, the logic, and techniques that produced the outcome.
RIGHT TO HUMAN DETERMINATION
All individuals have the right to a final determination made by a person.
IDENTIFICATION OBLIGATION
The institution responsible for an AI system must be made known to the public.
FAIRNESS OBLIGATION
Institutions must ensure that AI systems do not reflect unfair bias or make impermissible discriminatory decisions.
ASSESSMENT AND ACCOUNTABILITY
An AI system should be deployed only after an adequate evaluation of its purpose and objectives, its benefits, as well as its risks. Institutions must be responsible for decisions made by an AI system.
ACCURACY, RELIABILITY, AND VALIDITY
Institutions must ensure the accuracy, reliability, and validity of decisions.
DATA QUALITY
Institutions must establish data provenance, and assure quality and relevance for the data input into algorithms.
PUBLIC SAFETY
Institutions must assess the public safety risks that arise from the deployment of AI systems that direct or control physical devices, and implement safety controls.
CYBERSECURITY
Institutions must secure AI systems against cybersecurity threats.
PROHIBITION ON SECRET PROFILING
No institution shall establish or maintain a secret profiling system.
PROHIBITION ON UNITARY SCORING
No national government shall establish or maintain a general-purpose score on its citizens or residents.
TERMINATION OBLIGATION
An institution that has established an AI system has an affirmative obligation to terminate the system if human control of the system is no longer possible.
@THECAIDP
Center for AI and Digital Policy
Center for AI and Digital Policy

The 12th

Asia Privacy Bridge Forum 2023

Day 1 **Session 1**

Session Chair

Kwang Bae Park

Attorney, Lee&Ko, Korea

1

Josh Lee Kok Thong

Managing Director, Future of Privacy Forum, NGO

2

Hitomi Iwase

Attorney, Nishimura & Asahi, Japan

3

Raina Yeung

Director of Privacy and Data Policy Engagement, APAC at META

The 12th

Asia Privacy Bridge Forum 2023

Josh Lee Kok Thong

Managing Director, Future of Privacy Forum, NGO

ABOUT FPF

FPF Global Offices:
Washington, D.C.
Brussels
Singapore
Tel Aviv

The Future of Privacy Forum (FPF) is a **global** non-profit organization that brings together academics, civil society, government officials, and industry to evaluate the societal, policy, and legal implications of data uses; identify the risks; and develop appropriate protections.

fpf.org

FUTURE OF PRIVACY FORUM

FPF MEMBERS AND TEAM

200 Companies

20+ Civil Society

45+ Academics

50+ Staff & Fellows

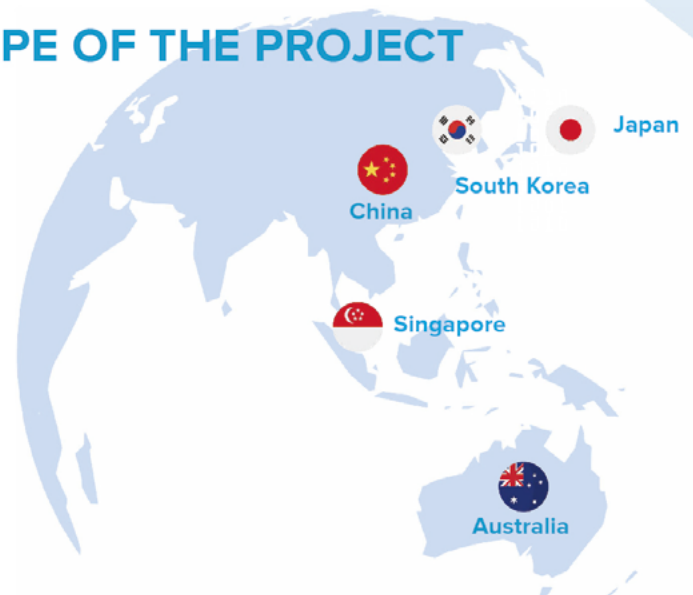
FPF Workstreams

Ad Tech	Digital Identity	Open Banking
AI & Machine Learning	Ethics	Policymaker Education
AR/VR	Global & Europe	Research
Biometrics	Health	Smart Communities
De-Identification	Mobility & Location	Youth & Education

fpf.org

FUTURE OF PRIVACY FORUM

SCOPE OF THE PROJECT



fpf.org

FUTURE OF PRIVACY FORUM

SCOPE OF THE PROJECT

Publish a report that will:

- Provide stakeholders with an **accessible explanation of how generative AI systems work**;
- Identify **policy issues** arising from these technologies;
- Assess whether **existing laws and regulations** and **emerging AI governance frameworks** are **suitable to address these issues**; and
- Suggest **approaches** that stakeholders can adopt to **address these issues**.

fpf.org

FUTURE OF PRIVACY FORUM

GENERATIVE AI

A category of artificial intelligence (AI) models that **generate new content**, including, but not limited to:

- **Text**
- **Images**
- **Video**
- **Music**
- **Speech**
- **Computer code**.

fpf.org

FUTURE OF PRIVACY FORUM

Artificial Intelligence (AI)

Any technique that enables a computer to imitate human intelligence using logic, if-then statements, or machine learning

Machine Learning (ML)

A subset of AI that uses machines to search for patterns in data to build logic models automatically.

Deep Learning (DL)

A subset of ML that is composed of deeply multi-layered neural networks that perform tasks like speech and image recognition.

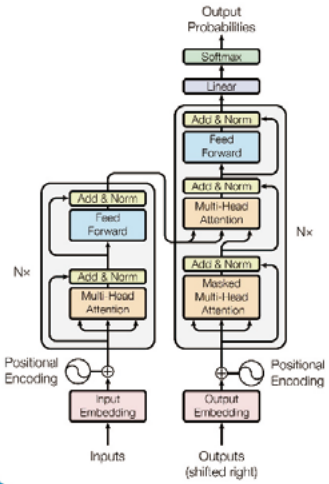
Generative AI

A subset of DL that is powered by "foundation models" – large models that are pre-trained on vast datasets.

FUTURE OF PRIVACY FORUM

fpf.org

FOUNDATIONAL MODELS



Transformers + "Attention" + Large unstructured datasets

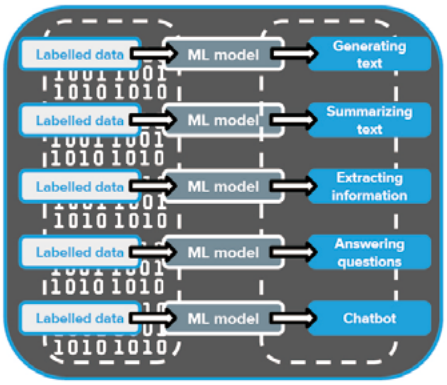
Examples:

- General Pretrained Transformer (GPT)
- Bidirectional Encoder Representations from Transformers (BERT)

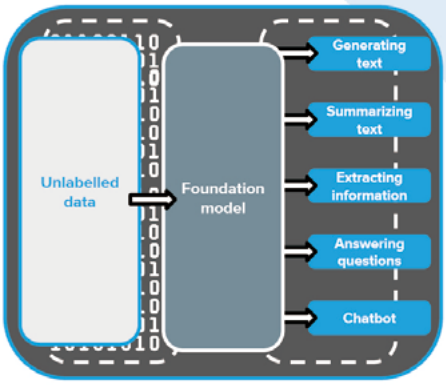
FUTURE OF PRIVACY FORUM

fpf.org

FOUNDATION MODELS



Traditional ML models



Foundation models

fpf.org

FUTURE OF PRIVACY FORUM

FOUNDATION MODELS

Examples:

- **Visual data** e.g., CLIP, GPT-4 (OpenAI); FLAVA (Meta), Flamingo (DeepMind)
- **Computer code** e.g., Codex (OpenAI); Github Copilot (Microsoft), AlphaCode (DeepMind), Project Wisdom (IBM)
- **Chemistry data** e.g., ChemBERTa (University of Toronto); Chemformer (AstraZeneca), MoLFormer (IBM)
- **Climate data** e.g., ClimaX (microsoft); Chemformer (AstraZeneca), IBM geospatial intelligence foundation model
- **Financial data** e.g., BloombergGPT (Bloomberg)

fpf.org

FUTURE OF PRIVACY FORUM

WHY DOES THIS MATTER?

Oops: Samsung Employees Leaked Confidential Data to ChatGPT

Employees submitted source code and internal meetings to ChatGPT just weeks after the company lifted a ban on using the chatbot.

10 reasons to worry about generative AI

After decades of speculation, real-world artificial intelligence has finally hit a tipping point. Now that we know what AI models like ChatGPT and DALL-E can do, should we be worried?

Lawyer apologizes for fake court citations from ChatGPT

ChatGPT banned in Italy over privacy concerns

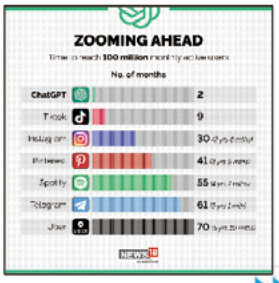
Commentary: ChatGPT is a data privacy nightmare - anyone who has ever posted online ought to be concerned

ChatGPT creator OpenAI Inc has been sued for stealing "vast amounts" of personal information to train its artificial intelligence models in a heedless hunt for profits. Together with Microsoft, its major backer, the company was sued on Wednesday by sixteen pseudonymous individuals who claim the companies AI products based on ChatGPT collected and divulged their personal information without adequate notice or consent.

A.I.-generated images of Pope Francis have earned more views, likes and comments than many other A.I. photos.

How ChatGPT Kicked Off an A.I. Arms Race

Man ends his life after an AI chatbot 'encouraged' him to sacrifice himself to stop climate change



FUTURE OF PRIVACY FORUM

fpf.org

AI Governance Frameworks

Ethical Principles

- Australia: AI Ethics Principles
- China: Ethical Norms for New Generation AI
- Japan: Social Principles of Human Centric AI
- Singapore: Model AI Governance Framework, Annex A
- South Korea: Human-Centered National Guidelines for AI Ethics

Guidance on Internal Governance

- Australia: Tech Trends Position Statement – Generative AI (eSafety Commissioner)
- Japan: Governance Guidelines for Implementation of AI Principles (METI)
- Singapore: Model AI Governance Framework (IMDA)

Laws and Regulations

- China: Regulations on the Administration of Deep Synthesis of Internet Information Technology.

  Interim Measures for the Management of Generative Artificial Intelligence Services.
- South Korea: AI Bill (draft)

- Accountability
- Explainability
- Fairness
- Human Centricity
- Privacy
- Reliability, Safety, Control
- Security
- Transparency

FUTURE OF PRIVACY FORUM

fpf.org

AI-SPECIFIC: VOLUNTARY FRAMEWORKS

Ethical Principles

- Australia: AI Ethics Principles
- China: Ethical Norms for New Generation AI
- Japan: Social Principles of Human Centric AI
- Singapore: Model AI Governance Framework, Annex A
- South Korea: Human-Centered National Guidelines for AI Ethics

Guidance on Internal Governance

- Australia: Tech Trends Position Statement – Generative AI (eSafety Commissioner)
- Japan: Governance Guidelines for Implementation of AI Principles (METI)
- Singapore: Model AI Governance Framework (IMDA)

fpf.org

FUTURE OF PRIVACY FORUM

AI-SPECIFIC: VOLUNTARY FRAMEWORKS

Preliminary findings: Emerging consensus around ethical principles for AI in APAC (and beyond). Most frameworks share the following 8 principles in some form:

- Accountability
- Human Centricity
- Fairness
- Privacy
- Reliability, Safety, Control
- Security
- Explainability
- Transparency

fpf.org

FUTURE OF PRIVACY FORUM

AI-SPECIFIC: LAWS AND REGULATIONS

AI-Specific Laws and Regulations

China:

- **Regulations on the Administration of Deep Synthesis of Internet Information Technology.**
- **Interim Measures for the Management of Generative Artificial Intelligence Services.**
- **(National law?)**

South Korea:

- **AI Bill (draft)**

Other Laws and Regulations

- **Personal data protection and privacy laws.**
- **Intellectual property.**
- **Consumer protection law.**
- **Competition law.**
- **Sectoral laws.**
- **Criminal law.**
- **Civil remedies.**

FUTURE OF PRIVACY FORUM

fpf.org

ROLE OF DATA PROTECTION LAWS AND DPAS

Globally and in the Asia-Pacific region, data protection authorities are acting as "de-facto regulators" of generative AI and have been the most proactive regulators in addressing policy risks from generative AI.

ChatGPT banned in Italy over privacy concerns

By Shiona McCallum
Technology reporter

Italy has become the first Western country to block advanced chatbot ChatGPT.

The Italian data-protection authority said there were privacy concerns relating to the model, which was created by US start-up OpenAI and is backed by Microsoft.

OpenAI under the Japanese watchdog's scrutiny over data collection

A Japanese privacy watchdog has issued a warning to OpenAI over the collection of sensitive data without individuals' permission.

South Korea: PIPC fines OpenAI KRW 3.6 million following data breach

ico. The ICO exists to empower you through information.

Generative AI: eight questions that developers and users need to ask

FUTURE OF PRIVACY FORUM

fpf.org

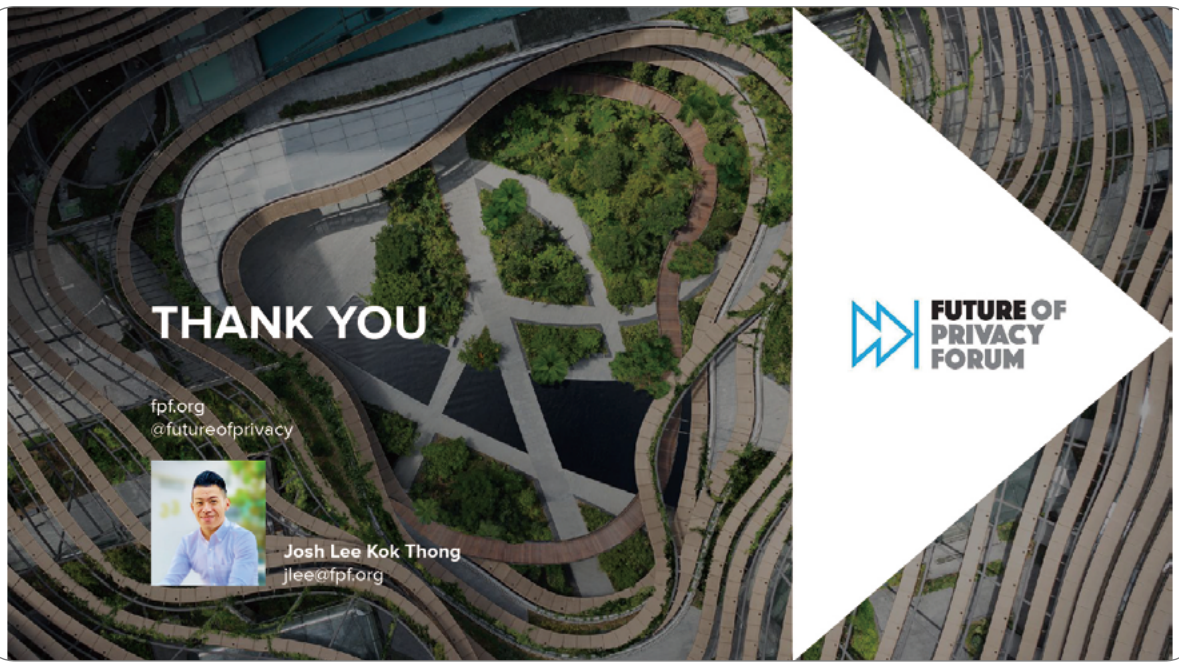
EARLY FINDINGS

Through multi-stakeholder discussions, early findings about potential approaches to generative AI include:

- An **agile, future-proof approach** to AI governance;
- **Developing existing governance principles** incrementally, rather than enacting "hard law;"
- Ensuring that principles account for **different use cases for the technology** and **different concerns at each layer** of the AI technology stack, i.e.,
  - Infrastructure;
  - Models;
  - Applications.
- Ensuring responsible **open-source innovation**;
- Not just future-proofing regulation, **but backwards-compatible regulation**;
- Avoiding **cross-border disharmony**;
- Working on **standards and common taxonomies**.

fpf.org

FUTURE OF PRIVACY FORUM



The 12th

Asia Privacy Bridge Forum 2023

Hitomi Iwase

Attorney, Nishimura & Asahi, Japan

NISHIMURA & ASAHI

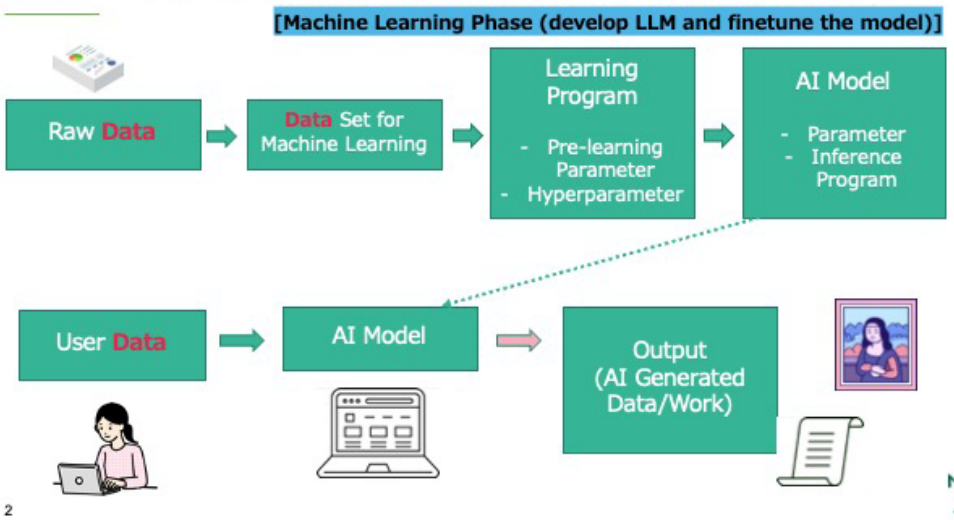
AI Transparency from a Japanese Privacy Law Perspective

October 12, 2023

Hitomi Iwase

1

Intro – What Does AI (Generative AI) Do?



2

Japanese Privacy Law (APPI)

- **Definition of "Personal Information"/"Personal Data" under the APPI* can be quite broad**
  - "Personal Information" is information about a living individual that meets either of the following descriptions:
    i. information that can identify a specific individual by name, date of birth, or other description contained in such information (including information that would allow easy reference to other information and thereby enable identification of a specific individual); or
    ii. information that contains a Personal Identification Code**.

*The Act on the Protection of Personal Information (Act No. 57 of 2003) (*kojinjoho no hogo ni kansuru horitsu*)

**Personal Identification Code: a code (including characters, numerical characters, and marks) that can be used to identify a specific individual and is designated by a Cabinet Order. The relevant Cabinet Order provides that a Personal Identification Code includes DNA sequence data, iris pattern data, gait pattern data, palm print data, voice recognition data, basic pension numbers, and national health insurance numbers

NISHIMURA & ASAHI

Japanese Privacy Law (APPI)

- **When collecting Personal Information…**
  - You must not acquire Personal Information by deception or other wrongful means
  - You must specify the Purpose of Use to the extent possible, on the basis that such Purpose of Use is reasonably foreseeable or can be anticipated by you at the time of acquisition
  - You must notify data subjects of or publicly announce the Purpose of Use immediately after its acquisition, except in cases where the Purpose of Use has already been publicly announced
  - No concept of "legitimate interest" like in the GDPR
  - No consent is necessary in principle
    - But in case of collecting Special Care-Required Personal Information (sensitive personal information)* you must obtain prior data subject consent (there are some exceptions to this rule)

*Special Care-Required Personal Information: Personal Information comprising an individual's race, creed, social status, medical history, criminal record, fact of having suffered damage by a crime, or other descriptions, etc. prescribed by a Cabinet Order as those whose handling requires special care so as not to cause unfair discrimination, prejudice, or other disadvantages to the individual.

NISHIMURA & ASAHI

Japanese Privacy Law (APPI)

- **When using Personal Information/Personal Data･･･**
  - You must not use Personal Information beyond the scope necessary to achieve the specified Purpose of Use without obtaining prior data subject consent
  - You must not change the Purpose of Use beyond that reasonably related to the Purpose of Use before the change
  - You must strive to keep Personal Data accurate and up to date within the scope necessary to achieve the Purpose of Use and to delete Personal Data without delay when such utilization has become unnecessary
  - You must not use Personal Information in a manner that has the potential to incite unlawful or unfair acts
  - You must take necessary and appropriate action for security control
  - There are some requirements for disclosure (details regarding the data and the operator)

NISHIMURA & ASAHI

Japanese Privacy Law (APPI)

- **When transferring Personal Data･･･**
  - You must not provide Personal Data to a third party without prior data subject consent (there are some exceptions to this rule)
  - There are also some exceptions to "third party" where no consent is necessary
    - Service provider exception: where Personal Data are transferred as a result of commissioning a third-party service provider for all or part of the processing of the Personal Data that is necessary to achieve the Purpose of Use, and the service provider does not process the data for its own Purpose of Use ➔ no consent is necessary, but you must exercise necessary and appropriate supervision over the entrusted party
  - There are also different requirements for cross-border data transfers

NISHIMURA & ASAHI

Development of AI Models

- **Collecting and using Personal Data for the purpose of developing AI models are relatively easy**
  - You need to specify the Purpose of Use and put it in your privacy policy; but as long as AI development (machine learning) is included in the Purpose of Use, you can use the data for that purpose
  - No special rules for the Personal Data of minors
  - Exception is Special Care-Required Personal Information (sensitive personal information)
- When obtaining data from a common crawl or similar organization, you need to know how the data was collected and whether any Special Care-Required Personal Information (sensitive personal information) is included
- **PPC's Cautionary Reminder to a Developer of Generative AI (issued on June 2, 2023)** [*next slide]

NISHIMURA & ASAHI

*PPC's Cautionary Reminder to a Developer of Generative AI (June 2, 2023)

- **Acquisition of Special Care-Required Personal Information (sensitive personal information)**
  - Do not acquire sensitive personal information without prior consent
  - Regarding collecting information publicly available on the Internet for training models:
    - i. take necessary measures to exclude sensitive personal information when collecting information;
    - ii. take measures to reduce the amount of sensitive personal information to the extent possible from the collected information as soon as you can after collecting the information;
    - iii. in the case where you find out that sensitive personal information is included in collected information even after taking the measures described in (i) and (ii) above, take measures to delete the sensitive personal information or to make it impossible to identify a data subject as soon as you can and before processing it into training data; and
    - iv. in the case where a data subject or the PPC, etc. requests or instructs that sensitive personal information not be collected from a specific website or third party, follow the request or instruction unless there is a justifiable reason.
- **Notification of Purpose of Use, Etc.**
  - Publicly announce the Purpose of Use of Personal Information of users and persons other than users in Japanese or notify them of the purpose in Japanese

NISHIMURA & ASAHI

Use of AI

- Input a prompt containing Personal Data
  - Data transfer to AI vendor? – Consent required, or is the service provider exception applicable?

- PPC's Cautionary Reminder on Use of Generative AI Services (issued on June 2, 2023) [*next slides]

NISHIMURA & ASAHI

*PPC's Cautionary Reminder on Use of Generative AI Services (June 2, 2023)

- **For Business Operators**
  - When inputting a prompt containing Personal Information into a generative AI service, sufficiently confirm that the input is within the scope necessary to achieve the specified Purpose of Use of the relevant Personal Information.
  - If you enter a prompt containing Personal Data into a generative AI service without obtaining prior data subject consent, and the relevant Personal Data is handled for any purposes other than outputting the response to the prompt, the Personal Information handling business operator may be in violation of the provisions of the APPI; therefore, when inputting such prompts, sufficiently confirm that no generative AI service vendor will use such Personal Information for training AI models.

NISHIMURA & ASAHI

*PPC's Cautionary Reminder on Use of Generative AI Services (June 2, 2023)

- **For general users**
  - Personal Information entered in generative AI services may be used for training generative AI models, and there is a risk that Personal Information entered in generative AI services may output on the basis of statistical linkages with other information, and with accurate or inaccurate content. Therefore, when inputting, etc. Personal Information into a generative AI service, take such risks into consideration and make an appropriate decision.
  - Responses to prompts of generative AI services may include inaccurate content. For example, some generative AI services are capable of outputting natural sentences as response results, but since such sentences are generated based on probabilistic correlations, there is a risk that the response results may contain inaccurate Personal Information. Therefore, when handling Personal Information using a generative AI service, it should be noted that general users should make an appropriate decision in light of such risks.
  - General users of generative AI services should fully check the terms of use and privacy policy of the generative AI service providers and make appropriate decisions regarding the use of the services considering the content of information to be input.

NISHIMURA & ASAHI

Conclusion

- Under the current Japanese privacy law (APPI), there seem to be no critical challenges to developing and using AI; however, rules regarding sensitive data could raise some issues in developing AI model
- Due to the "black box" feature of AI (generative AI), transparency as to how data are collected and used is key
- Without transparency, users, including companies and consumers, would not be able to accurately and appropriately determine risks and liabilities associated with use of AI

NISHIMURA & ASAHI

Speaker

Hitomi Iwase

Partner | Tokyo
h.iwase@nishimura.com

Hitomi is a partner in the firm's IP/IT practice and heads the trademark/design team. She covers all aspects of intellectual property (IP), information technology (IT), and data.

Hitomi handles patents, copyrights, trademarks, trade secrets, and other IP-related matters in multiple business sectors, including IT, life sciences and healthcare, machinery, food, fashion, environment and energy, entertainment, financial services, and e-commerce. Hitomi's expertise encompasses all forms of IP transactional work, both cross-border and domestic, including licensing, strategic alliances, joint development, and asset transfers, as well as various types of IP disputes, including patent/trademark infringement litigation.

She regularly advises clients on emerging legal issues relating to the latest technology, such as IoT and artificial intelligence (AI), as well as on complex system-related transactions and disputes over such transactions.

In the area of data privacy, she extensively provides advice on data protection and privacy compliance including establishing global compliance systems as well as data breach responses.

Experience

- IP Litigation / IP Transactions
- Trade Secrets / Unfair Competition
- Anti-Counterfeiting / Brand Management
- Personal Data & Privacy / Big Data Businesses
- IT

13

Professional Experience

- 2023 - Board Member, International Association for the Protection of Intellectual Property
- 2021 - Regional Vice Chair Asia Pacific, Intellectual Property Practice Group of Lex Mundi
- 2019 - Advisor, Japan DPO Association

Publications

- 2022.6 Practical Law Global Guide 2022: Intellectual Property Transactions – Japan
- 2020.9. Corpus Juris Series - Personal Information Protection Legislation (Global)
- 2020.8 Amendments to the Act on the Protection of Personal Information in 2020 and Practical Approaches

Education

- Stanford Law School (LL.M.)
- Waseda University (LL.B.)

Awards

Chambers Global 2023 Hitomi Iwase
Chambers Asia-Pacific 2023 Hitomi Iwase
The Legal 500 Asia Pacific Leading Individual 2023

NISHIMURA & ASAHI

NISHIMURA & ASAHI

Nishimura & Asahi (Gaikokuho Kyodo Jigyo)

Otemon Tower, 1-1-2 Otemachi, Chiyoda-ku
Tokyo 100-8124, Japan

The 12th

Asia Privacy Bridge Forum 2023

Raina Yeung

Director of Privacy and Data Policy Engagement, APAC at META

The 12th

Asia Privacy Bridge Forum 2023

Day 1 Session 2

Session Chair

Jong Soo Yoon
Lee&Ko, Attorney, Korea

1 **Peng Cai**
Attorney, Zhong Lun, China

2 **Eunjung Han**
Attorney, ROUSE, Vietnam

3 **Byungnam Lee**
Senior Advisor, Kim&Chang, Korea

The 12th

Asia Privacy Bridge Forum 2023

Peng Cai

Attorney, Zhong Lun, China

Challenges and Solutions for China CBDT

the latest regulatory development in a nutshell

Peng Cai

October 2023

中倫 ZHONG LUN

Speaker Bio

Peng Cai

Tel : +86 (10) 5957 2786

Email: caipeng@zhonglun.com

Practice Areas and Experience:

Mr. Peng Cai specializes in cybersecurity and data protection, serving diverse sectors such as TMT, manufacturing, finance, and healthcare. With a deep involvement in legislation and hands-on practice, he focuses on helping clients navigate complex challenges like data and privacy compliance amid various scenarios such as stringent regulatory environments, IPOs, and global expansions.

Highly skilled in managing data security risks and compliance challenges, Mr. Cai's expertise encompasses network security, data lifecycle compliance, privacy risk identification, and cross-border data transfer schemes. He excels at devising global privacy compliance strategies, incident response, and data audits. Additionally, he adeptly advises businesses on digital transformation, from risk identification to transactional structuring and compliance measures for online operations.

Work Experience

- From 2016 to present, Beijing Zhonglun Law Firm, Partner
- From 2016 to present, the E-commerce Law Committee of the Beijing Bar Association, Director

Education Background

- Australian Awards Leadership Program, Australia
- School of law Wuhan University, PRC

Major Honors and Awards

- Leading Lawyer (The Legal 500, 2021/2022/2023)
- Top 15 TMT Lawyers in China (ALB, 2022)
- Outstanding Contribution Award for the Beijing Olympics by the Beijing Bar Association

2

ZHONG LUN 中倫律師事務所

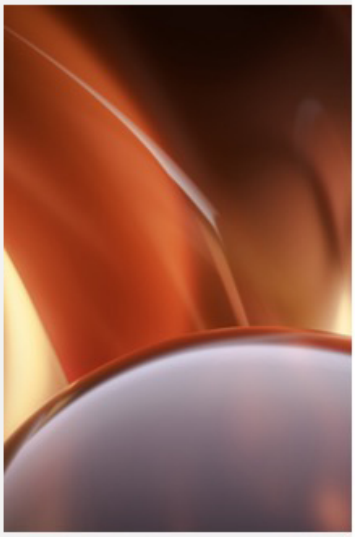


TABLE OF CONTENT

ZHONG LUN 中倫律師事務所

CBDT Legal Framework in China

Pillar laws regulating cross-border data transfer

① Cyber Security Law of the People's Republic of China (2017)

② Data Security Law of the People's Republic of China (2021)

③ PI Protection Law of the People's Republic of China (2021)

Important regulations and National Standards governing cross-border data transfer

① Measures for the Security Assessment of Outbound Data Transfer (2022)

② TC260-PG-20222A V.2.0 (2022)

③ Measures for the Standard Contract of Outbound Transfer of PI (2023)

④ Provisions on Regulating and Facilitating Cross-border Data Flows (Draft for Comments）（2023）

➢ **Major Regulatory Bodies**

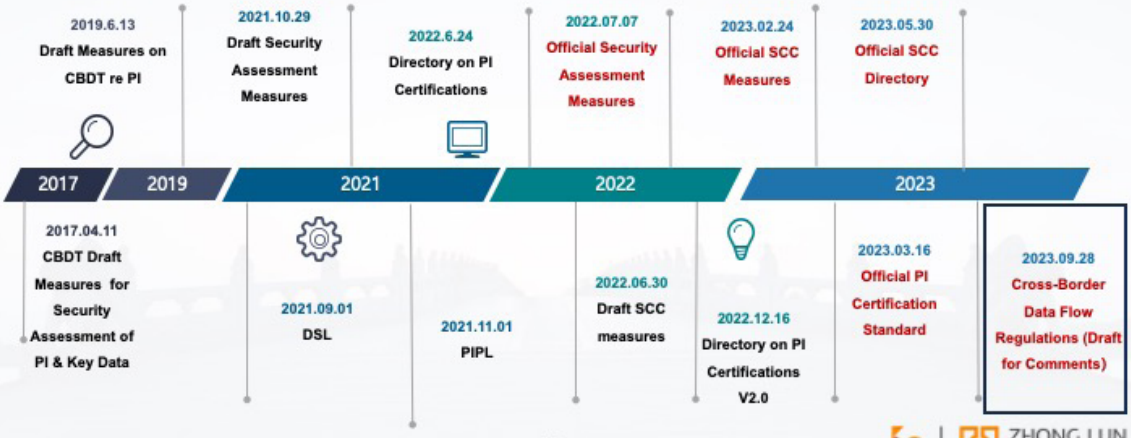
中华人民共和国国家互联网信息办公室 | 国家市场监督管理总局 | 中华人民共和国国家发展和改革委员会 | 公安 POLICE

4

ZHONG LUN 中倫律師事務所

Trends: Ongoing Refinements in China's CBDT Legislation

■ Current Status in a Nutshell: ***Forming Three Distinct CBDT Mechanism Centered on Article 38 of the PIPL***



5

ZHONG LUN 中倫律師事務所

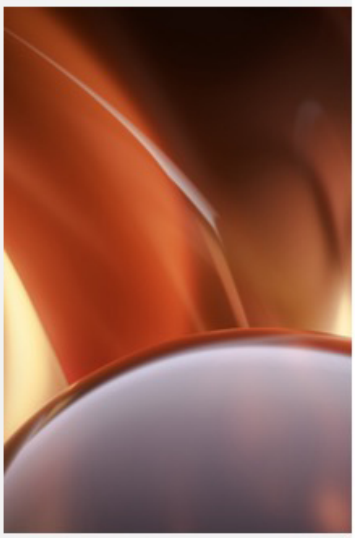


TABLE OF CONTENT

ZHONG LUN 中倫律師事務所

Current Challenges in Security Assessment for CBDT

■ Key Factors Affecting Success Rate in Security Assessment—From the Latest Regulatory Perspective

1. **Lack of Key Evidence for Compliant CBDT:** For instance, companies often fail to provide compliant documentation and backend records showing that PI subjects have consented to CBDT, thereby undermining their legal basis to substantiate their CBDT.
2. **Lack of Necessity in CBDT Scenarios:** MNCs declaring Security Assessment often fails to present compelling cases, resulting in insufficient reasoning and evidence, making it more likely for their declaration to be denied.
3. **Lack of Necessity in Data Fields for CBDT:** MNCs struggle with providing necessary justification for specific data fields required for CBDT, failing to present compelling cases to regulatory bodies concerning why these particular fields must be transferred abroad.
4. **Strict Review Standards:** Due to the CAC's rigorous scrutiny of security assessments and the general lack of in-depth understanding of regulatory requirements among MNCs, the overall pass rate for security assessments is low. (SH CAC: less than 1% passing rate)
5. **Lack of Corrective Measures:** Regulators discourage bulk CBDT lacking requisite legality, necessity, and legitimacy justification. Remedial actions like localization should be clearly outlined in CDBT Risk Assessment Report.
6. **Other Factors Affecting Passing Approval:** Missing fair forecasts for future CBDT PI subjects; lack of plans regarding the treatment of PI by foreign recipients after its storage period has expired, etc.

Any declaration not in compliance with the Data Export Security Assessment Guidelines (First Edition)'will be rejected by regulators.

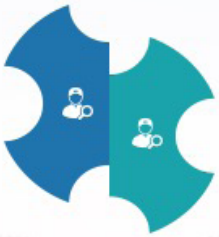
ZHONG LUN 中倫律師事務所

Current Challenges in SCC for CBDT

■ Key Factors Affecting the SCC Recording

External Challenges in Executing SCC

Enterprises encounter two primary challenges when sharing personal information with third-party foreign recipients during CBDT. First, these foreign recipients frequently exhibit reluctance in adhering to China's CBDT compliance requirements after agreements have been made. Secondly, they often show hesitation or even resistance to negotiating SCCs, casting doubts on the need to comply with Chinese data export regulations.



Misunderstanding SCC as Simple Filing

SCCs represent more than just routine administrative filings. Enterprises are not only required to supplement and sign the SCCs provided by the CAC, but they must also undertake an exhaustive Personal Information Assessment (PIA). This entails assessing the necessity, legality, and legitimacy of data transfers. Furthermore, they must scrutinize data lifecycle management, ensure robust security protocols, obtain the necessary consents, and implement policies in line with outbound PIA guidelines. Submissions that do not satisfy these comprehensive criteria are liable to be rejected.

8

ZHONG LUN 中倫律師事務所

Solutions- For Security Assessment & SCC

1. **Evaluating Business Necessity for CBDT: A Strategic Approach**

Enterprises should undertake a thorough analysis of business operations CBDT. The goal is to ascertain the necessity of CBDT in each business scenario and to prioritize them based on the robustness of their justifications. For less compelling cases, a localization plan ('Plan B') should be developed in advance. Particularly for the Security Assessment, our experience indicates that MNCs are more likely to get approval for CBDT from the CAC in the context of global HR management Scenarios (now the global HR management scenarios may be exempted under the new draft regulations promoting data flow).

2. **Evaluating Necessity during CBDT for All Data Fields**

For example, in the case of global HR management MNCs, certain data fields—such as the addresses of employees' registered domiciles or their past working experience involving CCP, political nature, military nature, or other confidential post—are typically restricted from cross-border transfer.

3. **Staying in Alignment with CAC Guidelines on CBDT**

Companies should rigorously comply with CAC guidelines (both security assessment guidelines and the SCC guidelines) to prevent unnecessary bulk data exports. For scenarios or data fields lacking sufficient justification for export, companies should implement effective localized corrective measures. Additionally, companies should supply valid supporting documentation and maintain close communication with regulators to stay updated on the latest requirements, avoiding superficial compliance efforts.

ZHONG LUN 中倫律師事務所

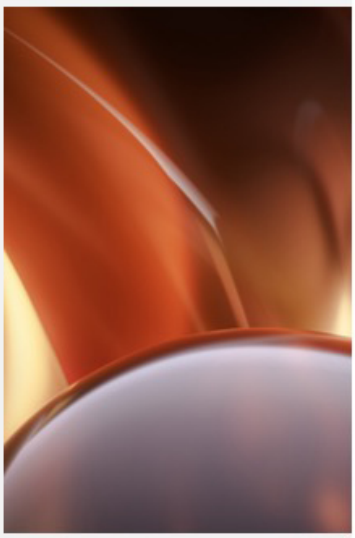


TABLE OF CONTENT

ZHONG LUN 中倫律師事務所

Changes and Consistency for CBDT under the New Draft Regulation

■ **Exemption Mechanism under the Cross-borderData Flow Regulations (Draft for Comments) :**

Companies that meet one of the following criteria will be exempt from security assessments, SCC and certification procedures during CBDT

① Less than 10,000 individuals' PI is transferred abroad within 1 year

② PI transferred abroad is not generated within the Chinese Mainland

③ necessary for the conclusion and performance of a contract to which individual is a contracting party.
cross-border shopping, remittance, air ticket and hotel booking, visa application, etc.

④ Transferring employee's PI abroad is required for HR management under legally-established labor rules and signed collective contracts.

⑤ exempts data transfers in emergencies from need to be filed, including the need to safeguard a natural person's life, health, or property.

⑥ Data excluded from the negative list formulated by the Free Trade Experimental Zone.
The power has been decentralized.

ZHONG LUN 中倫律師事務所

Changes and Consistency for CBDT under the New Draft Regulation

■ **More Streamlined and Straightforward Triggering Condition under the New Draft Regulation**

① Transferring personal information of more than one million people abroad;
② Data to be CBDT'd is informed or cataloged by the supervisory department or regional department as **Key Data**.

CBDT now falls under the security assessment

CBDT now falls under the SCC or certification procedures

It is estimated to provide more than 10,000 people but less than 1 million people's personal information is transferred within 1 year.

12

ZHONG LUN 中倫律師事務所

Key Data Remains to Be Further Clarified

Several Provisions on Automotive Data Security Management (for Trial Implementation)

Key Data

is defined as any data that may endanger China's national security, economic operation, social stability, public health or public security, if it is tampered with, destroyed, leaked, or illegally acquired or used.

➢ **Key Data Scope (Objective Qualification)**

- (I) geographic information, passenger flow, vehicle flow and other data of important sensitive areas such as military administrative zones, entities of science, technology and industry for national defense, and Party and government organs at the county level or above;
- (II) ***data reflecting economic operation such as vehicle flow, logistics, etc.***;
- (III) operational data of the automobile ***charging network***;
- (IV) ***video and image data outside the vehicles that contain face information, license plate information, etc.***;
- (V) the personal information of ***more than 100,000 persons*** as the subjects of personal information is involved; and
- (VI) other data.

13

ZHONG LUN 中倫律師事務所

Key Data Remains to Be Further Clarified

How to identify key data?

Key Data Follows the Regulator's Beats

The identification of key data is based on notification or public release by relevant departments or regions. If data has not been notified as important or is not included in the publicly released list of important data, the export of such data does not require a security assessment.

the catalogues and scopes of key data in some industries is on the way.

Waiting for guidance from the relevant competent departments ?

instead of wait and see, Companies is supposed to communicate with the relevant competent authority to confirm whether their data processing belongs to key data before starting to carry out cross-border data transmission.

14

ZHONG LUN 中倫律師事務所

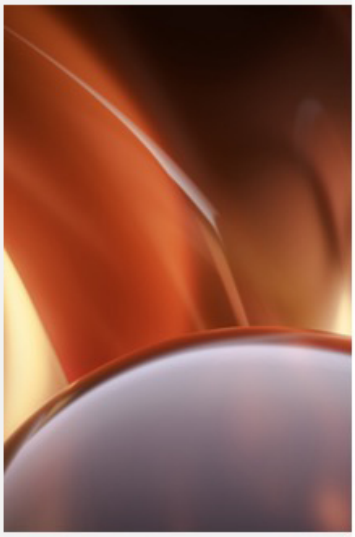


TABLE OF CONTENT

ZHONG LUN 中倫律師事務所

Compliance Obligation

- The New Draft Regulation is still in Draft shape

At present, the CBDT new regulation is still in the stage for public comments, waiting to be finalized.

Companies should not "race ahead" based on the draft version right now. Especially for companies who has already undergo the security assessment, and their data did not pass the security assessments but will be exempted by the CBDT new regulation, since these data have already been "registered" by the CAC, it is inappropriate to react now absent the finalized regulations.

Companies are encouraged to closely monitor the progress of the finalization of the CBDT new regulations, and then evaluate which compliance mechanism they should use for CBDT

16

ZHONG LUN 中倫律師事務所

Compliance Obligation

- **Special Case: About sensitive information involving the CCP, political nature, military nature, or other confidential post**

Transferring sensitive information involving the CCP, political nature, military nature, or other confidential post abroad shall be carried out in accordance with relevant laws, administrative regulations, and departmental rules.

For example: the personal information of medical personnel from military background may constitute the "sensitive information", and it should be processed with caution.

Companies should actively identify such sensitive information. To ensure compliant CBDT, we recommend to localized such information without any CBDT actions

ZHONG LUN 中倫律師事務所

Compliance Obligation

- **Other compliance obligations**

1. **Fulfilling the obligation of notification**
   - Before transferring personal information abroad, personal information processor shall fulfill the obligation of notification in accordance with the PIPL.
2. **Conducting personal information protection impact assessment**
   - Before transferring personal information overseas, personal information processors shall conduct personal information protection impact assessment, and record the processing information in accordance with the PIPL.
3. **Ensuring the level of protection of personal information of overseas recipient**
   - The personal information processor shall take necessary measures to ensure that personal information processing activities of the overseas recipient meet the personal information protection standards provided in PIPL.
4. **Establishing a data security emergency response mechanism**
   - It is recommended that companies formulate local measures according to the requirements of Chinese regulatory agencies to effectively conduct internal supervision and risk remediation of data processing activities.

ZHONG LUN 中倫律師事務所

To do list

Due diligence

Review specific business scenarios and find out the exact data fields leaving the country.

Compliance analysis

Based on the full-scale DD, assess and analyze whether the company needs to carry out a security assessment or fulfill the SCC recordation obligations, and the existing compliance gap.

Compliance rectification

Complete compliance rectification (including necessary policies, consent forms, etc.)

An "exemption" opinion should be issued and validated by experienced professionals.

19

ZHONG LUN 中倫律師事務所

——LEGAL SOLUTIONS FOR CHINA BUSSINESS——

Thank You for Your Time !

Peng Cai (Zhong Lun Law Firm, EP.)
E-mail: **caipeng@zhonglun.com**
DL: +86 010 5087 2786 Tel: +86 138 0135 2664

Data & E-commerce Lab

严格保密

中倫律師事務所 ZHONG LUN LAW FIRM

The 12th

Asia Privacy Bridge Forum 2023

Eunjung Han

Attorney, ROUSE, Vietnam

ROUSE

Personal Data Protection Decree 2023: Navigating Vietnam's Cross-Border Data Transfer Landscape

12 October 2023

Eunjung Han – Attorney, Rouse Legal Vietnam
eunjunghan@rouse.com

Agenda

- *Personal Data is hereafter referred as PD*
- *Personal Data Protection Decree is hereafter referred as the PDP Decree*

ROUSE

Rouse – a leading global IP firm providing full range of IP Service

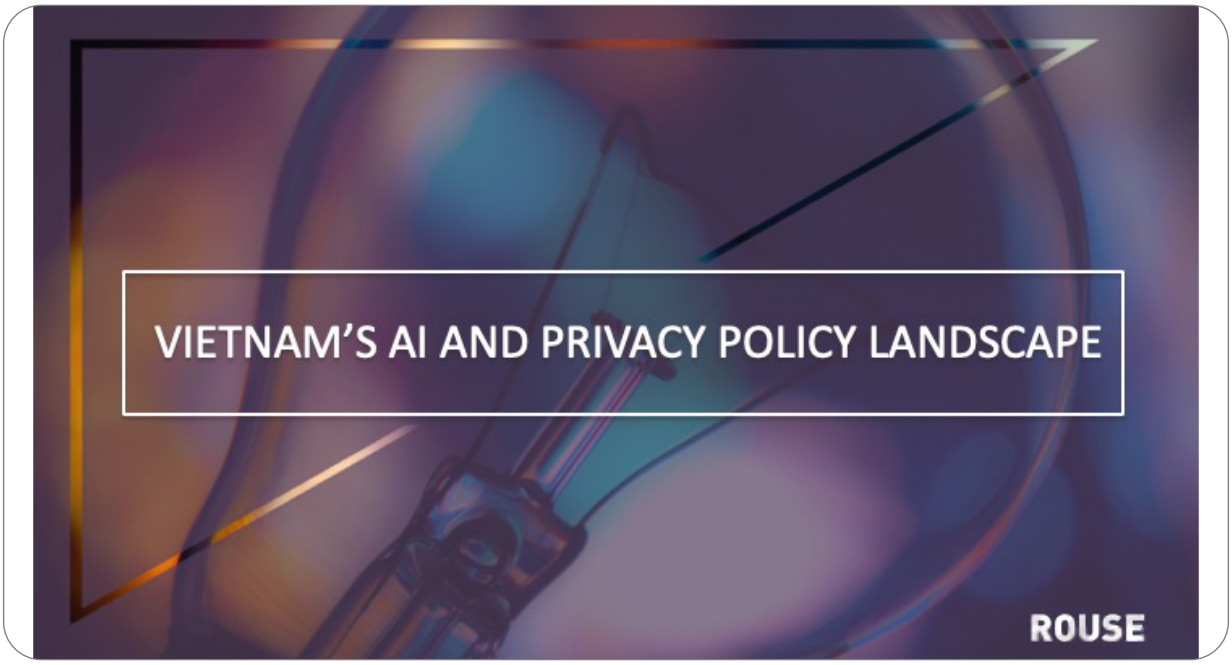
YEARS	JURISDICTIONS	OFFICES	PEOPLE	ASIA PACIFIC & UNITED ARAB EMIRATES
33	13	20	750+	BAND 1

"Rouse is an undisputed leader when it comes to pan-Asian IP practice as well as a top global consultancy."
- WTR1000, 2021

Rouse in Vietnam

- We have been present in Vietnam since 1993 and opened our first office in 1997. We now have offices in Ho Chi Minh City and Hanoi, and can provide IP services in Cambodia and Laos as well as Vietnam itself.
- Our legal services are provided by a local branch of our UK law firm Rouse Legal.
- In Vietnam Rouse is ranked as a Tier 1 in Trade Mark and Copyright & related rights by IP Stars (2018-2022) and Tier 1 in Trade Mark Contentious and Copyright by AsiaIP (2020-2022).
- We also advise top multinational companies on data protection, cross-border data transfer, highly technical data processing, and cybersecurity/cybercrime legal risk assessment.

ROUSE



Vietnam's digital potential in numbers

- Vietnam's population is close to 100 million.
- Vietnam boasts a high internet penetration rate of 79,1%, with over 77.93 million users as of January 2023.
- In early 2023, there were 161.6 million active mobile connections in Vietnam, equivalent to 164% of the total population..
- Over 2/3 of Vietnamese's PD is being collected and shared online in 2022.
- Vietnam has been among the top 10 countries with the most cross-border data flow in the last decade.
- In 2022, Vietnam ranked 6th out of 10 ASEAN members and 55th globally in the Government AI Readiness Index, surpassing the global average and jumping 7 places compared to the previous year.
- Vietnam holds the second position in SEA for the number of AI patents obtained.

→ **Vietnam is keen on developing on effective PD protection**

ROUSE

Vietnam's AI policies

The National AI Strategy by 2030

- **Aims and Goals**:
  - Make Vietnam a leading country in AI development, research, and application;
  - Develop reputable AI brands; and adopt AI in online public services; etc.
- **Implementation:** 17 Ministries are tasked with developing legal instruments on AI, including those in the fields of data protection, intellectual property, e-transactions, etc.

The National Digital Transformation Programme by 2025, with an orientation to 2030

- **Focus:** Prioritize AI research and development as a key aspect of digital transformation.

Ho Chi Minh City AI Application Plan (2020-2030) - 2023 Update

- **Initiative**: Launch a project to build computing infrastructure based on research from HCMC National University by Q4 2023.
- **Objective**: Support the AI research and application ecosystem in Ho Chi Minh City.

ROUSE

International impacts on establishing a framework on cross-border data transfer

- In APEC Leaders' Summit (November 2022), APEC Leaders endorsed a declaration committing to "cooperate on facilitating the flow of data, and strengthening business and consumer trust."
- In late 2022, the US launched discussions with Vietnam and some other Asian allies on "open trade commitments", including "trusted and secure cross-border data flows".
- The Dubai International Financial Centre's Index 2022 treats as "high risk" data transfers to Vietnam.

→ Vietnam needs a legal framework that support a cross-border digital environment that is both open and secure.

ROUSE

Vietnam's privacy laws: before and now

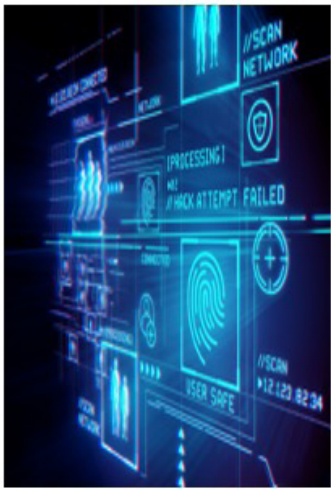
Before

- No consolidated privacy law in place; regulations scattered across different legal documents.
- No separate set of rules on cross-border transfer; consent is the only requirement

Now

PDP Decree (issued on 17 April 2023, effective from 1 July 2023) – Vietnam's 1st comprehensive legal instrument on PD:

- Includes specific requirements for cross-border transfer;
- Applies to –
  - onshore and offshore Vietnamese entities and individuals;
  - foreign entities and individuals
    - based in Vietnam; or
    - directly participating in or involved in the PD processing in Vietnam.



ROUSE

PDP Decree's key concepts

- PD **Processing** is defined broadly. It essentially means anything that is done to/with PD.
- **PD**: Information expressed in the form of symbols, text, numbers, images, sounds, or equivalences , that is associated with an individual or helps to identify an individual, including –
  - Basic PD, and
  - Sensitive PD → processing of which requires (i) notifying data subjects of such processing; and (i) DPO/DPD appointment + update to A05.*
- Regulated parties:
  - **Controller** - deciding on the PD processing's purposes and means.
  - **Processor** – processing PD on behalf of Controller via a contract.
  - **Controller-cum-processor** – deciding on the PD processing's purposes and means + directly performing the processing.
  - **Third parties** – other than the above, authorized to process PD.

**A05: Department of Cybersecurity and Hi-tech Crime Prevention under the Ministry of Public Security (MPS)*

Article 24.1(b), PDP Decree implies that Controllers and Controlling and Processing Entities must appoint DPO/DPD in all cases.

ROUSE

Basis for PD processing

Consent

Emergency
To protect data subject's life or health

Public disclosure
in accordance with the law

Competent state agencies' processing

Serving State agencies' operations
in accordance with sector-specific law

PD recorded in public places
by competent authorities

Data subject's contractual obligations

Potential grounds for Government's access to PD held by private entities

ROUSE

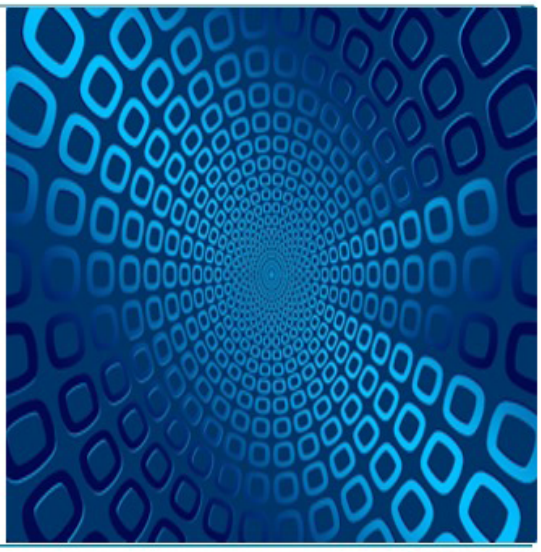
Data Processing Impact Assessment (DPIA)

DPIA is required for both onshore and offshore PD processing.

DPIA must be prepared in Vietnamese, submitted to A05 and maintained by assessing parties, including –

- PD Controller and Controller and processor in all cases, from the PD processing's commencement, and
- PD Processor, under its agreement with the PD Controller.

DPIA's contents under the PDP Decree include the assessing party's contact details, potential and unwanted consequences and/or damage, etc.

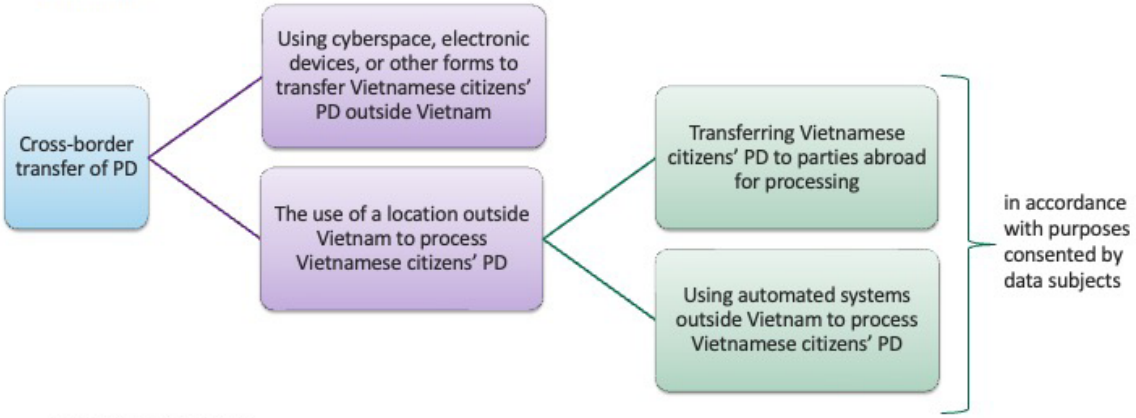


13

ROUSE

Cross-border transfer of PD under the PDP Decree

Definition



Article 2.14, PDP Decree

ROUSE

Cross-border transfer of PD under the PDP Decree

Requirements for Cross-border transfers of personal data

Previous Legislation	PDP Decree + Draft Sanction Decree
• No separate rules on cross-border transfer	• Data subject's consent;
• Consent is the only requirement, unless they are made under other legal obligations (e.g., court orders)	• Prepare a dossier for assessing the impact of the cross-border transfer of PD (**"CTIA"**) + always keep it available for the MPS' inspection and evaluation
• PD transfer involving state secrets (very rare currently) is restricted and must be approved by the Government	• Upon successful transfer, notify A05 in writing.
Sanction for non-compliance: Up to VND 70 million (approx. US$2,897)	Proposed sanction for non-compliance: Up to VND 200 million (approx. US$8,278) and an up-to-3-month PD processing suspension + other sanctions and remedies.

ROUSE

Cross-border transfer of PD under the PDP Decree

CTIA – what's needed

- **Contact details** of the Transferor and the recipient; and the Transferor's organization/individuals responsible for the transfer
- Description and explanation of the **PD processing's objectives** after the transfer
- Detailed description of the **transfer's compliance** with the PDP Decree and **measures applied** for PD protection
- **Assessment** on the PD processing; potential and unwanted **consequences and/or damage**
- The data subject's **valid consent** when he/she is informed of the feedback and complaint mechanism in case any problem or request arises and measures to mitigate/eliminate such risks
- Document(s) showing the Transferor and the recipient's **responsibilities** for the PD processing (e.g., data transfer agreement)

ROUSE

CTIA Submission Procedure

Transferor → A05
- 01 original copy of the CTIA, and
- a notification

Timeline: within **60 days** from the date of PD transfer.

A05
- evaluate the submission;
- if the submission doesn't meet the required criteria → request for the Transferor's revision.

Successful Transfer
- Transferor to notify A05 information about that transfer and contact details of the party in charge thereof

A05's request for revision
- Transferor must revise CTIA

Any change to the CTIA
- Transferor to update A05

A05's receipt time: Working hours from Monday to Friday (excluding national holidays) **Timeline for Processing:** 10 working days

ROUSE

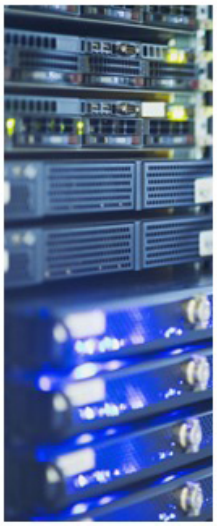
Cross-border PD Trading – Is it allowed under PDP Decree?

- The purchase or sale of PD (whether it is cross-border or domestic) is **prohibited** in any form, unless otherwise provided by law.
- Software system installation, implementation of technical measures or organization of collection, transfer, purchase or sale of PD without the data subject's consent is a **violation** of law.
- MPS's verbal clarification: "***only the law can regulate the cases in which PD trading is permitted.***"

ROUSE

Data Localisation Requirement under Decree 53

Regulating Instrument	• Decree 53/30222/ND-CP guiding the Cybersecurity law
Types of data subject to localisation ("Regulated Data")	• PD of service users in Vietnam • User-generated data in Vietnam • Data on the relationship of service users in Vietnam
Types of business subject to data localisation	• All domestic entities, including foreign invested ones. • Foreign entities (any entity established under a foreign law) – only when certain triggering events occur.
Proposed Sanctions under the Draft Sanction Decree	• Up to VND 200 million (~ US$ 8,552) • Additional sanctions and remedial measures to be imposed



ROUSE

The TEST

When do offshore enterprises have to comply with data localisation and local office requirements?

Entity operates in Regulated Services (10 services)?

Yes

Entity

- failed to comply or inadequately complied to written notification by A05? *or*
- resisted, obstructed, or disabled cybersecurity measures applied by specialised task force?

Yes

Minister of Public Security

➢ decision requesting local storage and local office establishment

A05

➢ notify, provide instructions, monitor, and makes sure entity localise data and set up a branch or representative office in Vietnam;

➢ notify relevant agencies

Entity must comply within **12 months**

No

No localisation required

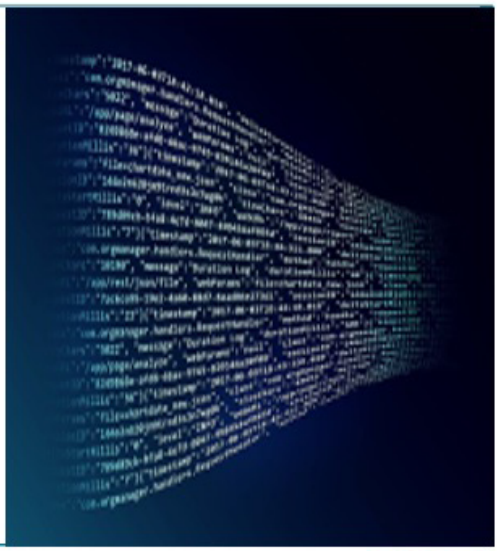
No

21

ROUSE

Data localisation - its relation to the PDP Decree

- The PDP Decree has no provision on data localisation.
- Neither the PDP Decree nor Decree 53 prohibits the cross-border PD transfer subject to the localisation requirement.



22

ROUSE

Compliance roadmap for cross-border PD transfer

Prepare a compliance checklist based on your operation

- ✓ Identify yourself if you are a controller/processor/controller-cum-processor/third party.
- ✓ Identify the current legal basis for PD processing.

General Compliance Checklist

Personnel	Technical	Administrative	
• Appoint a data protection officer/ department (DPO/DPD).	• Apply appropriate technical measures (e.g., encryption, software updates, etc.).	• Adopt mechanisms for collecting valid consent.	• Prepare and submit to A05 (i) a DTIA; and (ii) a CTIA.
• Appoint responsible personnel for cross-border transfer of PD (can be the DPO).		• Prepare: (i) privacy policy/notice informing the data subjects of the PD processing; (ii) internal privacy policy; (ii) contract template for processing between controller and processor.	• Notify A05 in writing of data transfer information and contact details of in-charge individuals and/or organizations after completing cross-border transfers.
• Conduct training for staff.			

ROUSE

POTENTIAL ENFORCEMENT LANDSCAPE AND ENFORCEMENT PRACTICES

ROUSE

Recent developments and what to expect

PDP Decree

- MPS issued templates for compliance.
- No published records on implementation/enforcement practice.
- The launch of National PDP Portal is still pending.

Draft Decree on Sanctions against Administrative Violations in Cybersecurity (Draft Sanction Decree)

- The draft has been pending since 31 May 2023 until now.
- Will provide legal grounds to tackle violations against PD protection and cybersecurity regulations via administrative measures.

PD Protection Law

- To be developed by the MPS and the Ministry of Justice.

ROUSE

Draft Sanction Decree – Notable issues

- **Regulatory Scope:**
  - **Extra-territorial application scope:** Proposed to be applicable to both onshore and offshore entities.
  - **Regulate administrative sanctions related to five main areas**:
    (i) information security;
    (ii) PD protection;
    (iii) cyberattack prevention;
    (iv) implementation of cybersecurity protection activities;
    (v) prevention and protection against using cyberspace, information technology and electronic devices to violate the law on social order and safety.
- **Types of Administrative Sanctions:** Monetary fine (main sanctions) + other sanctions and remedies (e.g., suspension of PD processing, operations, business licenses).
- **Tentative Effective Date**: 1 December 2023.

ROUSE

Increased Focus on Cybersecurity and Data Protection

The MPS' report of cybersecurity situation

- High risk of information insecurity, especially at the State's central agencies and Vietnam's large economic corporations.
- Attack, infiltration, and appropriation of state secret information and documents.
- High-tech crimes committed on online platforms, social networks, applications, etc.
- On-going illegal exchange and transaction of personal data.

ROUSE

The 12th

Asia Privacy Bridge Forum 2023

Byungnam Lee

Senior Advisor, Kim&Chang, Korea

KIM & CHANG

Chronology of Korean Laws and Regulations Governing the Cross-border Transfer of Data

KIM & CHANG

Table of Contents

I. Reasons for Amending the PIPA

KIM & CHANG

I. Reasons for Amending the PIPA

Background of Amendment It is essential to revise applicable laws and systems to ensure the safe and secure use of data when the country is transitioning into the digital era

▶ The data industry is growing exponentially year on year driven by the emergence of global service providers and the cross-border transfer of data.

In 2022,
the size of the global data industry reached **approx. KRW 660 trillion**

(2022 Data Industry Trends Paper by the Korea Data Agency)

▶ Countries worldwide are realigning their laws and systems to increase support for data use and to manage personal data in a safe and secure manner.

U.S.
Started to discuss privacy bills at the federal level, and newly organized the Division of Privacy and Identity Protection under the FTC's Bureau of Consumer Protection (2021)

Japan
Integrated the supervisory functions divided between the public (i.e., Ministry of Internal Affairs and Communications) and private sectors (i.e., Japanese Personal Information Protection Committee) (2021), following the launch of the Japanese Personal Information Protection Committee (2016)

EU
Enacted the General Data Protection Regulation (GDPR) that came into effect in 2018, and strengthened the cooperation system between the European Data Protection Board (EDPB) and the supervisory agencies of the member states

4

KIM & CHANG

I. Reasons for Amending the PIPA

Current Status

The need for cross-border transfer of personal data keeps increasing due to the expansion of borderless commercial transactions online.

In the EU, personal data can be transferred overseas through various means, such as by obtaining consent from data subjects. However, the existing laws of Korea require consent to be obtained from data subjects in order to transfer personal data overseas.

EU

In addition to obtaining consent from data subjects, the EU has various requirements for allowing cross-border transfer of personal data, such as *(i)* adequacy decision, *(ii)* standard contractual clauses (SCC), *(iii)* binding corporate rules (BCR), *(iv)* certifications, and *(v)* codes of conduct.

(When having trade negotiations, the EU has continued to request the Korean government to revise Korean laws and regulations in this respect.)

Adequacy Decisions by the EU and the UK

As a result of the adequacy decisions by the EU (December 17, 2021) and the UK (December 19, 2022) on the Korean PIPA, Korea is acknowledged as a country with an adequate level of protection for personal data that is equivalent to the level of protection within the advanced countries. These decisions have also helped reducing legal risks of companies and their time and cost burdens.

* Korean companies may transfer the EU and UK citizens' personal data to Korea without going through an additional procedure to obtain consent from data subjects (as for the EU, such data includes public data).

5

KIM & CHANG

I. Reasons for Amending the PIPA

Amendment Direction Increase the interoperability with international regulations on personal data, and prepare safeguards

▶ **(Diversification of Requirements for Cross-border Transfer)** Diversify the cross-border transfer requirements beyond the requirement of "obtaining additional consent from data subjects"

※ Provisions Stipulating the Requirements for Cross-border Transfer of Personal Data (Article 28-8 (1) of the PIPA)

(i) Where additional consent has been obtained from the data subject; ***(ii)*** where any law or treaty has a provision concerning cross-border transfer of personal data; ***(iii)*** where the matters required to be notified by law are disclosed in the privacy policy or informed to the data subject in order to outsource the processing of, or store, personal data necessary for the execution and performance of a contract with the data subject; ***(iv)*** where the person to whom personal data is to be transferred, has obtained the certification determined and notified by the Personal Information Protection Committee ("**PIPC**"); or ***(v)*** where the PIPC acknowledges that the level of personal data protection by the country or international organization to which personal data is transferred, is equivalent to the level of protection under the PIPA.

▶ **(Order to Stop Cross-border Transfer of Personal Data)** Prepare regulatory safeguards to manage personal data in a safe and secure manner by introducing stop-transfer order against cross-border transfer of personal data causing damage to Korean citizens

6

II. Developments & Summary of the Amendments to Data Laws and the Enactment of Notifications

II. Developments & Summary of the Amendments to Data Laws and the Enactment of Notifications

KIM & CHANG

Progress of Amending Data Laws & Enacting Notifications

II. Developments & Summary of the Amendments to Data Laws and the Enactment of Notifications

KIM & CHANG

Amended Provisions on Cross-border Transfer of Personal Data

Classification		Before Amendment		After Amendment
Cross-border Transfer of Personal Data	Scope of Application	Personal information controller (Article 17 (3) of the PIPA)	Information and communications service provider, etc. (Article 39-12 of the PIPA)	Personal information controller (Article 28-8 of the PIPA) encompassing both online and offline channels
	Requirements	• Obtain consent from the data subject in order to provide personal data to a third party overseas	• Obtain consent from the data subject in order to transfer* personal data overseas * also meaning provision (including inquiry), outsourcing of the processing, and storing • When outsourcing the processing of, or storing, personal information, the data subject's consent is deemed to have been obtained if the relevant matters are disclosed in the privacy policy.	• Obtain additional consent from the data subject in order to transfer* personal data overseas * also meaning provision (including inquiry), outsourcing of the processing, and storing • Where the relevant matters are disclosed in the privacy policy in order to outsource the processing of, or store, personal data necessary for the execution and performance of a contract with the data subject • Where the person to whom personal data is to be transferred, has obtained the certification determined and notified by the PIPC • Where the PIPC acknowledges the adequacy of the level of personal data protection by the country or international organization to which personal data is transferred
Order to Stop Cross-border Transfer of Personal Data Newly Inserted	Scope of Application			Personal information controller (Article 28-9)
	Requirements			• Where the personal information controller is in violation of the provisions concerning cross-border transfer • Where any damage is caused, or highly likely to be caused, to the data subject

9

III. Requirements for Cross-border Transfer of Personal Data

KIM & CHANG

III. Requirements for Cross-border Transfer of Personal Data

1. Where "additional" consent has been obtained from the data subject (Article 28-8 (1) 1 of the PIPA)

- When transferring personal data overseas, the data subject is allowed to exercise his/her rights, such as by refusing the cross-border transfer after being aware of the likelihood that the level of personal data protection by the person, country or international organization to which personal data is transferred, may not be equivalent to the level of protection in Korea.
- It is stipulated that additional consent must be obtained from the data subject in order to transfer personal data overseas, in addition to his/her consent required by Articles 15 (collection and use of personal data) and 17 (provision of personal data) of the PIPA.

KIM & CHANG

III. Requirements for Cross-border Transfer of Personal Data

2. Where outsourcing of the processing of, or storing, personal data is necessary for the execution and performance of a contract with the data subject (Article 28-8 (1) 3 of the PIPA)

- When it is necessary to outsource the processing of, or store, personal data for the execution and performance of a contract with the data subject, personal data may be transferred overseas without the data subject's consent if the matters required to be notified by law are disclosed in the privacy policy or informed to the data subject by email, etc.

※ **(Before Amendment)** (Before Amendment) Article 39-12 (2)
Personal data may be transferred overseas without the data subject's consent if the relevant matters are disclosed in the privacy policy or informed to the data subject by email, etc. in order to outsource the processing of, or store, personal data.

KIM & CHANG

III. Requirements for Cross-border Transfer of Personal Data

3. Where certification has been obtained for cross-border transfer of personal data (Article 28-8 (1) 4 of the PIPA)

▶ Personal data may be transferred overseas if the person to whom personal data is to be transferred, **has obtained the certification determined and notified by the PIPC**, such as the certification of personal information protection under Article 32-2 of the PIPA.

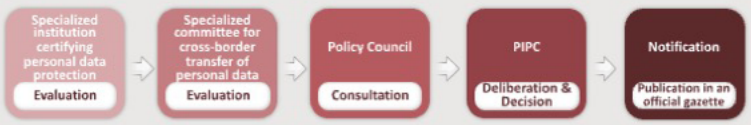
In that case, the following measures must be taken:

- Safeguards necessary for the protection of personal data, and measures to guarantee the data subject's rights; and
- Measures necessary for implementing the certified matters in the country to which personal data is transferred.

KIM & CHANG

III. Requirements for Cross-border Transfer of Personal Data

4. Certification process for cross-border transfer of personal data (Article 28-8 (1) 4 of the PIPA)



- **Certifications are determined and notified by the PIPC**, such as the certification of personal information protection under Article 32-2 of the PIPA.
- The evaluation criteria are informed through the Notification of the "Regulation on Cross-border Transfer and Management of Personal Information."
- **Certification may not be granted if the level of personal data protection falls below the required level.**

KIM & CHANG

III. Requirements for Cross-border Transfer of Personal Data

5. Where the PIPC acknowledges that the level of personal data protection by the country, etc. to which personal data is transferred, is equivalent to the required level (Article 28-8 (1) 5 of the PIPA)

▶ **Where the PIPC acknowledges that the level of personal data protection by the country or international organization to which personal data is transferred, is equivalent to the level of protection under the PIPA.**

- The level of protection is acknowledged by comprehensively taking into account *(i)* the personal data protection system, *(ii)* the scope of guaranteeing the data subject's rights, and *(iii)* the procedures for damage relief.

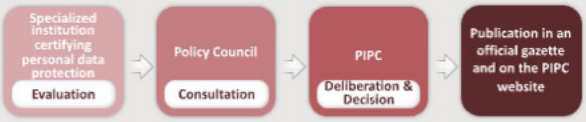
※ **Matters to be considered to acknowledge the level of personal data protection by the country, etc. to which personal data is transferred (Article 29-9 (1) of the Enforcement Decree of the PIPA)**

(i) Whether the personal data protection system, including laws and regulations, is in line with the principle of personal data protection and guarantees the rights of data subjects; ***(ii)*** whether there is any independent supervisory institution; ***(iii)*** whether public institutions process personal data in accordance with applicable laws and regulations, and whether there are protection measures that are guaranteed for data subjects; ***(iv)*** whether there are damage relief procedures for data subjects, and whether such procedures work effectively; ***(v)*** whether the supervisory institution can smoothly cooperate with the PIPC; and ***(vi)*** any other matters notified by the PIPC in order to acknowledge the level of personal data protection

KIM & CHANG

III. Requirements for Cross-border Transfer of Personal Data

6. Certification process for cross-border transfer of personal data (Article 28-8 (1) 5 of the PIPA)



- The scope of personal information controller to whom personal data is transferred, the period during which the level of personal data protection is acknowledged, and the requirements for cross-border transfer can be set differently for each country (or international organization).
- When acknowledging, or revoking or changing its acknowledgement of, the level of personal data protection by the country, etc. to which personal data is transferred, the PIPC should publish such facts in an official gazette and on its website.
- **When there is any change in the level of personal data protection, the PIPC may revoke or change its acknowledgment thereof based on the opinion of the relevant country (or international organization).**

IV. Order to Stop Cross-border Transfer of Personal Data

KIM & CHANG

IV. Order to Stop Cross-border Transfer of Personal Data

Order to Stop Cross-border Transfer of Personal Data (Article 29-9 of the PIPA)

- Newly introduced a system whereby an order can be issued to stop the cross-border transfer of personal data *(i)* when the personal information controller is in violation of the **provisions concerning cross-border transfer***, or *(ii)* **when any damage is caused, or highly likely to be caused, to the data subject** due to inappropriate protection of personal data

*** Violation of the provisions concerning cross-border transfer (i.e., Article 28-8, Paragraphs (1), (4) and (5))**

- **Paragraph 1** The requirements for cross-border transfer must be satisfied (i.e., *(i)* where additional consent has been obtained from the data subject; *(ii)* where any law or treaty has a provision concerning cross-border transfer of personal data; *(iii)* where the matters required to be notified by law are disclosed in the privacy policy or informed to the data subject in order to outsource the processing of, or store, personal data necessary for the execution and performance of a contract with the data subject; *(iv)* where the person to whom personal data is to be transferred, has obtained the certification determined and notified by the PIPC; or *(v)* where the PIPC acknowledges that the level of personal data protection by the country or international organization to which personal data is transferred, is equivalent to the level of protection under the PIPA).
- **Paragraph 4** In the event of cross-border transfer, the following Articles of the PIPA must be complied with, along with the protection measures prescribed by Presidential Decree: **Article 17** (Provision of Personal Information), **Article 18** (Out-of-Purpose Use of Personal Information), **Article 19** (Limitation to Use and Provision of Personal Information on Part of Its Recipients), and **Chapter V** (Guarantee of Rights of Data Subjects).
- **Paragraph 5** It is prohibited to execute any cross-border transfer contract that contains provisions in violation of the PIPA.

KIM & CHANG

IV. Order to Stop Cross-border Transfer of Personal Data

Process of issuing an order to stop cross-border transfer of personal data & Matters requiring consideration

Specialized committee for cross-border transfer of personal data — Evaluation → PIPC — Deliberation & Decision

- A stop-transfer order should be issued after taking into account various factors, including whether the provisions concerning cross-border transfer is violated.

※ **Matters requiring consideration before issuing an order to stop cross-border transfer (Article 29-11 (1) of the Enforcement Decree of the PIPA)**

(i) The type and scale of personal data to be transferred overseas; ***(ii)*** the severity of violation of laws concerning cross-border transfer; ***(iii)*** whether the damage caused, or likely to be caused, to data subjects is significant or irreparable damage; ***(iv)*** whether issuing an order to stop cross-border transfer is clearly beneficial to data subjects rather than not issuing such order; ***(v)*** whether a corrective order can protect and prevent breaches of personal data; ***(vi)*** whether effective measures are in place to provide damage relief to data subjects; and ***(vii)*** whether there are circumstances where appropriate protection of personal data is acknowledged to be difficult due to a material breach of personal data, etc.

- **When receiving a stop-transfer order, the personal information controller may raise an objection within seven days** from the date of receiving the order.
- The PIPC notifies the personal information controller of its review results within 30 days from the date of receiving the objection.
- **The stop-transfer order remains in effect even after an objection is raised** to the order.

19

Thank You

KIM & CHANG
서울특별시 종로구 사직로8길 39
(우)03170
T 02 3703 1114
F 02 737 9091/9092
www.kimchang.com
lawkim@kimchang.com

The 12th

Asia Privacy Bridge Forum 2023

Day 1 Session 3

Session Chair

Sang-Mi Chai
Professor, Ewha Womans University, Korea

1 **Ryumie Hwang**
Senior Manager, Digital Business Dept., KEARNEY

2 **Muhammad Sufyan bin Basri**
Senior Director, Personal Data Protection of Malaysia

3 **Cecilia Siu**
Assistant Privacy Commissioner, PCPD, Hong Kong

The 12th

Asia Privacy Bridge Forum 2023

Ryumie Hwang

Senior Manager, Digital Business Dept., KEARNEY

Generative AI and Security risks

Asia Privacy Bridge Forum 2023
October 12th, 2023

KEARNEY

Presenter

Hwang, Ryumie
Senior Manager
KEARNEY Korea

KEARNEY

KEARNEY Korea, Senior Manager
- Digital Strategy leader in Digital Transformation Group
- Experts in Corporate Strategy, New Business Development, Go-To-Market Strategy, Innovation

HYUNDAI

Hyundai Motor Group
- Hyundai AutoEver America (US): IT Strategy & Planning
- Hyundai Card/Capital (KR): Corporate Strategy & Business Innovation

accenture EY KPMG

ACCENTURE / EY / KPMG
- IT/DT Transformation Consultant
- Experts in IT Strategy, Information Strategy Planning, PMO, Business Process Re-engineering

Source: KEARNEY

KEARNEY has more than 4,200 people strong in 40+ countries, with more than 20,000 people in our alumni network

KEARNEY Global

- Established in 1926 Chicago, USA
- Globally more than 4,200 Consultants
- Performing more than 3,500 projects annually
- Over 90% of renewal contract rate
- Exceed annual growth rate of 26% since 1980

KEARNEY Asia

- First branch established in 1972
- Exceed annual growth rate of 30% since 1980
- 16 Asia Branches

KEARNEY Korea

- Seoul Office established in 1995
- More than 400 Consultants ('22 YE)
- Performing more than 300 projects annually

Americas

Atlanta, Bogotá, Boston, Calgary, Chicago, Dallas, Detroit, Houston, Mexico City, Minneapolis, New York, San Francisco, São Paulo, Toronto, Washington, D.C.

Asia Pacific

Bangalore, Bangkok, Beijing, Brisbane, Hong Kong, Jakarta, Kuala Lumpur, Melbourne, Mumbai, New Delhi, Perth, Seoul, Shanghai, Singapore, Sydney, Tokyo

Europe

Amsterdam, Berlin, Brussels, Bucharest, Copenhagen, Düsseldorf, Lisbon, Ljubljana, London, Madrid, Milan, Moscow, Munich, Oslo, Paris, Prague, Rome, Stockholm, Vienna, Warsaw, Zurich

Middle East and Africa

Abu Dhabi, Doha, Dubai, Istanbul, Johannesburg, Riyadh

Source: KEARNEY

KEARNEY Analytics global team is comprised of 500+ data scientists, analytics experts, and technologists

Advanced analytics and data capabilities

1 Breadth of expertise and experience

Truly global firm

500+ advanced digital and analytics specialists **globally**

>20 years of **successful collaboration** with clients

Success anchors

1. Analytic transformation
2. Applied data science
3. Big data, AI/ML[1]
4. Bespoke analytics solutions

2 Proven track record

Dozens of industries

400+ projects over the past decade

Expertise guiding **top regional** and **global companies** through large-scale transformation

Advanced analytics and data science
Industry expertise
Domain expertise
Value

3 Differentiating capabilities

One of the **largest organically grown analytics teams at a full-service consulting firm**

Data science lab

Modeling — Rapid prototyping

Immediate value

Analytics Impact Index (AII) connecting analytics with business impact

Strategic partnerships

KEARNEY

provide early access to innovative methods and technologies

Underpinned by KEARNEY's proprietary data use case library with

100+ proven examples

1. AI/ML: Artificial Intelligence/Machine Learning

Source: KEARNEY

Table of Contents

Source: KEARNEY

More than just AI: What was once an intelligent model is now a virtual assistant plugging in across operations and engaging with consumers

What AI was before….

Intelligent Learning models that used internal historical data and external public information such as market dynamics and consumer trends to inform future data driven decisions

What Generative AI is now…

Intelligent Learning models paired with **generative new content capabilities** and interactive user interfaces to create a personalized engagement experience

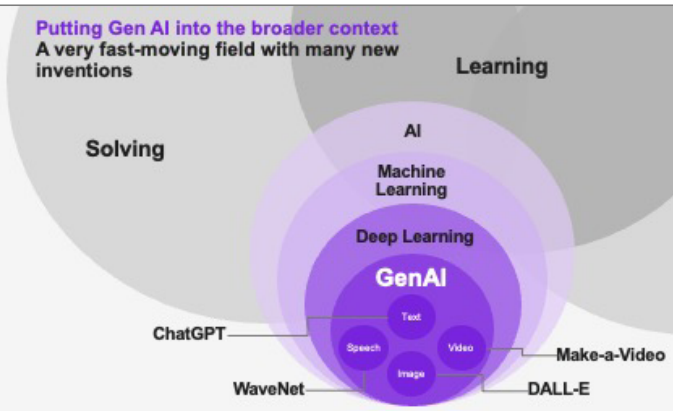
Voice Generation	Text Generation	Media Generation
"Read all my email and draft responses."	"What are current risks to our supply of toilet paper in the US?"	"Which procurement contracts have less than 60 days payment terms?"	"Please generate a campaign strategy and media content for the new launch of our make up brand."

Source: KEARNEY

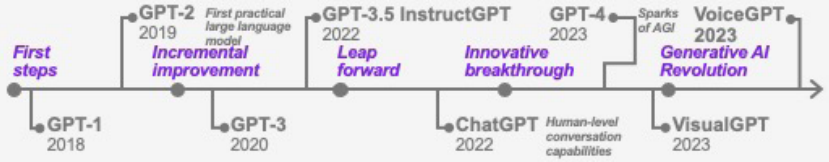
The technology and application landscape of Gen AI is rapidly evolving – companies who can evolve with Gen AI will see significant benefits

Putting Gen AI into the broader context

A very fast-moving field with many new inventions



Rapid Advances in GenAI



Source: KEARNEY

Big Tech and Niche AI companies are continuously rolling out new Gen AI releases

The evolving landscape of Gen AI players with a very rapidly "exploding" landscape of plugin applications;
Open AI rolled out its 70+ plugins to its Plus users

Niche AI companies

Creating foundation AI models

Player	Key AI products (LLMs)
OpenAI	ChatGPT, DALL-E 2, GPT-4, ... and several more
DeepMind	Google Bard
ALEPH ALPHA	Luminous
stability.ai	Stable Diffusion
X.AI	...founded in April 2023 by Elon Musk
cohere, ANTHROPIC, NVIDIA, Synthesis.ai, glean, Jasper	List growing daily…

Source: KEARNEY

Big Tech

Scaling AI through leading infrastructure

Player	Infrastructure / Platform
Microsoft	Azure
Google	Google Cloud
amazon	aws
SAP	SAP AI

3rd parties and plugins

Commercializing AI on provided infrastructure

ChatGPT apps ("plugins")

Extending ChatGPT capabilities beyond training data through connection to external databases and services, e.g., webshops, booking systems, knowledge repositories etc.

OpenTable, instacart, Expedia, WOLFRAM, KAYAK, Klarna.

Generative AI may affect 80% of US workforce for 10% of their tasks

Market Size

$109B

market size for generative AI by **2030** with an expected **CAGR of 35.6%**[1]

Operations

80%

of US **workforce** may have **10%** of their **work tasks affected**, 19% may see ≥ 50% of tasks impacted[2]

Experience

14%

productivity increase in a study conducted with 5K **customer support** agents[3]

Commercial

$112B

retail sales from **AI-powered** chatbot interactions by the **end of 2023**[4]

GAI = Generative Artificial Intelligence, CAGR = Compound annual growth rate
Source: (1) Grand View Research, (2) OpenAI, OpenResearch & University of Pennsylvania, (3) National Bureau of Economic Research, (4) Juniper Research, Luxury CPG player, KEARNEY

Table of Contents

Source: KEARNEY

Application of underlying generative AI technology to optimize work performance in various industries

Non-exhaustive

Gen AI use cases across industries

Starting with automated content generation, generative AI applications will evolve into core business use cases

Aerospace and defense Autonomous systems Quality control Mission Planning	**Automotive** Autonomous vehicles Predictive maintenance Advanced driver systems	**Chemicals** Process optimization Research & development Quality control	**Consumer and retail** Brand messaging Pricing strategy Customer service
Energy Process optimization Safety and compliance Energy management	**Financial services** Fraud detection Risk management Personal financial advice	**Health** Medical research Clinical decision support Medical coding	**Industrial goods and services** Process optimization Quality control Safety and compliance
Infrastructure Project management Smart cities Predictive maintenance	**Media** Advertising Recommendation Sentiment analysis	**Metals and mining** Resource exploration Predictive maintenance Process optimization	**Private equity** Due diligence Portfolio optimization Market research
Public sector Sentiment analysis Chatbots Scenario planning	**Technology** Product development Cyber security Chatbots	**Telecommunication** Network optimization Fraud detection Predictive maintenance	**Transportation and travel** Route optimization Automating dispatching Streamlining logistics

Source: KEARNEY

For example, in the retail industry, Gen AI holds immense promise in personalizing CX, revolutionizing store ops and optimizing productivity to an exceptional degree for retailers

Non-Exhaustive

Consumer Facing	**Awareness**	**Consideration**	**Purchase**	**Loyalty**
	Personalized ads	Gen AI Powered Sales Assistant	Personalized pricing and offers	Personalized reward program
	Customized marketing content	Tailored product descriptions	Cross-selling recommendations	Gen AI Powered Customer Service
	Landing page customization	Interactive product configurators	Visual search product catalogs	Post-purchase appreciation
Company Facing	**Supplier Engagement**	**Warehouse & Distribution**	**Store Operations**	**Sales & Product Portfolio**
	RFP generation, negotiation, & evaluation	Warehouse layout and slotting	Shelf position planning	Market trend analysis and reporting
	Contract intelligence	Route optimization	Store layout optimization	Voice of consumer
	Demand forecasting	Inventory and assortment mgmt.	"Smart" store experience	In-store custom marketing
	Supplier management	Customer delivery and installation	Fraudulent activity detection	Virtual fitting room (try before you buy)
E2E Enablers	**Enablers**			
	Knowledge management	Intelligent coding assistant	Synthetic data for AI/ML models	Smart recruiting
	Meetings & Email assistance	Automated prescriptive reports	Training & Onboarding programs	

Source: KEARNEY

Awareness

Personalized ads

Generate personalized social media content (images, videos) for target consumers

Click rate · Sales uplift

Customized marketing content

1:1 hyper personalized messaging & content catering to diverse demographics

Click rate · Sales uplift

Landing page customization

Generate custom landing pages for certain markets and consumer demographics

Click rate · Sales uplift

Consideration

Gen AI Powered Sales Assistant

Personalized product recommendations and consumer guidance through the purchase process

Customer experience · Conversion rate

Tailored product descriptions

Personalized product description based on user preferences and behavior

Customer experience · Conversion rate

Interactive product configurators

Allows customer to visualize changes to the product based on prompts

Customer experience · Conversion rate

Purchase

Personalized pricing and offers

Generate personalized offers and/ or dynamic pricing based on customer data

Sales uplift · Conversion rate

Cross-selling recommendations

Personalized recommendations on which products can complement current purchase

Cross-Selling · Customer experience

Visual search product catalogs

Searchable product catalogs by inputting video or picture and receiving similar products

Customer experience · Sales uplift

Loyalty

Personalized reward program

Personalized rewards and automated communication based on purchase history and consumer behavior

Brand loyalty · Repeat purchases

Gen AI Powered Customer Service

Chatbot that acts as a personal assistant to solve any post-sale issues

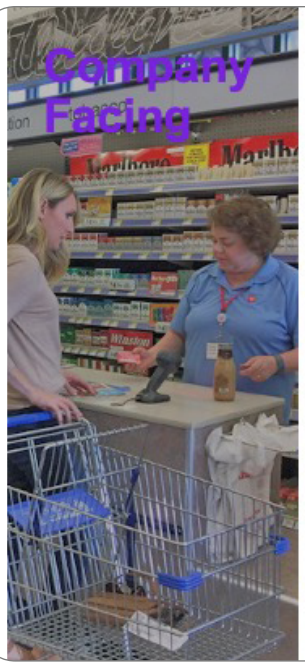
Customer experience

Post-purchase appreciation

Custom thank you notes and automated order confirmation, tracking, and return process based on customer comments

Customer experience · Repeat purchases

Source: KEARNEY



Supplier Engagement

RFP generation, negotiation, & eval.

Create RFPs, and provide real-time negotiation strategies and scenario analyses

Profit margins · Employee productivity

Contract intelligence

Automated contract generation with embedded intelligence to ensure compliance

Compliance rate · Employee productivity

Demand forecasting

Improve forecast accuracy, provide unbiased single source forecasts

OTIF · Carrying costs

Supplier management

Manage relationships, track SLAs & compliance to contracts

Profit margins · Compliance

Source: KEARNEY

Warehouse & Distribution

Warehouse layout/slotting

Optimize warehouse layout and create picking routes to increase warehouse efficiency

OTIF · Carrying costs

Route optimization

Analyze capacity, constraints and real-time information to optimize delivery routes

OTIF · Delivery costs

Inventory/assortment mgmt.

Track inventory and inform assistants of availability and alternatives if out-of-stock

Customer experience · Cross-Selling

Customer delivery and installation

Automated shipment label configurations, and streamlined installation requirement gathering

Customer experience · Repeat purchases

Store Operations

Shelf position planning

Recommends shelf placement by analyzing complimentary products and product popularity

Sales uplift

Store layout optimization

Optimize store layout planning by generating and testing layout plans under different parameters

Sales uplift · Time in store · Cust. Exp.

"Smart" store experience

Personalized store navigation, customized in store music and announcements, in-store tablets

Sales uplift · Time in store · Cust. Exp.

Fraudulent activity detection

Detect fake returns, identify counterfeit products, aid in analyzing security footage

Brand image · Product waste · Safety

Sales & Product Portfolio

Market trend analysis

Identify consumer pain points and provide deeper insights for product, pricing, promotions

Customer experience · Time to market

Voice of consumer

Generate insights based on NLP of customer reviews and social media comments

Customer experience

In-store custom marketing

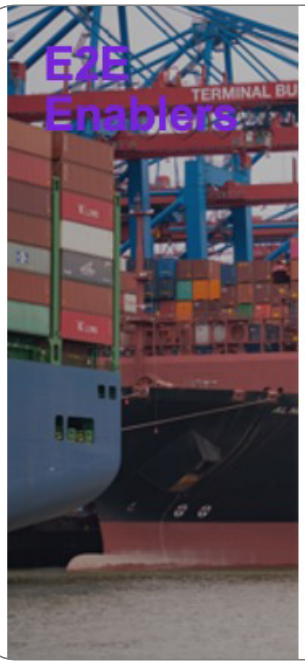
Personalized banners, aisle posters, ambassadors, and store wide discounts

Brand image · Sales uplift

Virtual fitting room (try before you buy)

Virtual product interaction such as clothing or make up try-ons

Customer experience · Sales uplift



E2E

Knowledge management

Assist in organizing and retrieving internal knowledge resources in Q&A format

Productivity

Meetings & Email assistance

Accurate summaries of key discussions, lists action items; and draft responses to emails

Productivity · Response time

Intelligent coding assistant

Suggests new lines of code, entire functions, tests, complex algorithms using natural prompts

Productivity · Errors/ bugs

Automated prescriptive reports

Accurate summaries of key discussions, lists action items; and draft responses to emails

Time to action

Synthetic data for AI/ML models

Automate visual based processes such as shelf monitoring/ planning using virtual products

Monitoring time · Costs

Training & Onboarding programs

Customized programs driven by a virtual assistant for faster, efficient processes

Costs · Employee engagement

Smart recruiting

Auto generate job descriptions, create customized candidate assessment tests

Hiring TAT · Talent level

Source: KEARNEY

Table of Contents

Source: KEARNEY

What are some challenges with Generative AI?

Data Privacy and Security
Generative AI relies on large amounts of data, making it crucial companies ensure data privacy, comply with regulations, and implement robust security measures to protect sensitive customer information.

Customer perception and acceptance
The use of AI-generated content or personalized experiences may evoke mixed reactions from customers. It is essential to monitor customer feedback, address concerns, and maintain transparency.

Transparency
It can provide inaccurate and misleading information. Without knowing the source of information, it can be difficult to trust.

Ethical considerations
The use of generative AI raises ethical concerns, such as the potential for bias in algorithms or the creation of misleading content. Ignoring the rights of content creators of original content can promote new types of plagiarism.

Potential job losses
Automation through generative AI tools may impact certain job roles. Businesses must plan for reskilling or redeployment of employees to mitigate the potential negative effects on the workforce.

Scalability
Scaling up generative AI implementations and ensuring ongoing maintenance and updates can be complex. It requires careful planning, adequate resources, and a robust infrastructure.

Skill requirements
Implementing generative AI tools may require specialized skills and expertise. Retailers and suppliers must invest in training their workforce or collaborate with experts to effectively leverage the technology.

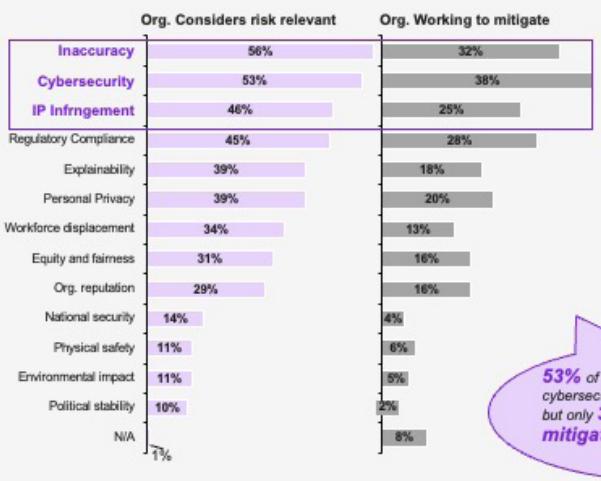
Integration
Integrating generative AI into existing systems and workflows can present technical challenges. Ensuring compatibility, seamless data exchange, and efficient integration with existing processes is essential for smooth implementation.

Source: KEARNEY

17 KEARNEY

Potential risk of generative AI adoption must be acknowledged and considered to mitigate the risks

Generative AI-related Risks
that organization consider relevant and are working to Mitigate
(% of respondents)



Source: Mckinsey Global Survey (Apr. 2023)

Potential Threats

- Unintended Bias
- Misinformation & Manipulation
- Security Risk
- Ethical Dilemmas
- Lack of Accountability

53% of organizations acknowledge cybersecurity as gen AI-related risk, but only 38% are working to mitigate that risk

18 KEARNEY

Potential threats of adopting generative AI must be identified by regardless of its industry, and it needs to be resolved with proper procedure

Potential Threats - examples

Non-Exhaustive

Unintended Bias

- **Explainability**
  - Contents may not be generated as intended
- **Political Stability**
  - Certain political party may be supported

Misinformation & Manipulation

- **Inaccuracy**
  - False information may be provided
- **Physical Safety**
  - Actual safety standard may not be aligned with physical safety standards

Security Risk

- **Cybersecurity**
  - Malware and Virus can attack Gen AI biased system
- **Personal/National Security**
  - Personal or national level of information can be shared without permission

Ethical Dilemmas

- **Workforce Displacement**
  - Displacement may occur only based on statical rates
- **Equity & Fairness**
  - Gender and ethnic may not be considered

Lack of Accountability

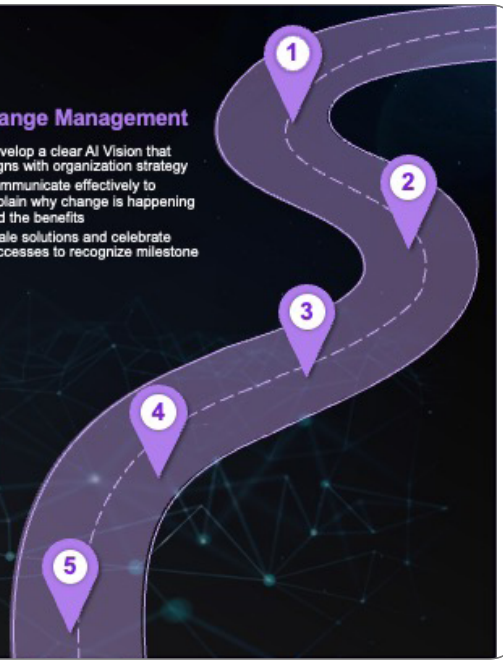
- **IP Infringement**
  - Intellectual Property can be used without permission
- **Organization Reputation**
  - Inaccurate information can be shared to impact its reputation

To maximize the effectiveness of Generative AI tools lies in the combination of human intelligence, ethical and automation data, underpinned by an understanding of the domain

19 KEARNEY

Source: Expert interview, KEARNEY

Gen AI Security Risk Mitigation Direction (in business sectors)



1 New Cyber-Risk Policy Development

- Establish new cyber-incident reporting and regulation requirements
- Consider social, humanitarian, and sustainable risks, as well as technology ones
- Prioritize risk modeling and risk assessment scoring

2 Keywords Filtering

- Prioritize and constant monitoring for sensitive keywords
- Keyword Filtering to prevent leakage of sensitive information and source code

3 Data Access Authority Management

- Identify data access authority per level to define accessible data by authority
- Manage access grants for user/organization within enterprise level to provide result based on access level

4 Cybersecurity Capability Enhancement

- Gen AI and security training for all employees
- Compliance with local and regional Data and AI laws and policies

5 Change Management

- Develop a clear AI Vision that aligns with organization strategy
- Communicate effectively to explain why change is happening and the benefits
- Scale solutions and celebrate successes to recognize milestone

Source: KEARNEY

The 12th

Asia Privacy Bridge Forum 2023

Muhammad Sufyan bin Basri

Senior Director, Personal Data Protection of Malaysia

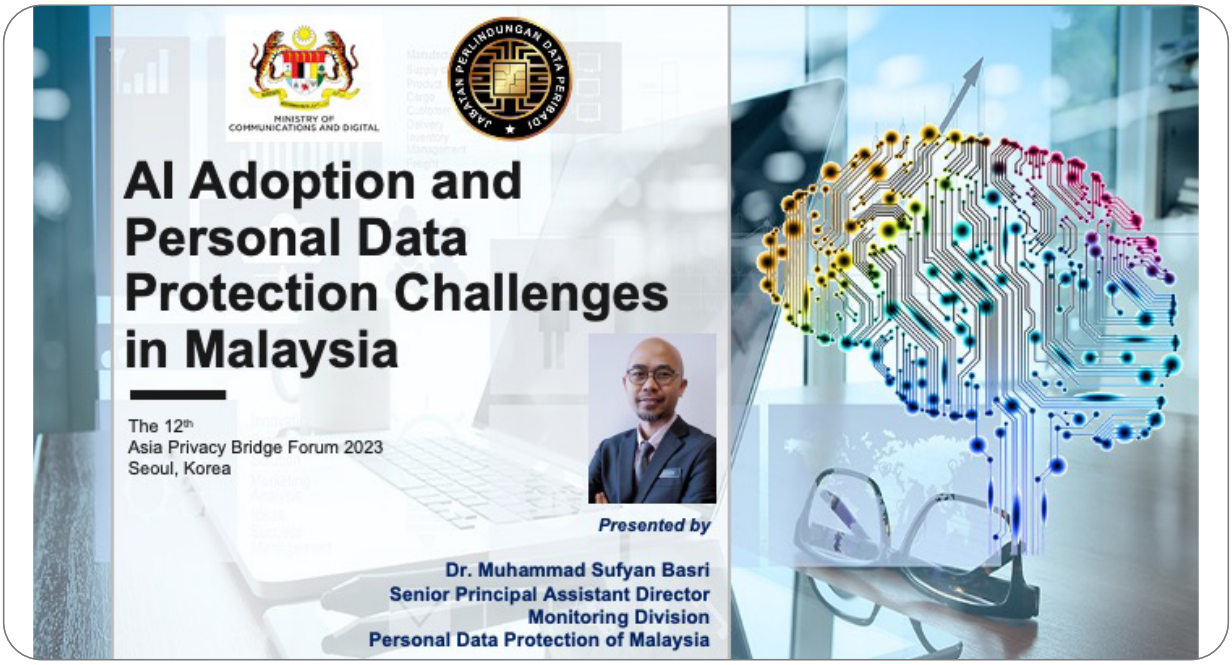
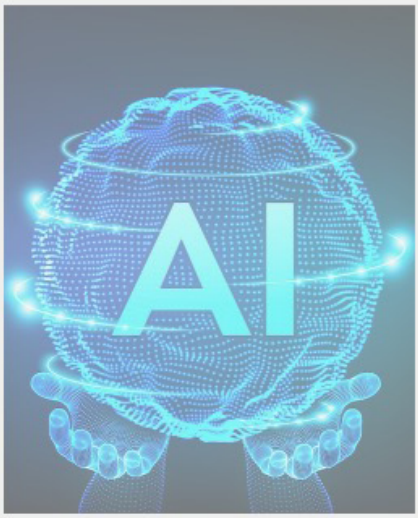


Table of contents

Section 01.

Government Policies on Artificial Intelligence (AI)

— Anwar Ibrahim,
Malaysia's 10th Prime Minister



Government Initiatives in AI

AI-RMAP

Malaysia National Artificial Intelligence Roadmap 2021 – 2025 (AI-RMAP)

MyDIGITAL

Malaysia Digital Economy Blueprint (MyDIGITAL)

NBAIC

National Blockchain and Artificial Intelligence Committee (NBAIC)

Government Commitment on Personal Data Protection & Privacy

MyDIGITAL

Malaysia Digital Economy Blueprint (MyDIGITAL)

Government Commitment on Personal Data Protection & Privacy

S2: Enhancing institutions commitment to personal data protection and privacy

3 Strengthen data protection and related regulatory framework to ensure holistic personal data protection and privacy

OBJECTIVE

Ensure that laws, practices and enforcement regarding personal data protection and privacy are comprehensive, fit-for-purpose and timely

DESCRIPTION OF INITIATIVE

- This initiative aims to enhance the nation data protection and related regulatory framework to be more holistic, covering more than just industry
- Review of existing laws, including Personal Data Protection Act (PDPA), Digital Signature Act, Cyber Security Act and Official Secrets Act
- Enhance the capacity and capability of related enforcement agencies, including through standards and certification

OUTCOME

- Individual rights are well protected through better governance of personal data and data privacy
- Enhanced public and business trust in the management of personal data and data privacy

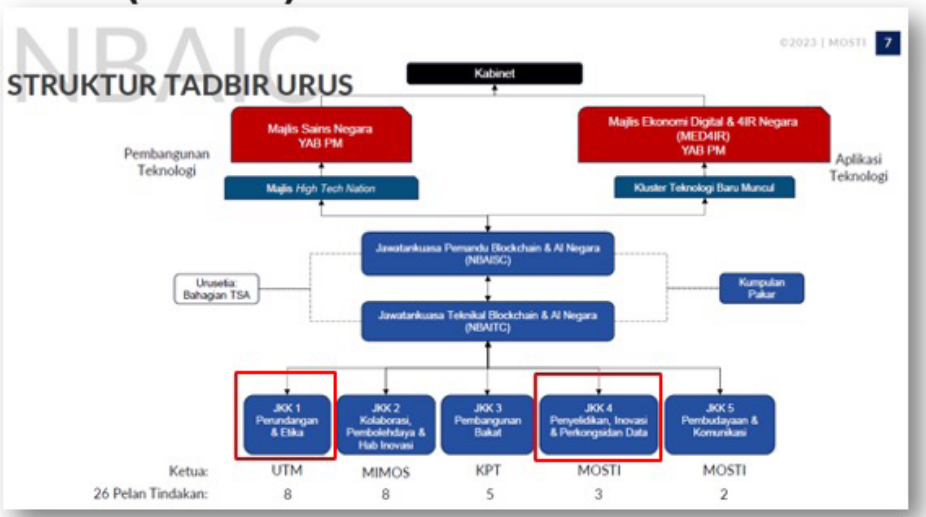
Timeline: Phase 1 to Phase 3 (2021-2030)

LEAD	TARGET
KKMM	• PDPA reviewed by 2025 • Other relevant laws reviewed by 2030

MyDIGITAL

Malaysia Digital Economy Blueprint (MyDIGITAL)

National Blockchain & Artificial Intelligence Committee (NBAIC)



National Blockchain & Artificial Intelligence Committee (NBAIC)

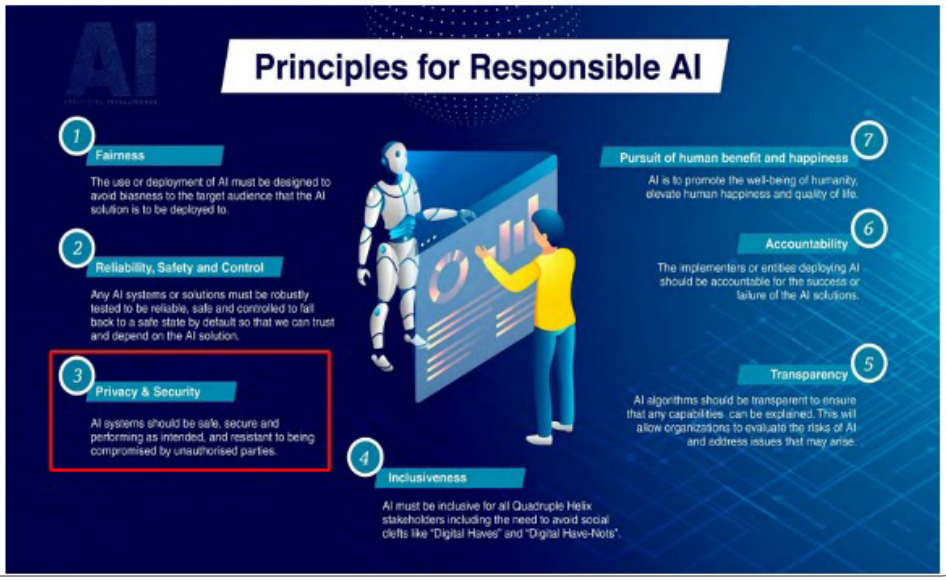
Working Committee 1 – Legislation and Ethics

To draft **legal solution** that put restrictions on the **advancement** of blockchain and **artificial intelligence technology** to make sure that all activities are carried out in **compliance with responsible principles, guidelines**, and associated act changes

Working Committee 4 – Research, Innovation and Data Sharing

To **accelerate the use** of Blockchain and **AI technology** and develop multi-party collaboration by creating a **collaboration platform** to foster Blockchain and **AI technology innovation**

Malaysia National AI-RMAP 2021-2025



Source: https://airmap.my/

Section 02.

AI Trends in Malaysia

12

AI Adoption Rate in Malaysia

- A 2019 study from Microsoft and IDC Asia/Pacific reported that only **26% of organisations** in Malaysia have started **adopting AI**.

Microsoft

IDC

- IBM Malaysia reported in June 2023 that more companies in Malaysia are exploring and integrating **Generative AI** into their business operations.
- A study by IBM's Institute for Business Value indicated over **40% of ICT professionals** reported that their organisations are actively exploring the use of Generative AI.
- The same study also indicated **1/3 of the companies** surveyed have already **integrated Generative AI**.

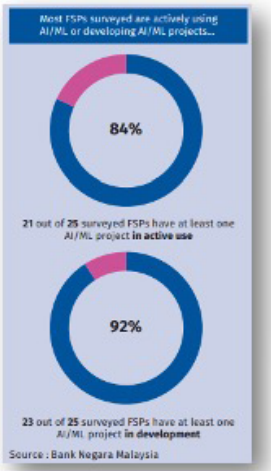
IBM

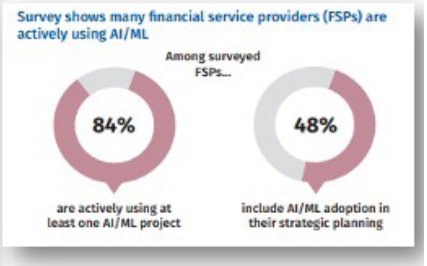
13

AI Adoption Rate in Malaysia

Adoption of AI is increasing in Malaysia:

- Based on a survey conducted by Malaysia Central Bank in 2021, with 25 respondents (FSP's):
  - **84% have at least 1 AI/ML project in active use;**
  - **92% have at least 1 AI/ML project in development;**
  - **48% to include AI/ML adoption in their strategic planning.**
- Based on a poll conducted with **315 HR professionals** by Employment Hero in May 2023:
  - **99% report using software leveraging AI;**
  - **46% use AI to identify and report on employee data trends/performance.**

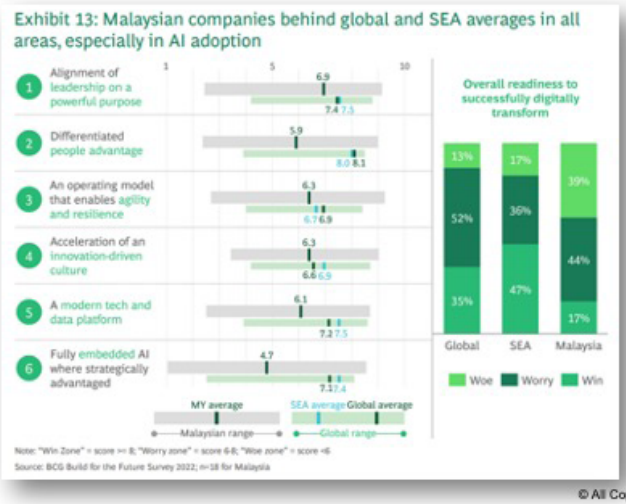




Source: Financial Stability Review 2H 2022

14

AI Adoption Rate in Malaysia



However,

- **Malaysian companies** are **behind global and SEA averages** […] especially in AI adoption.
- **Malaysian** respondents have a **score of 4.7**, compared to a **SEA average of 7.4** and **global average of 7.1**.
- This is based on a **survey of over 18 Malaysian companies** which incorporated insights from executives in a wide range of industries.

Source: Joint Report by MDEC and BCG

AI Implementation in Malaysia

Manufacturing & Automotive
- AI solution in manufacturing
- Autonomous vehicles
- Smart mobility

Financial Services
- Credit underwriting
- Anti Money laudering Fraud Detection
- Liquidity Planning
- Technology Risk Management
- KYC Digital Onboarding
- Human resources
- Customer analytics
- Customer engagement
- Trading

Healthcare & Life Sciences
- AI enabled stethoscope
- Lung cancer screening & detection

Consumer Goods & Retail
- AI SEO platform
- AI for data analytics

Communications & Multimedia
- AI news anchor
- AI generated news report

Video from Astro Awani

Section 03.

Global AI Development and Malaysia's Legislation Challenges

Patchwork of Laws

Existing law	New law and updates to existing law
Use case specific laws (e.g., self-driving cars, employment)	Industry regulation (e.g., FS, healthcare, public sector)
Guidance from regulators	Data and other AI-adjacent laws

Global AI Developments

Canada

Directive on use of Automated Decision-Making by Federal Government in effect April 2020
Artificial Intelligence and Data Act (AIDA) June 2022

United States

Maintaining American Leadership in AI 2019
AI in Government Act 2020
Executive Order on Promoting the Use of Trustworthy AI in the Federal Government 2020
OMB Guidance on Regulation of AI in Private Sector- 2020
The National AI Initiative Act 2021
NY automated employment decision tools law 2021
Blueprint for an AI Bill of Rights
AI Training Act 2022
Algorithmic Accountability Act of 2022
Draft NIST AI Risk Management Framework 2023
Federal Trade Commission issues warning Feb 2023
National AI Research & Development Strategic Plan 2023

Brazil

Senate Committee Publishes AI Report and Draft AI Law Dec 2022

Norway

DPA Sandbox on AI - 2020

France

CNIL creates AI department - Jan 2023

Egypt

National AI Strategy framework 2019

OECD

Principles on Artificial Intelligence
Recommendation of the Council on Artificial Intelligence 2019

India

Exploring AI Principles 2021

Australia

AI Ethics Framework 2019
Automated Decision Making and AI Regulation Consultation 2022
The State of AI Governance in Australia 2023

China

New Generation Code of Ethics 2021
Internet Information Service Algorithmic Recommendation Management 2022
Regulation on Promoting the Development of Artificial Intelligence Industry (Shanghai, Shenzen) 2022
Deep Synthesis Provisions 2022
Interim Measures for the Management of Generative Artificial Intelligence Services 2023

Japan

Social Principles of Human-centric AI, 2019
AI Governance Guidelines 2022

Korea

Ethics Guidelines for Intelligence Information Society, 2018
Regulatory Sandbox, 2019
Human Centered national Guidelines for AI Ethics, 2020

Singapore

Model AI Governance Framework 2019 (Updated 2020) + Implementation Self-Assessment Guide
A Guide to Job Re-Design in the Age of AI 2020
MAS Framework for Responsible AI + Veritas Consortium Phase 1 – 2020; Phase 2 - 2021
National AI Programmes in Government & Finance 2021
Proposed Advisory Guidelines on use of Personal Data in AI Recommendation and Decision Systems 2023

Source: https://oecd.ai/en/dashboards/overview

Malaysia

- Currently, there are **no general laws that are specific to AI** in Malaysia.
- Ministry of Science, Technology and Innovation ("MoSTI") recently announced that it is considering plans to develop a **legal framework to regulate the use of AI** in Malaysia.
  - Aims to cover aspects such as **data privacy, public awareness about AI use, transparency, accountability, and cybersecurity**.
  - **Labelling requirement** for **content generated by AI**.
  - **Guidelines** for **educating the public about AI** and **promoting research** in the field.
- Upcoming sectoral guidelines: **Guidelines on Technology Risk Management** issued by the **Securities Commission of Malaysia**
  - Sets out **guiding principles relating to AI and ML adoption** by capital market entities in Malaysia
  - Expected to come into force by the **third quarter of 2024**

Regulations Challenges

*"…, senior analyst at the Institute of Strategic and International Studies Farlina Said told Malay Mail that there were **no existing laws specifically for regulating AI**, but that existing policies such as **the Personal Data Protection Act (PDPA) 2010 can be used as a foundation**."*

Source: https://www.mida.gov.my/mida-news/putrajaya-working-towards-framework-to-regulate-ai/


MIDA OFFICIAL WEBSITE MALAYSIAN INVESTMENT DEVELOPMENT AUTHORITY INVEST IN MALAYSIA >YOUR PROFIT CENTRE IN ASIA

Home | Why Malaysia | Industries

Media & Events > News > Putrajaya working towards framework to regulate AI

Putrajaya working towards framework to regulate AI

07 Jun 2023

The government will develop a framework to regulate the use of artificial intelligence (AI) in Malaysia, according to Science, Technology and Innovation Minister Chang Lih Kang today.

Malaysia was also aiming for the AI industry to create 10,000 positions in the country and eventually grow the country's economy by 30 per cent, the minister said in a written reply to Merbok MP Mohd Nazri Abu Hassan.

"This regulatory framework is important as a guide in developing the artificial intelligence ecosystem in the country," the minister said.

AI and Data Protection Principles

Malaysia PDPA Principles	Tension to be Resolved	Artificial Intelligence Challenges
General Principle (Consent)		Not practical to obtain consent for the processing of personal data (including sensitive data)
Notice and Choice Principle		May produce unexplainable and unanticipated outcomes; hard to provide meaningful notice
Disclosure Principle		Uses data for new and unforeseen purposes beyond original scope
Security Principle		To consider things like risk analysis, organizational policies, physical and technical measures
Retention Principle		Needs to retain data for AI training, traceability, audit and oversight
Data Integrity Principle		Inaccurate, incomplete, non-representative data sets may lead to AI biasness and unfairness
Access Principle		Difficult to facilitate access, correction, deletion or explanation of the logic involved

Source: CIPL 1st AI Report on Data Protection in Tension

The 12th

Asia Privacy Bridge Forum 2023

Cecilia Siu

Assistant Privacy Commissioner, PCPD, Hong Kong

The 12th

Asia Privacy Bridge Forum 2023

Day 1 **Session 4**

Session Chair

Hyesun Yoon

Professor, Hanyang University, Korea

1

Issa Gayas

Attorney IV, National Privacy Commission, Philippines

2

Mohammad Saad Al-Ahmadi

Assistant Dean, KFUPM Business School, Saudi Arabia

3

Anna Gamvros

Head of IGPC, APAC at Norton Rose Fulbright

The 12th

Asia Privacy Bridge Forum 2023

Issa Gayas

Attorney IV, National Privacy Commission, Philippines

BAGONG PILIPINAS

NATIONAL PRIVACY COMMISSION

Data Sharing and Data Access Policies in the Philippines

ISO 9001:2015 CERTIFIED

SOCOTEC

NPC_DIT_PPT-V2.0, R0.0, 01 March 2022

An independent body mandated to administer and implement the provisions of the Data Privacy Act of 2012, and to monitor and ensure compliance of the country with international standards set for data protection.

BAGONG PILIPINAS

NATIONAL PRIVACY COMMISSION

Asia Privacy Bridge 2023

SOCOTEC

General Principles

Section 17. General Data Privacy Principles. The processing of personal data shall be allowed, subject to compliance with the requirements of the Act and other laws allowing disclosure of information to the public, and adherence to the principles of transparency, legitimate purpose, and proportionality.

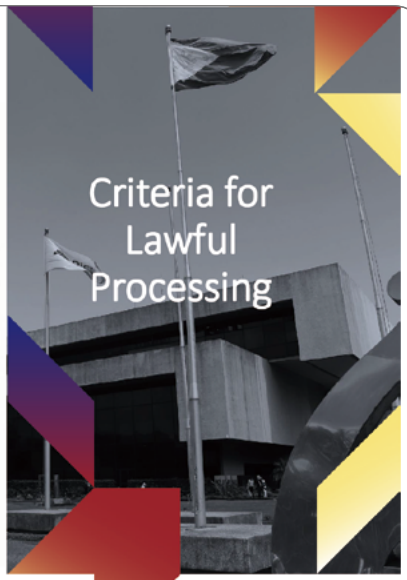
Section 18. Principles of Transparency, Legitimate Purpose and Proportionality. The processing of personal data shall be allowed subject to adherence to the principles of transparency, legitimate purpose, and proportionality.

a. Transparency. The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.

b. Legitimate purpose. The processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy.

c. Proportionality. The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

Criteria for Lawful Processing



- Consent
- Protection of Life and Health; Medical Treatment
- Laws and Regulation; Legal obligation
- Public order and public safety
- Legitimate interest
- Court proceedings, Legal claims

Advisory Opinions on Government Access

- The exemption under the DPA for information necessary to carry out the law enforcement or regulatory function of a public authority is **strictly construed.**
- There must be strict adherence to all due process requirements.
- The legitimacy of the purpose and the proportionality of the request for access or disclosure should be taken into consideration.
- Only the specified information falls outside the scope of the DPA.

Advisory Opinions on Government Access

- PICs must establish a system to avoid abuse and ensure that the requested information shall be limited only to the purpose stated by the requesting party.
- Government agencies, as personal information controllers, must implement reasonable and appropriate safeguards to secure and protect personal data, considering the provisions of NPC Circular No.16-01 on the Security of Personal Data in Government Agencies.


Data Sharing
NPC Circular – Data Sharing Agreements
State lawful basis of processing
Establish adequate safeguards for data privacy and security, and upholding of the rights of data subjects
Provide data subjects with the required information prior to collection or before data is shared, and
Adhere to the data privacy principles.
NATIONAL PRIVACY COMMISSION
Asia Privacy Bridge 2023


Data Sharing Agreement
Purpose/s of data sharing, including the public function or public service
Overview of the operational details to ensure protection of personal data
Identity of the PIC/s
DSA's term or duration
How the data subject may access the DSA
The specific method for return, destruction or disposal of information; and
General description of security measures
Details on online access, if applicable to the particular DSA;
NATIONAL PRIVACY COMMISSION
Asia Privacy Bridge 2023

The 12th

Asia Privacy Bridge Forum 2023

Mohammad Saad Al-Ahmadi

Assistant Dean, KFUPM Business School, Saudi Arabia

The 12th

Asia Privacy Bridge Forum 2023

Anna Gamvros

Head of IGPC, APAC at Norton Rose Fulbright

NORTON ROSE FULBRIGHT

Responsible Data Sharing between Public and Private Sectors

Asia Privacy Bridge Conference, Seoul

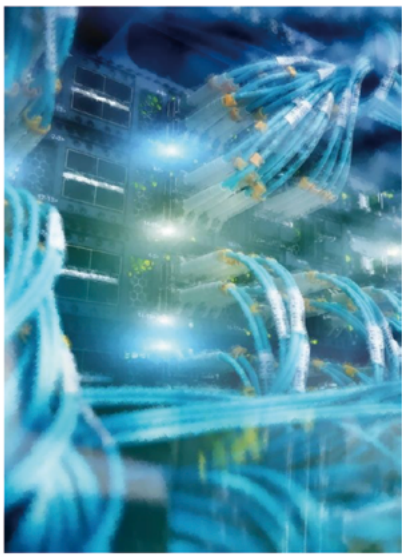
Anna Gamvros
12 October 2023
Norton Rose Fulbright LLP

Speaker

Anna Gamvros
Head of Information Governance, Privacy and Cybersecurity Asia Pacific
+852 5500 8997
anna.gamvros@nortonrosefulbright.com

Agenda

1. Importance of data sharing
2. Real-word examples
3. How is data shared?
4. What are the benefits?
5. What are the challenges?
6. How can we make it responsible?
7. How can government encourage data sharing?
8. Framework for data sharing



Importance of data sharing

Real world examples

How is data shared?

Contractual agreements

- Arrangements/agreements to sell or license data
- Preferred by technology, utilities and financial services companies, as they are more inclined to commercialise data

Open data

- Making data available to be freely used, re-used and redistributed
- No sharing of personal data or confidential data
- Expected to be provided for free or at cost
- Preferred by governments

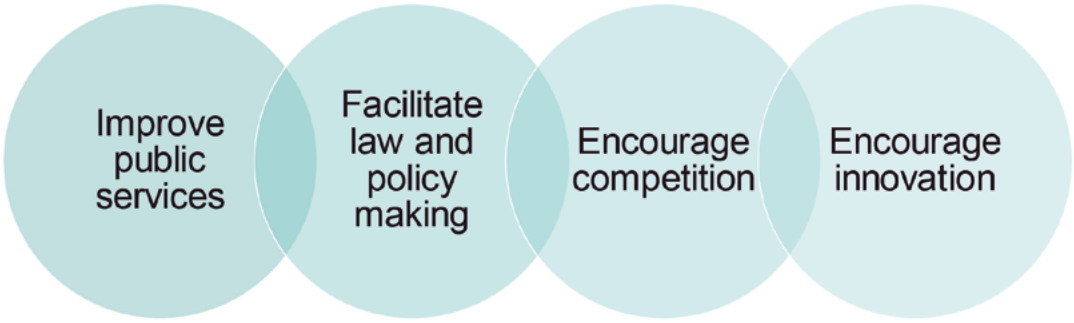
Data sharing partnerships

- Arrangements/agreements to share and mutual enrich data sets (often by cross-licensing agreements)
- Need to ensure fairness
- Used in private-private or public-private data transfers

Data of public interest

- Sharing of private-sector data considered of public interest
- Shared voluntarily by private companies or increasingly mandated by governments

What are the benefits?



What are the challenges?

- Loss of control
- Data security
- Privacy
- Regulatory and legal constraints
- Discrimination/bias
- Cross-border issues

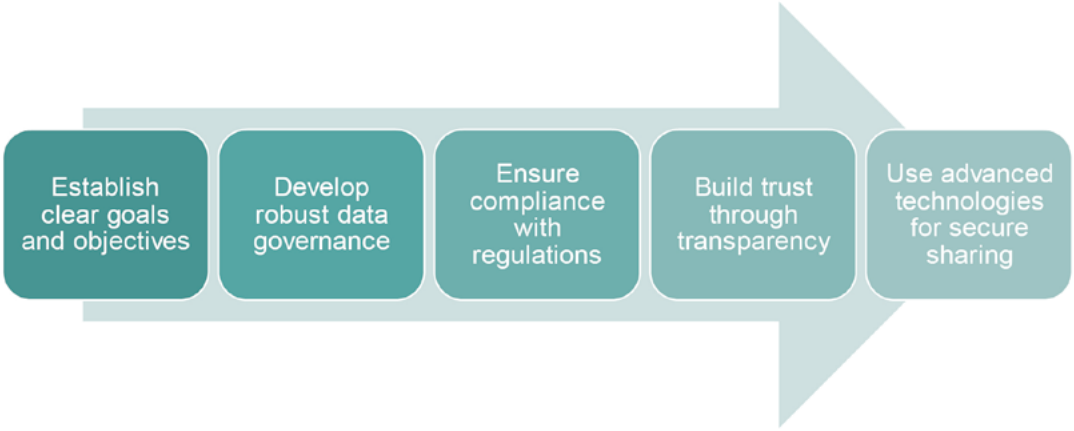
How can we make it responsible?

Oversight	Impact assessment	Technical and security measures	Data governance
Data verification	Training	Inclusiveness	Transparency

How can government encourage data sharing?

Increase data availability	Increase data portability	Increase data analytic capacities
Lower transfer costs	Maintain policy coherence	Encourage cross-border sharing

Framework for data sharing



Questions

Appendix

Published frameworks

Europe

- EU Data Governance Act (covers transfers within the private sector)
- EU Data Act (mandate during public emergencies) (proposed)
- Ethical Health Data Sharing in Public-private Partnership by Switzerland's Personalised Health Network

US

- National Strategy to Advance Privacy-Preserving Data Sharing and Analytics (covers transfers within the private sector)

Asia Pacific

- Australia's Best Practice Guide to Applying Data Sharing Principles (covers transfers of public sector data within the public sector, originally aimed to allow sharing of such data to the private sector)
- Singapore's Trusted Data Sharing Framework (covers transfers within the private sector)
- India's Data Empowerment and Protection Architecture (covers transfers within the private sector)

Global

- OECD's Recommendation on Enhancing Access and Sharing of Data (covers transfers within the private sector)
- Centre for Information Policy Leadership's Data Sharing between Public and Private Sectors

NORTON ROSE FULBRIGHT

nortonrosefulbright.com

The 12th

Asia Privacy Bridge Forum 2023

Day 2 Session 1

Hiroshi Miyashita

Professor, Chuo University, Japan

Data Free Flow with Trust
-Human Rights and Trade-

13 October 2023
Hiroshi Miyashita
Professor (LL.D.), Chuo University

DFFT (Data Free Flow with Trust)

- **The Prime Minister's Speech at the World Economic Forum** (January 2019)

*'Let Osaka G20 set in train a new track for looking at data governance--call it the Osaka Track--**under the roof of the WTO.***

We have yet to catch up with the new reality, in which data drives everything, where the D.F.F.T., the Data Free Flow with Trust, should top the agenda in our new economy.'

- **G20 OSAKA LEADERS' DECLARATION** (June 2019)

'... we can further facilitate data free flow and strengthen consumer and business trust. In this respect, it is necessary that legal frameworks, both domestic and international, should be respected. Such data free flow with trust will harness the opportunities of the digital economy. '

- Japan's host of the G7 Summit in 2023

WTO and Data Flow Rules

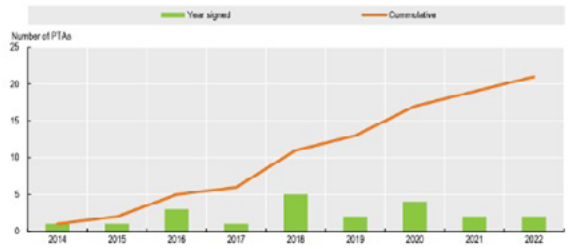
- *General Exemption clause (GATS Art.14(C)(ii)) of 'the protection of the privacy of individuals in relation to the processing of dissemination of personal data' and 'a means of arbitrary or unjustifiable discrimination'*
- *'The WTO has many Members, so providing it with rules on digital trade that materialize "Data Free Flow with Trust" (DFFT) will make business more predictable and stable. This will in turn promote further digital trade. With the aim of achieving early results, we will work to accelerate and add further impetus to the negotiations'*

Cost of Data Localisation

'Digitalisation has significantly reduced the cost of engaging in international trade; facilitated the coordination of global value chains; helped diffuse ideas and technologies; and connected a greater number of businesses and consumers globally.'

- OECD, Digital Trade and Market (2018)

Figure 5. Data localisation provisions in PTAs *PTAs=preferential trade agreements



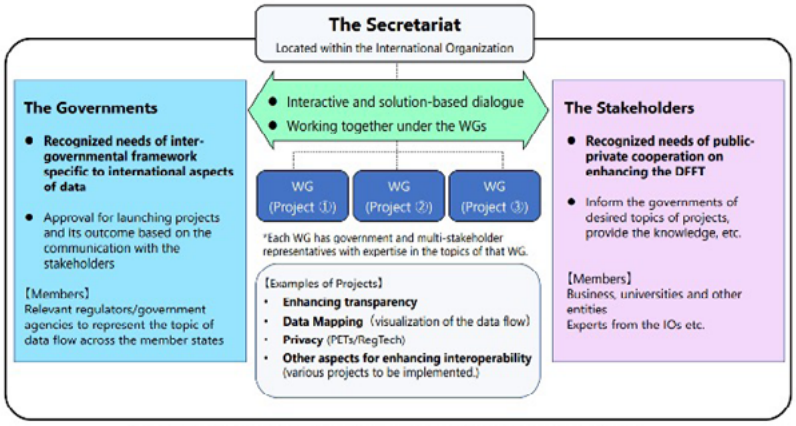
Note: See Annex Table A1 for a list of agreements.
Source: Author's compilation based on TAPED database (Burri and Polanco, 2020[7]).

OECD, A Preliminary Mapping of Data Localisation Measures (June 2022).

Institutional Arrangement for Partnership (IPA)

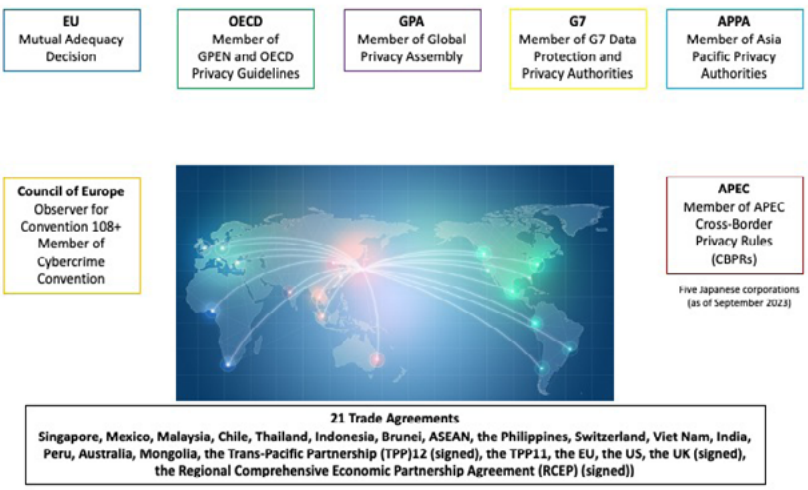
G7 Hiroshima Leaders' Declaration, 2023

'we endorse the Annex on G7 Vision for Operationalising DFFT and its Priorities from the Digital and Tech Ministers' Meeting, and the establishment of the Institutional Arrangement for Partnership.'



Digital Agency of Japan, IAP Structure Chart (https://www.digital.go.jp/en/dfft-iap-en)

Global Context of the Japan's data flow



The G7 heads of state attend a meeting during the G7 Leaders' Summit in Hiroshima. The summit endorsed the Ministerial Declaration which promoted the Data Free Flow with Trust initiative. May 19, 2023. REUTERS/Brendan Smialowski/Pool

Data Free Flow with Trust: The Group of Seven (G7) and Group of Twenty (G20) countries also have focused in recent years on international data transfers. These groups can serve as incubators for new thinking and can provide an impetus for institutionalizing further work in existing regional international organizations.

concluded a digital trade agreement with the United States containing data flow guarantees.[59] Japan sees itself as a pragmatic broker in the multilateral arena between the US and EU perspectives.

Since its 2019 launch, there has been work under the DFFT ru-

Japan sees itself as a pragmatic broker in the multilateral arena between the US and EU perspectives.

-Kenneth Propp, More than Adequate: New Directions in International Data Transfer Governance, Atlantic Council (June 2023)

EU-Japan Mutual Adequacy Decision
(23 January 2019)

The Commission considers that **the APPI (the Japanese Act on the Protection of Personal Information) as complemented by the Supplementary Rules contained in Annex I, together with the official representations, assurances and commitments contained in Annex II**, ensure a level of protection for personal data transferred from the European Union that **is essentially equivalent** to the one guaranteed by Regulation (EU) 2016/679. (para 171)

EU- South Korea Adequacy Decision (17 December 2021)
The Commission considers that the Republic of Korea – **through PIPA, the special rules applicable to certain sectors (as analysed in Section 2) and the additional safeguards provided in Notification No 2021-5 (Annex I)** – ensures a level of protection for personal data transferred from the European Union that **is essentially equivalent** to the one guaranteed by Regulation (EU) 2016/679. (para209)

President Koen Lenaerts
Cour de justice de l'Union européenne

*... it makes clear that **a measure that compromises the essence of a fundamental right may not be justified on any ground**, not even where the national security of a third country is at stake.*

The judgment of the CJEU in Schrems sends a clear message to the EU political institutions to the effect that they may only adopt measures that respect the essence of the fundamental rights in question.

- 'Limits on Limitations: The Essence of Fundamental Rights in the EU' 20 German Law Journal (2019) 779.

The Japan-U.S./U.K. Trade Agreement

24 December 2020

7 October 2019

ARTICLE 8.73 Source code
1. A Party **shall not require the transfer of, or access to, source code of software** owned by a person of the other Party, **or the transfer of, or access to, an algorithm expressed in that source code,** as a condition for the import, distribution, sale or use of that software, or of products containing that software, in its territory.

Trade Agreement between Japan and the United States of America concerning Digital Trade (entry into force on 1 January 2020)
ARTICLE 17 **Neither Party shall require the transfer of, or access to, source code of software** owned by a person of the other Party, **or the transfer of, or access to, an algorithm expressed in that source code,** as a condition for the import, distribution, sale, or use of that software, or of products containing that software, in its territory.

Cf.) EU-UK Trade and Cooperation Agreement Article DIGIT.12: Transfer of or access to source code
1. A Party shall not require the transfer of, or access to, the source code of software owned by a natural or legal person of the other Party

(source) MOFA: https://www.mofa.go.jp/press/kaiken/kaiken4e_000842.html
https://www.mofa.go.jp/ecm/ie/page22e_000914.html
https://ustr.gov/about-us/policy-offices/press-office/ustr-archives/usita

Algorithmic Transparency in the Trade Agreements

Trade agreement	Data protection law
Prohibition of accessing source code	Transparency of the logic involved

'[C]ontrollers cannot rely on the protection of their trade secrets as an excuse to deny access or refuse to provide information to the data subject.'
(European Data Protection Board, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 6 February 2018 p.17)

ARTICLE22 Automated individual decision-making, including profiling

1. The data subject shall have **the right not to be subject to a decision based solely on automated processing, including profiling,** which produces legal effects concerning him or her or similarly significantly affects him or her.
2. Paragraph 1 shall not apply if the decision:
(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
(c) is based on the data subject's explicit consent.
3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at **least the right to obtain human intervention** on the part of the controller, to express his or her point of view and to contest the decision.
4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

ARTICLE13 Information to be provided where personal data are collected from the data subject

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:
(d) **the existence of automated decision-making, including profiling**, referred to in Article 22(1) and (4) and, at least in those cases, **meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject**.

The 12th

Asia Privacy Bridge Forum 2023

Day 2 Session 2

Janssen Esguerra

IT officer I, National Privacy Commission, Philippines

BAGONG PILIPINAS

NATIONAL PRIVACY COMMISSION

Data Breach Notification Across Borders

ISO 9001:2015 CERTIFIED

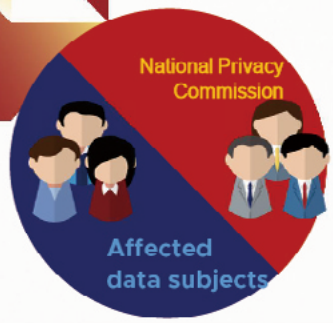
SOCOTEC

NPC_DIT_PPT-V2.0, R1.0, 01 September 2023

Introduction

The Data Privacy Act of 2012 (DPA) is the Philippine law that protects the privacy of individuals' personal data. It applies to all entities that process personal data, regardless of nationality or location.

Who should be notified?



- Notification must be made to the **NPC*** and to any **affected individuals**.
- This obligation applies even if the breach occurred outside of the Philippines, as long as the affected individuals are Philippine residents.

***DATA BREACH NOTIFICATION AND MANAGEMENT SYSTEM (DBNMS)** Launched on 20 April 2022 for ease of reporting Personal Data Breach Notifications (PDBN) to the Commission https://dbnms.privacy.gov.ph

When is data breach reporting mandatory?

Notification of a data breach is **mandatory** when:

All three elements must be present!

- It involves sensitive personal information or that may be used for identity fraud.
- Information may have been acquired by an unauthorized person or group of people.
- It is likely to give rise to a real risk of serious harm to the affected data subjects.

When to notify?

The **NPC** must be notified **within 72 hours** upon knowledge of, or when there is reasonable belief that a personal data breach has occurred.

Notification to the **Data Subject** must be sent **individually.**

How to notify?

- ❑ Data Breach Notifications are only made through the Data Breach Notification Management System (DBNMS) of the NPC.
- ❑ Other forms of Notification is not allowed or invalid.

Delay in Notification

The PIC may delay notification only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.

Cross-Border Data Breach Notification

The DPA does not specifically address the issue of cross-border data breach notification. However, the National Privacy Commission (NPC), the Philippine data protection authority, has issued guidelines on this issue.

Cross-Border Data Breach Notification

According to the NPC guidelines, a PIC must notify the NPC of a cross-border data breach if the breach is likely to give rise to a real risk to the rights and freedoms of Philippine data subjects. The NPC may also require the PIC to notify affected individuals directly.

Cross-Border Data Breach Notification

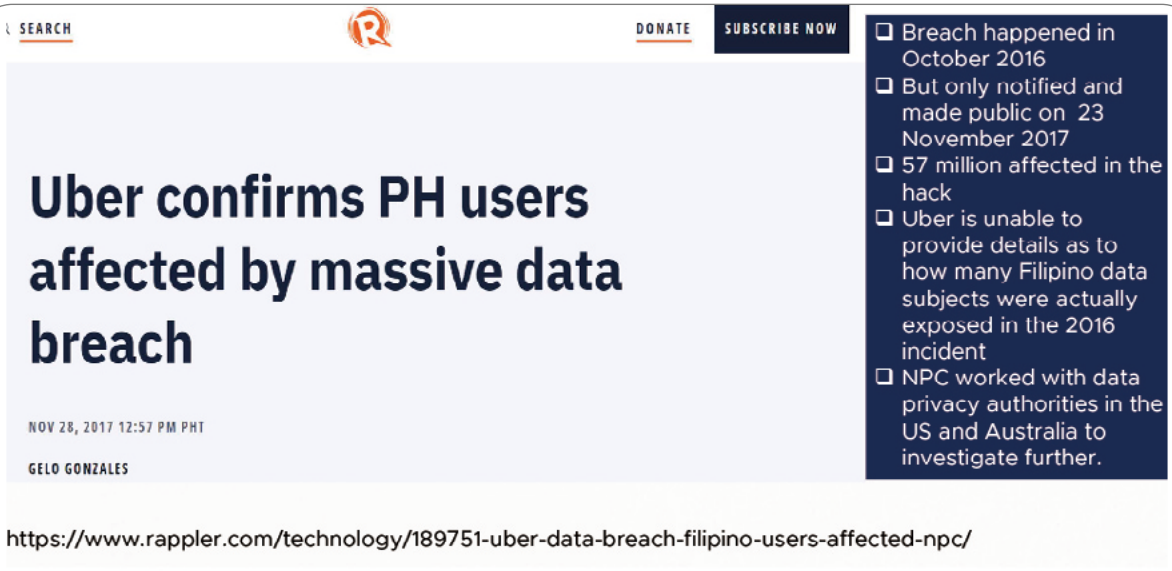
The NPC can cooperate with other data protection authorities in other countries to investigate and address cross-border data breaches.

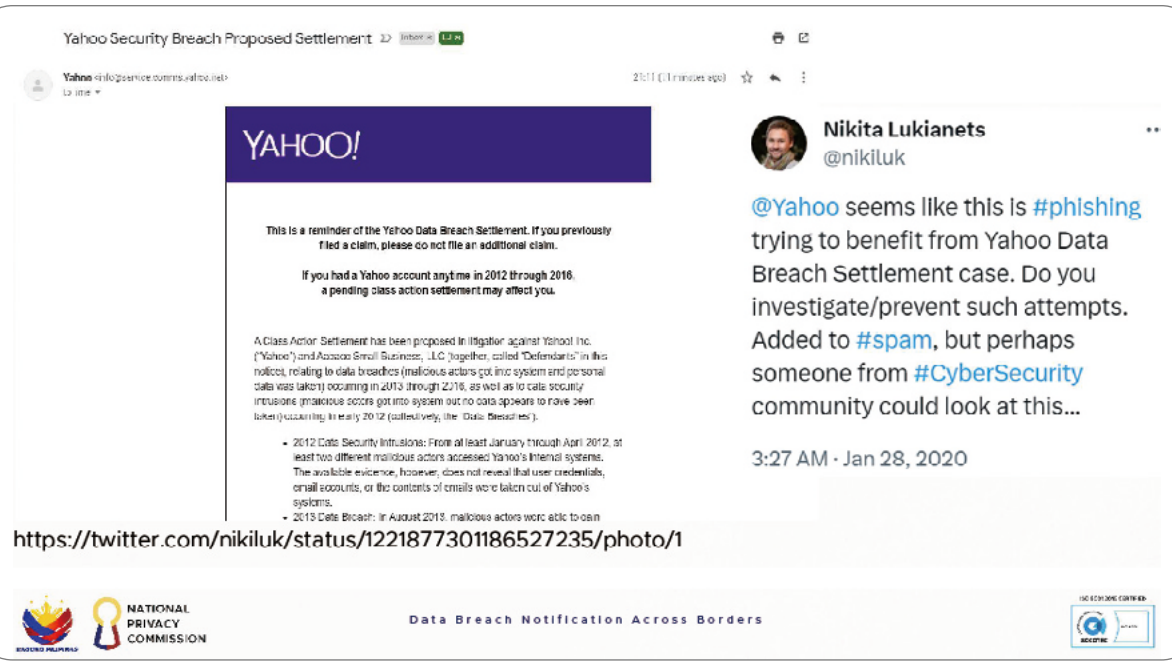
Challenges of Cross-Border Data Breach Notification

- ❑ Lack of uniformity in data protection laws around the world
  - Different countries have different requirements for data breach notification, which can make it difficult for PICs to comply with all applicable laws.

Challenges of Cross-Border Data Breach Notification

- ❑ Difficulty of determining which data subjects have been affected by a cross-border data breach
  - Especially true if the data breach involves the identity theft from a cloud server or other centralized repository.


SEARCH
DONATE
SUBSCRIBE NOW
Uber confirms PH users affected by massive data breach
NOV 28, 2017 12:57 PM PHT
GELO GONZALES
Breach happened in October 2016
But only notified and made public on 23 November 2017
57 million affected in the hack
Uber is unable to provide details as to how many Filipino data subjects were actually exposed in the 2016 incident
NPC worked with data privacy authorities in the US and Australia to investigate further.
https://www.rappler.com/technology/189751-uber-data-breach-filipino-users-affected-npc/
NATIONAL PRIVACY COMMISSION
Data Breach Notification Across Borders


Yahoo Security Breach Proposed Settlement
YAHOO!
This is a reminder of the Yahoo Data Breach Settlement. If you previously filed a claim, please do not file an additional claim.
If you had a Yahoo account anytime in 2012 through 2016, a pending class action settlement may affect you.
A Class Action Settlement has been proposed in litigation against Yahoo! Inc. ("Yahoo") and Aabaco Small Business, LLC (together, called "Defendants" in this notice), relating to data breaches (malicious actors got into system and personal data was taken) occurring in 2013 through 2016, as well as to data security intrusions (malicious actors got into system but no data appears to have been taken) occurring in early 2012 (collectively, the "Data Breaches").
2012 Data Security Intrusions: From at least January through April 2012, at least two different malicious actors accessed Yahoo's internal systems. The available evidence, however, does not reveal that user credentials, email accounts, or the contents of emails were taken out of Yahoo's systems.
2013 Data Breach: In August 2013, malicious actors were able to gain
Nikita Lukianets
@nikiluk
@Yahoo seems like this is #phishing trying to benefit from Yahoo Data Breach Settlement case. Do you investigate/prevent such attempts. Added to #spam, but perhaps someone from #CyberSecurity community could look at this...
3:27 AM · Jan 28, 2020
https://twitter.com/nikiluk/status/1221877301186527235/photo/1
NATIONAL PRIVACY COMMISSION
Data Breach Notification Across Borders

Current Initiatives of the NPC

Development of a new NPC Circular, "Security Incident Management"

- Proper management of security incidents should include prevention, incident response, mitigation and compliance with notification requirements;

NATIONAL PRIVACY COMMISSION

Recommendations

- ❑ Use of international standards for security incident management or incident response: the ISO/IEC 27035 family of standards provide common principles and guidelines towards preparing for, detecting, reporting, assessing, responding to incidents, and applying lessons learned accordingly
  - ❑ Other standards: NIST 800-128, 800-137
- ❑ Align and amend data protection provisions on breach notification according to global data protection frameworks
  - ❑ General Data Protection Regulation (GDPR)
- ❑ Leverage resource-sharing and joint investigations with other data protection authorities for "joint investigations when multiple individuals are affected in data breaches

NATIONAL PRIVACY COMMISSION

The 12th

Asia Privacy Bridge Forum 2023

Day 2

Session 3

Jong-Chul Shin

Professor, Yonsei University Law School, Korea

Past, Present and Future of the PERSONAL INFORMATION PROTECTION ACT in Korea

Jongchul Shin, Adjunct Professor, Yonsei University Law School
Attorney at law in Illinois of the U.S.A., Juris Doctor

연세대학교 YONSEI UNIVERSITY

Past of the Personal Information Protection Act in Korea (1)

1. The separation of two laws related to Personal information protection before 2020: (1) PERSONAL INFORMATION PROTECTION ACT and (2) ACT ON PROMOTION OF INFORMATION AND COMMUNICATIONS NETWORK UTILIZATION AND INFORMATION PROTECTION(hereinafter referred to as "NETWORK UTILIZATION AND INFORMATION PROTECTION ACT")

2. Law regulating personal information protection in the online: NETWORK UTILIZATION AND INFORMATION PROTECTION ACT

3. Law regulating personal information protection in the offline: PERSONAL INFORMATION PROTECTION ACT

Past of the Personal Information Protection Act in Korea (2)

1. Amendment of the so-called 3 Data Acts in 2020: (1) PERSONAL INFORMATION PROTECTION ACT, (2) CREDIT INFORMATION USE AND PROTECTION ACT, (3) NETWORK UTILIZATION AND INFORMATION PROTECTION ACT

2. Another new separation of two laws related to Personal information protection after 2020: (1) PERSONAL INFORMATION PROTECTION ACT, (2) CREDIT INFORMATION USE AND PROTECTION ACT

Past of the Personal Information Protection Act in Korea (3)

1. Law regulating personal information protection in general: PERSONAL INFORMATION PROTECTION ACT

2. Law regulating personal information protection on the financial and credit information: CREDIT INFORMATION USE AND PROTECTION ACT


ACT ON PROMOTION OF INFORMATION AND COMMUNICATIONS NETWORK UTILIZATION AND INFORMATION PROTECTION

CHAPTER I GENERAL PROVISIONS

PERSONAL INFORMATION PROTECTION ACT

CHAPTER I GENERAL PROVISIONS

CREDIT INFORMATION USE AND PROTECTION ACT

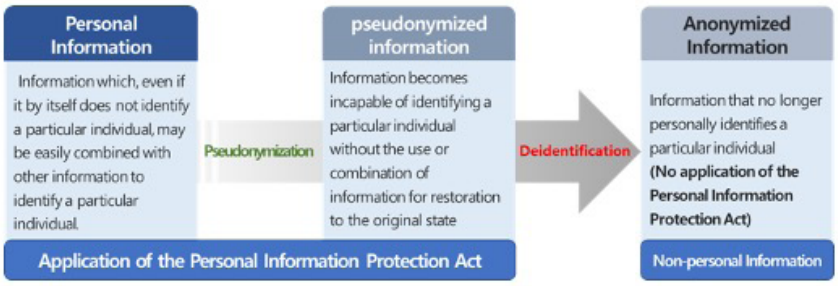
CHAPTER I GENERAL PROVISIONS

Present of the Personal Information Protection Act in Korea (1)

1. The Personal Information Protection Act, which was revised in 2020, has been revised in 2023 again
2. Repeal of the CHAPTER VI SPECIAL CASES CONCERNING PROCESSING OF PERSONAL INFORMATION BY PROVIDERS OF INFORMATION AND COMMUNICATIONS SERVICES OR SIMILAR in the Personal Information Protection Act of 2020
3. The former CHAPTER VI included rules regulating personal information protection in the online

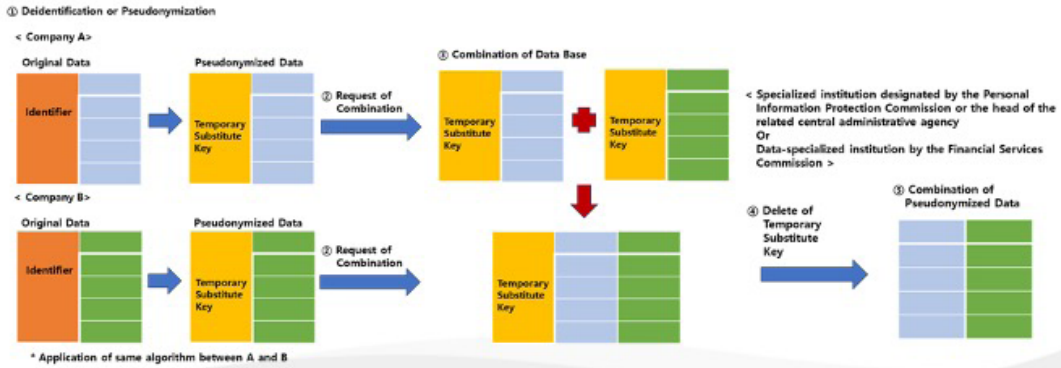
Present of the Personal Information Protection Act in Korea (2)

1. The Personal Information Protection Act stipulates the pseudonymization or de-identification



Present of the Personal Information Protection Act in Korea (3)

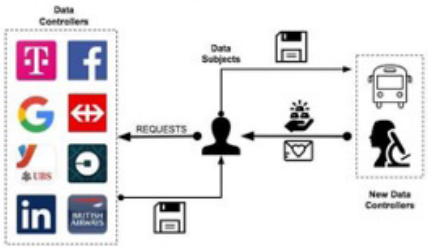
1. The Personal Information Protection Act stipulates the Combination of Pseudonymous Data (Personal Information)



Present of the Personal Information Protection Act in Korea (4)

1. The Personal Information Protection Act stipulates the Request for transfer of personal information, so-called "My data" like the Right to Data Portability in EU GDPR

2. The Credit Information Use and Protection Act already adopted "My data" in 2020



Present of the Personal Information Protection Act in Korea (5)

1. The Personal Information Protection Act stipulates the Imposition of Administrative Surcharges: From "3/100 of the total revenues relating to the concerned violation" to "3/100 of the total revenues"

2. The Personal Information Protection Act stipulates the Protection of Information Transferred Overseas: In addition to "Obtaining users' consent", New revised Act added the "Adequacy decision" like EU GDPR

Present of the Personal Information Protection Act in Korea (6)

1. The Personal Information Protection Act stipulates the Imposition of Limitation to Installation and Operation of Visual Data Processing Devices: in addition to "Fixed Visual Data Processing Devices" like CCTV device, New revised Act added "Mobile Visual Data Processing Devices" like Drone camera or Wearable camera

Future of the Personal Information Protection Act in Korea (1)

1. What are the problems?
2. Is it desirable the Personal Information Protection Act focusing on criminal punishment?
3. Is it desirable the Personal Information Protection Act to be based on "Users' Consent", so-called "Opt-In"?

Future of the Personal Information Protection Act in Korea (2)

1. What are the desirable solutions?
2. Criminal punishment is not a panacea(Cure-all): Change to the Absorption of economic benefits?, Not Criminal punishment
3. Users' Consent is not a panacea(Cure-all): Change to the Opt-Out?, Enhancement of real Users' Right to Self-Determination of Personal Information

Barun ICT Research Center

Barun ICT Research Center, Yonsei University
#720 Yonsei-Samsung Library 50 Yonsei-ro, Seodaemungu, Seoul 03722 Korea

Phone +82-2-2123-6694 | Fax +82-2-2123-8095 | barunict@barunict.kr | www.barunict.org