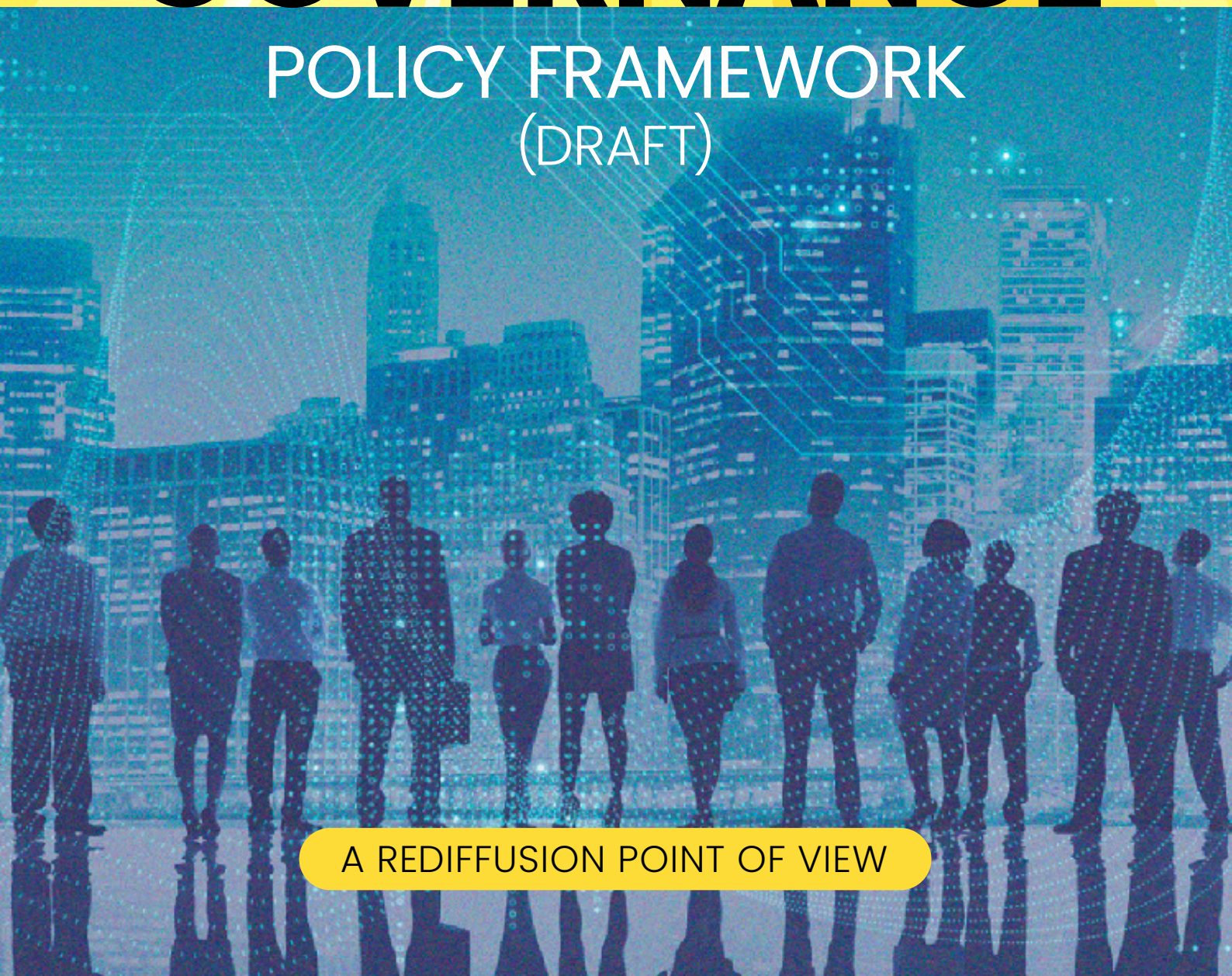
RED LAB™
Rediffusion Consumer Lab

NATIONAL DATA GOVERNANCE

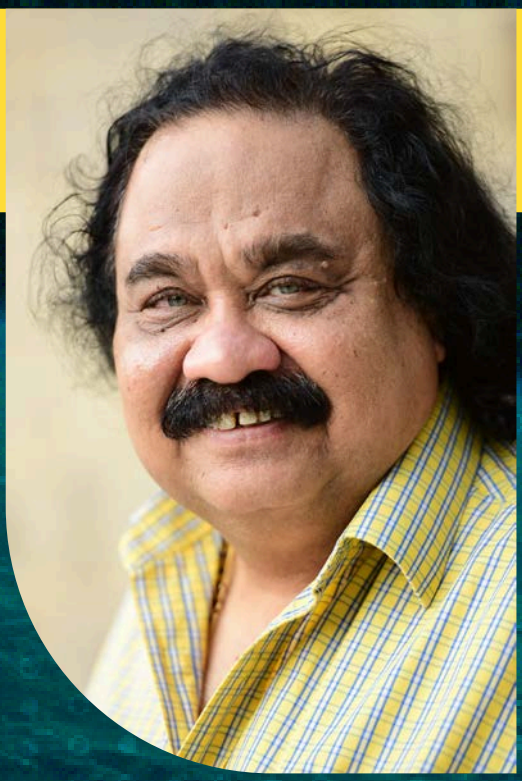
POLICY FRAMEWORK (DRAFT)



A REDIFFUSION POINT OF VIEW

FOREWORD

A POLICY IMPACTING EVERY INDIAN



Dr. Sandeep Goyal
Managing Director, Rediffusion &
Chief Mentor, Forum for Ethical Use of Data (FEUD)

The **Ministry of Electronics and Information Technology (MeitY)** has recently issued a fresh draft on the **National Data Governance Framework Policy (NDGFM)** with increased emphasis on sharing of non-personal data for building a large repository of India-specific datasets and for use by researchers and start-ups.

As part of the framework, a platform will be designed which will process requests and provide access to **non-personal** and/or **anonymised** datasets to Indian researchers and start-ups. Earlier, MeitY had issued a draft policy on the same but retracted it after the ministry faced widespread criticism over plans to monetise sharing of data. The new (current) draft does not have any provisions for data monetisation.

FOREWORD

A POLICY IMPACTING EVERY INDIAN

As part of the policy, the Indian government will also build the India Datasets program, which will consist of non-personal and anonymised datasets from Government entities that have collected data from Indian citizens or those in India. Private entities will be encouraged to share such data, according to the policy.

As per the draft policy, every government ministry/department/organisation will have to identify and classify available datasets. Private companies can also create datasets and contribute to the India Datasets program. IDMO will prescribe rules and standards in this regard, the draft policy reads.

Since the draft policy has very pronounced impact on every Indian citizen, every Indian consumer, Red Lab has put together this report on what is proposed, and what the implications are.

To read the bare report, CLICK HERE

Towards More Effective Data-Driven Governance

A BACKGROUND TO THE POLICY

Digitization of government, governance and **economy** is progressing at a rapid pace. India's unique platformisation strategy is showing the world how public service delivery and governance can be transformed at scale through public digital platforms.

These public digital platforms are empowering citizens, enhancing government-citizen engagement, driving data-driven governance, and leading to inclusive development.

Through creating the world's largest public digital platforms, India is becoming the world's pre-eminent country in deploying technology for transforming people's lives, improving governance and creating vibrant innovation eco-systems. During COVID-19 pandemic, Digital Governance played a big part in India's resilient response to the pandemic and its impact on lives, livelihoods, and the economy.

In the **post-COVID-19 era,** this digitization of government is accelerating faster. With this accelerated digitization, the volume and velocity of data generated is also increasing exponentially. This data can be used in turn to improve citizens' experience and engagement with the government and governance as a **'Digital Nagrik'.**

However, the **Digital Government data** is currently managed, stored and accessed in differing and inconsistent ways across different government entities, thus attenuating the efficacy of data-driven governance, and preventing an innovative ecosystem of data science, analytics and AI from emerging to its full potential. The power of this data must be harnessed for more effective Digital Government, public good and innovation, thus requiring a **National Data Governance Framework Policy (NDGFP).**

This **Policy** aims to realize the full potential of Digital Government with the aim of maximising data-led governance and catalysing data-based innovation that can transform government services and their delivery to citizens, especially in areas of social importance that include **agriculture, healthcare, law and justice, education,** amongst others.

This policy also launches **non-personal data** based **India Datasets program** and addresses the methods and rules to ensure that non-personal data and anonymized data from both government and private entities are safely accessible by the research and innovation ecosystem.

The Right Policy At The Right Time

OPINION

Ruchira Raina
Executive Director - South & East, Rediffusion

Mark Linscott

Anand Raghuraman

India's digital economy, as per **Mark Linscott & Anand Raghuraman,** has changed dramatically since it undertook its last major legislative overhaul in **2008** with amendments to the **Information Technology Act. Mobile devices, social media** and **e-commerce** are now ascendant. From a truly big picture perspective, India's digital economy can be characterized by these headline features:

- Indian companies and startups compete alongside **US, Chinese, Japanese, Korean,** and **other companies** – making India distinct as one of the world's most diverse, large-scale digital economies.
- India's dynamic and vibrant digital economy hosts nearly half a billion citizens. This figure is set to reach **840 million by 2022** as a dizzying array of apps, services and devices vie for Indians' attention and wallets.

- For the first time ever, there are more **rural Indians online** than urban Indians. That is an indicator of the rapid growth in India's digital ecosystem, but also of the potential of a new community with profoundly different life experiences and needs than early internet adopters.

- Nearly half a billion Indians have yet to come online. Integrating them into the digital economy is a profound challenge for policy makers.

I tend to agree with Linscott & Raghuraman. Digital India is at a cross-road. The new data governance framework comes at just the right time. I hope there will be adequate debate and discussion with all parts of the digital economy voicing their views and concerns on the draft policy.

The Institutional Framework

INDIA DATA MANAGEMENT OFFICE (IDMO)

An **"India Data Management Office (IDMO)"** shall be set up under the **Digital India Corporation ("DIC")** under MeitY and shall be responsible for framing, managing and periodically reviewing and revising the Policy.

The IDMO shall also be responsible for developing rules, standards, and guidelines under this Policy that shall be published periodically.

The IDMO shall also encourage and foster data and **AI-based Research,** start-up eco-systems by working with the **Digital India Start-up Hub** (the erstwhile MSH).

Every **Ministry/Department** shall have **Data Management Units ("DMUs")** headed by a designated CDO who shall work closely with the IDMO for ensuring implementation of the Policy.

IDMO will design and manage the **India Datasets** platform that will process requests and provide access to the non-personal and/or anonymized datasets to Indian researchers and startups.

ROLES & RESPONSIBILITIES

- **Data Storage & Retention**

  A comprehensive and evolving set of standards and rules would be developed and provided by IDMO - including on the cloud - to help Ministries/Departments define their data storage and retention framework.

- **Government-to-Government Data Access**

  A standard mechanism for inter-government data access shall be developed by the IDMO. All Government Ministries/Departments shall create detailed, searchable data inventories with clear metadata and data dictionaries for government-to-government data access.

- **India Datasets Program**

  IDMO will enable and build the India Datasets Program, which will consist of non-personal and anonymized datasets from the Government entities that have collected data from Indian citizens or those in India. Private entities will be encouraged to share such data. Private companies can also create Datasets and contribute to India Datasets Program.

- **Data Anonymisation**

  IDMO will set and publish data anonymization standards and rules to ensure informational privacy is maintained.

- **Datasets Access and Availability**

  The IDMO shall notify protocols for sharing of non-personal datasets while ensuring privacy, security and trust. IDMO will also judge the genuineness and validity of data usage requests, for datasets other than those already made available on Open Data Portal.

- **Capacity & Skill Building**

  The IDMO shall support holistic and comprehensive capacity building initiatives for officials in all government agencies to build data and digital literacy, knowledge, and skills. The IDMO shall also assist in setting up DMUs in Ministries and Departments to create dedicated capacity for data management.

- **Ethical and Fair Use of Data**

  The IDMO shall define the principles for ethical and fair use of data shared beyond the government ecosystem.

- **Redressal Mechanism**

  The IDMO shall institute a mechanism for citizens to request datasets, register grievances and establish responsibility of DMUs under the IDMO to respond in a timely manner, to facilitate transparent and accountable data sharing ecosystem.

- **Policy Monitoring & Enforcement**

  The IDMO will be responsible for the implementation and enforcement of the NDGFP and rules and standards issued from time to time.

- **Awareness Building**

  The IDMO shall ensure adequate awareness building by sharing SOPs, FAQs, Operating Manuals and shall also ensure appropriate branding for quick adoption of the Policy.

- **User Charges**

  The IDMO may decide to charge User charges/ Fees for its maintenance/services.

Baby Steps, But Big Strides Ahead

OPINION

Rajendra Gupta
Director, Rediffusion Smart Media

Oleg Petrov,
World Bank

Having spent over twenty years with **Airtel** and **Reliance,** I am really fascinated by all the developments that are taking place at the policy framework level. **Oleg Petrov** of the **World Bank** had once said that Government data is one of the most valuable assets; however, when the data is unused, its value is zero. I couldn't agree more with the sentiment expressed. It is a prudent, and definitive step by the **Government of India** to look at platformisation of the data, and its deployment.

The **National Data Sharing and Accessibility Policy (NDSAP)** in 2012 made India one of the first countries to make its public data open. Besides enabling transparency, open data has the potential to improve public services, increase efficiency and drive innovation and economic growth.

The draft policy is still baby steps but I am sure the big strides will come soon too. We are living in exciting times!

Data Governance Beyond Our Borders

Sanjay Sakalley
Head, Rediffusion FutureTech

Data legislation and policies around the world make for interesting reading. **Lawmakers'** efforts have intensified in the last two years, with many **data protection law initiatives** being passed and adopted. 2022 is likely to continue this trend, with regions such as **Europe,** the **Middle East,** the **United States, UK** and the **Asia Pacific** introducing or amending data privacy and protection laws. By 2023, **65%** of the world's population will have its personal data covered under modern privacy regulations, according to **Gartner.**

Let me take you through all that is happening on this front globally.

EUROPEAN UNION

Since its adoption in 2018, the **EU's General Data Protection Regulation (GDPR)** has become the baseline for a wave of new data protection legislation that has swept the globe. Many lawmakers around the world have sought parity with GDPR in hopes of a positive adequacy ruling from the **European Commission,** which would allow a free data flow between their country and the European market.

When companies need to transfer data to countries that do not have a European Commission adequacy ruling in place, they are obligated to use **Standard Contractual Clauses (SCCs)** for data transfers under GDPR to ensure the rights and freedoms of the EU data subjects are considered and upheld. In June 2021, the European Commission approved new Standard Contractual Clauses (SCCs). The previous set of SCCs was repealed as of 27 September 2021, meaning that all new contracts entered into after that date must use the new SCCs.

Going into 2022, organizations using SCCs have until 27 December to replace all contracts incorporating the old SCCs. This is likely to prove a significant task for many organizations in the year ahead as they will need to not only swap out the old clauses with the new but also to identify which data transfer contracts need to be reviewed and replaced.

Meanwhile in the EU, a new wave of legislation is also due:

- **The Digital Services Act** and **Digital Markets Act,** which "aim to create a safer digital space where the fundamental rights of users are protected and to establish a level playing field for businesses."
- **The Data Governance Act,** which aims to facilitate data sharing.
- The long-awaited **ePrivacy Regulation,** which was originally intended to take effect alongside the GDPR in 2018, and will replace the 2002 ePrivacy Directive (the 'cookie law') and all EU member state laws based on it.
- **The NIS2 (Network and Information Security) Directive,** which will supersede the existing NIS Directive, expanding its scope **"to achieve a high common level of cybersecurity across the member states."**

UNITED KINGDOM

On May 10, 2022, as part of the **Queen's Speech,** the UK government announced its intention to introduce a **Data Reform Bill.** The UK government's background and briefing notes to the Queen's Speech state that the purpose of the Bill is to **"take advantage of the benefits of Brexit to create a world class data rights regime... that reduces burdens on businesses, boosts the economy, helps scientists to innovate and improves the lives of people in the UK."**

The **Bill** will seek to modernize the UK **Information Commissioner's Office (ICO)**, providing it with the power to take **"stronger action"** against businesses that breach data rules, while also requiring the ICO to be accountable to Parliament and the public. The background and briefing notes further state that the Bill will focus on a flexible, **"outcomes-focused"** approach rather than **"box-ticking,"** and will simplify the rules relating to the use of personal data for research purposes, to promote the UK as a science and technology superpower.

The UK government also referred to the UK General Data Protection Regulation ("GDPR") (inherited as a result of the UK's former membership in the European Union) and the **Data Protection Act** of 2018 as **"highly complex and prescriptive"** legislation that imposes excessive administrative burdens on business while providing little benefit to citizens. The UK will nonetheless seek renewal of the European Commission's adequacy decision with respect to the UK upon its automatic expiry in 2025, which is required for personal data to continue to flow uninhibited between the EU and the UK. Any change in the UK's data protection regime that would lower the standard of data protection in the UK may, however, put at risk the UK's status as an adequate destination for personal data under the EU GDPR.

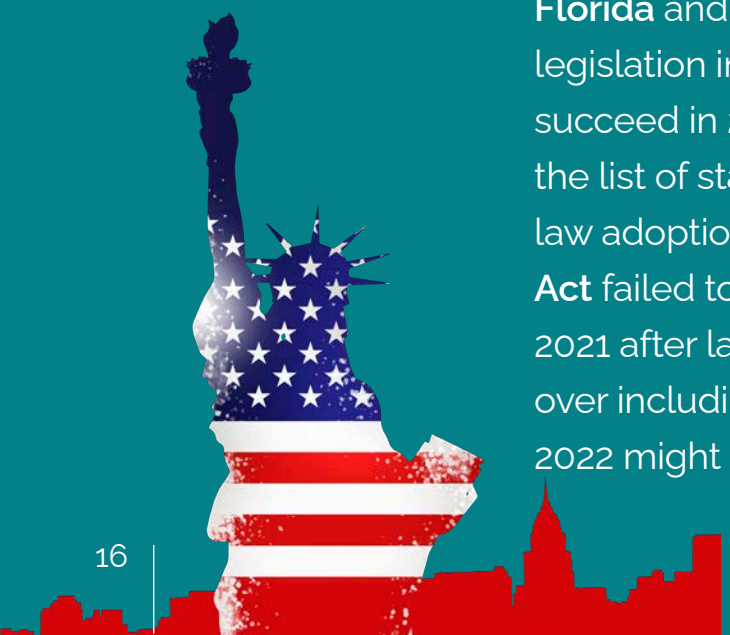
UNITED STATES OF AMERICA

In 2021, more than 160 consumer privacy-related bills were introduced in the US in 38 states, highlighting the growing concern with adopting laws that guarantee the protection of consumers' personal information.

US states **Virginia** and **Colorado** followed in the footsteps of **California** and passed data protection laws set to come into effect in 2023. California itself signed off on several amendments to its **California Consumer Privacy Act (CCPA)** which included changes relating to consumers' right to opt out of the selling of their personal information and authorized agent requests for information concerning consumers' personal information. The amendments took effect the same day they were passed.

The passing of the **Virginia Consumer Data Privacy Act (VCDPA)** and the **Colorado Privacy Act (CPA)** in 2021 is likely to increase momentum in other states and lead to further legislation being passed in 2022.

At least twelve states are set to consider comprehensive consumer privacy legislation in 2022. **Florida** and **Oklahoma** came close to passing legislation in 2021, which might mean they will succeed in 2022. **New York** and **Ohio** are also high on the list of states likely to see progress in data privacy law adoption in the year ahead. **Washington's Privacy Act** failed to be passed for the third year in a row in 2021 after lawmakers could not come to an agreement over including a private right of action into the bill, but 2022 might be the year it finally succeeds.



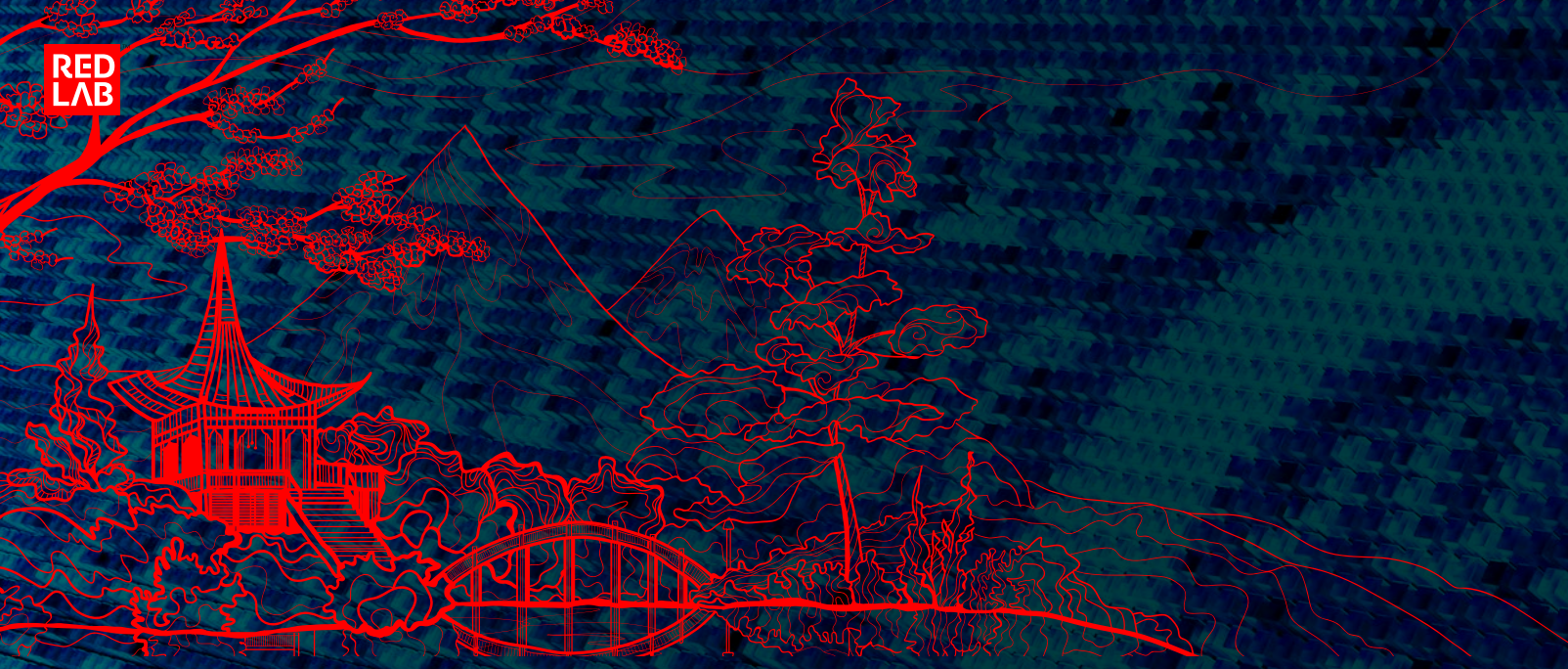
JAPAN

Japan modernized its Act on the **Protection of Personal Information (APPI)** in 2017 to bring it closer to European standards. Thanks to these changes, Japan secured the first adequacy decision issued by the **European Commission** under **GDPR.**

APPI applies to all business operators that handle the personal data of individuals in Japan. This refers to both companies that offer goods and services in Japan and are located within the country and those with offices outside it. Therefore, similarly to the GDPR, Japan's privacy law has an extraterritorial reach.

While the earlier version of the APPI applied only to business operators that had **5,000** identifiable individuals in their database on at least one day during the previous six months, the 2017 amended APPI removed this restriction, broadening its reach to include all business operators that process personal information for business purposes, even those with small databases of a few individuals.

Central government organizations, local governments, independent administrative agencies, and local incorporated administrative agencies, which fall under the scope of other regulations, are exempt from APPI compliance.



Further amendments to the law were enacted on 12 June 2020, based on the results of the **Personal Information Protection Commission's (PPC)** review and public consultation. The new changes, among other things, expanded the scope of Japanese data subjects' rights, made data breach notifications mandatory, and limited the range of personal information that can be provided to third parties. Penalties also saw a significant increase, with corporate entities now liable to fines of up to ¥100 million for violating the PPC's orders.

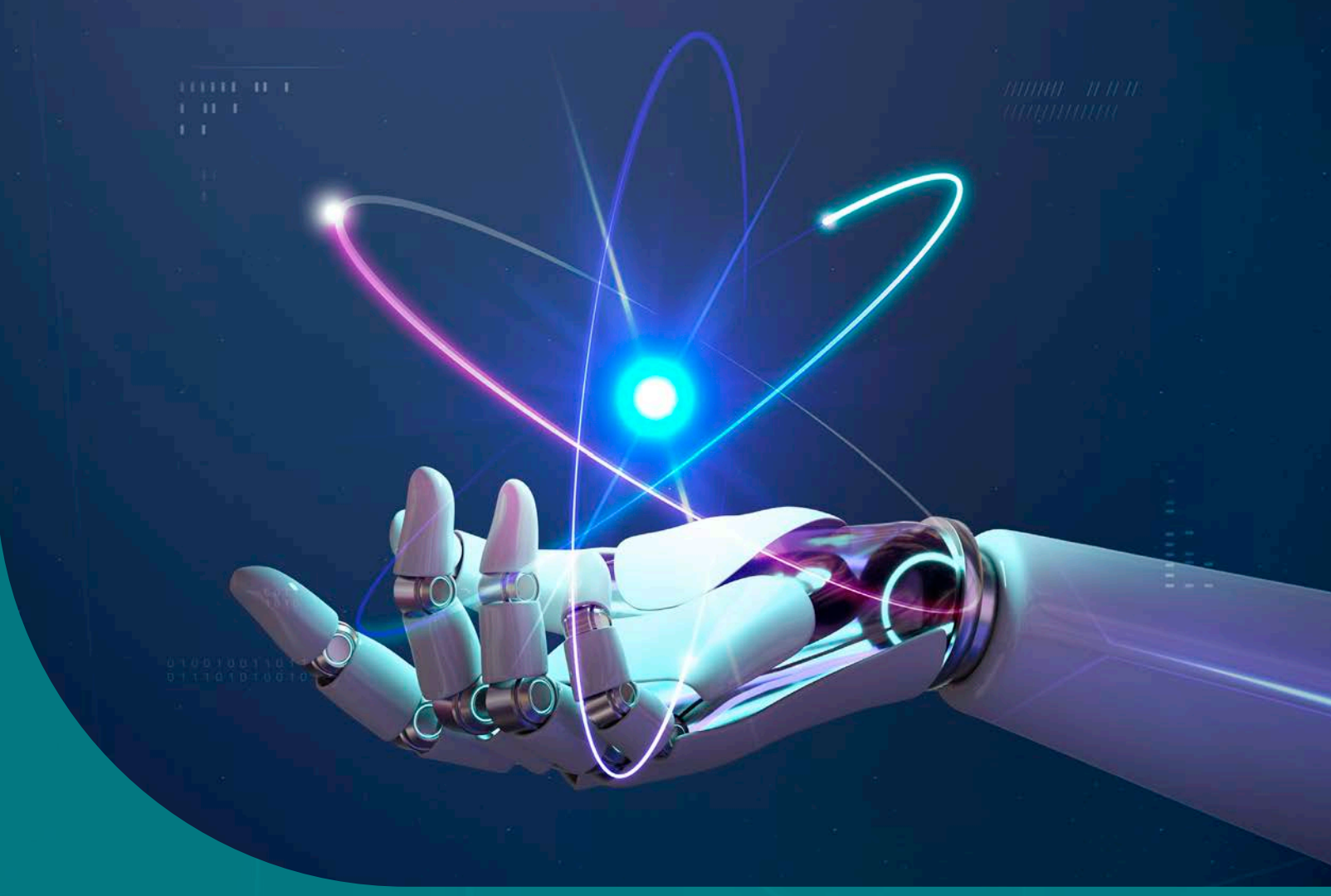
While the new penalties have been applied since 12 December 2020, the rest of the new amendments came into force on 1 April 2022.

SAUDI ARABIA

On 24 September 2021, **Saudi Arabia** adopted its first standalone personal data protection law through **Royal Decree No. M19/1443.** The **Saudi Data and Artificial Intelligence Authority (SDAIA)** is in charge of enforcing the new law that came into force on 23 March 2022 after Implementing Regulations are issued. Companies have one year to comply with the new law's requirements.

For the first two years, the **'competent authority'** responsible for the implementation of the Law will be the Saudi Data & Artificial Intelligence Authority ("SDAIA"). The supervisory function will eventually shift to the **National Data Management Authority ("NDMO"),** which falls under SDAIA, as the data protection landscape develops. Different licensing authorities may be delegated responsibility for the functions of the competent authority in respect of entities in the industry sectors for which they are responsible, although this is unclear.

As the competent authority, SDAIA is required to issue the Regulations prior to the Law coming into effect in March 2022. The Regulations will be developed in consultation with various government entities, including the **Ministry of Communications & Information Technology, the Ministry of Foreign Affairs, the Communications & Information Technology Commission ("CITC"), the Saudi telecoms regulator), the NCA, the Central Bank ("SAMA"),** and the Saudi Health Council.



The Law establishes a requirement for entities outside Saudi Arabia, that are processing personal data of data subjects in Saudi Arabia, to appoint a representative in Saudi Arabia to fulfil their obligations under the Law and Regulations. There is a long-stop date (five years from the law coming into effect), by which time the head of the competent authority must implement this requirement.

The competent authority is expected to educate data subjects, as well as personnel in data controller entities, with respect to rights and obligations set forth in the Law. Data controllers will need to hold workshops for personnel in order to train them on concepts and principles found in the Law, and the competent authority may be called on to provide support in this regard.

UNITED ARAB EMIRATES

The **United Arab Emirates (UAE)** passed its first federal data protection law, **Federal Decree Law No. 45/2021** on the **Protection of Personal Data,** on 27 November 2021. It also established the **UAE Data Office,** responsible for enforcing the data protection law through a separate decree. The new law came into force on **2 January 2022.** However, the **UAE Cabinet** will first need to issue a set of **Executive Regulations** to address the finer details of the law. From the date the Executive Regulations are published onwards, data controllers and processors will have six months to comply with the **Data Protection Law.**

This law imposes criminal liability for data protection violations where the perpetrator does not have authorised access to that personal data, such as hackers. The changes to the **Cybercrimes Law** clarify, strengthen and expand the scope of the earlier cybercrimes law.

One of the key principles of the new UAE data protection law is ensuring transparency in the collection and processing of data. In a move towards harmonisation with **DIFC** and **ADGM** data protection laws, the UAE's new law:

- defines personal data as **'any data related to an identified natural person or a related natural person who can be identified, directly or indirectly, through the linking of data';**

- requires data processing to be conducted in a **fair, transparent and lawful manner;**
- obliges personal data collections to have a clear and specific purpose and be conducted only within the scope of that purpose;
- empowers employees/data subjects to correct any inaccuracies in the data collected;
- requires security measures to safely store personal data and to protect against data breaches or unlawful and unauthorised processing; and
- restricts the storage of personal data once the purpose for collection no longer applies.

In particular, under the new federal data protection law, employees or data subjects have enhanced rights over their personal data. They may request that their personal data is transferred to another controller, that inaccurate information is corrected, and the deletion of personal data in certain circumstances. For example, an employee may request deletion of personal data if it is no longer necessary for the purpose it was collected, consent is withdrawn, or the processing of personal data violates the data protection law.

Elsewhere in the world

2022 is likely to bring the coming into force of several long-expected data protection laws in several countries.

- Following a two-year-long postponement because of the COVID-19 pandemic, **Thailand's Personal Data Protection Act (PDPA)** finally came into effect on **1 June 2022.**
- **Qatar's Data Protection Regulations** and **Data Protection Rules 2021** took effect on **21 May 2022.**
- **Switzerland's** revised **Federal Data Protection Act** was passed by the **Federal Council** in **September 2020** and is expected to enter into force in the **second half of 2022.** However, an official date has not yet been set.
- **China** also passed its first omnibus data protection legislation, the **Personal Information Protection Law (PIPL),** which seeks to protect personal data and regulate its processing, on **20 August 2021.** It came into effect on **1 November 2021.**

There's lots to look forward to: the world is becoming a better informed place.

A REPORT BY

RED LAB™

Rediffusion Consumer Lab

With contributions by Surya Pasricha

redi#usion

MUMBAI (Corporate)
1801 Lotus Corporate Park, Goregaon East, Mumbai - 400063
Ph: +91 22 49311000, +91 22 49312000

KOLKATA
10 Wood Street,
Kankaria Estates,
Elgin, Kolkata - 700016
Ph: +91 33 44066262, +91 33 22871232

CHENNAI
1st Floor, Prakash Building,
14, Deivasigamani Road,
Royapettah, Chennai - 600014
Ph: +91 44 28113426, +91 44 28113427

BANGALORE
22, Vaswani Ashton Woods,
Bellandur Post,
Bengaluru - 560103
Ph: +91 98100 96634

DELHI
Mogae House,
112, Udyog Vihar Phase IV,
Gurgaon - 122015
Ph: +012 42345598