



Gulistan Ladha
Director, Consumer Policy
GSMA

Industry perspective: Challenges for mobile operators

17 April 2024

GSMA - who we are

- Unite 1000+ mobile operators and organisations across the ecosystem and related industries
- Advance innovation and reduce inequalities around the world
- Three broad pillars:
 - Connectivity for Good
 - Industry Services
 - Solutions and Outreach

Website: www.gsma.com

Follow: [@GSMA](https://twitter.com/GSMA)



We provide the world's largest platform to convene the mobile ecosystem at the MWC and M360 series of events

In the Media

Top Data Breaches in 2022 and 2023 Point to Increases in Phishing and Ransomware

December 30, 2023

Africa grapples with surge in digital fraud



8 JUN 2023 NEWS

Cyber Extortionists Seek Out Fresh Victims in LatAm and Asia

The growing costs of cybercrime – a data breach can impact a business for many years to come

Scam alert: Beware of phishing emails that impersonate CBUAE

A fresh round of scam messages were sent to residents in the UAE, impersonating the Central Bank of the UAE

Does Customer Data Privacy Actually Matter? It Should.

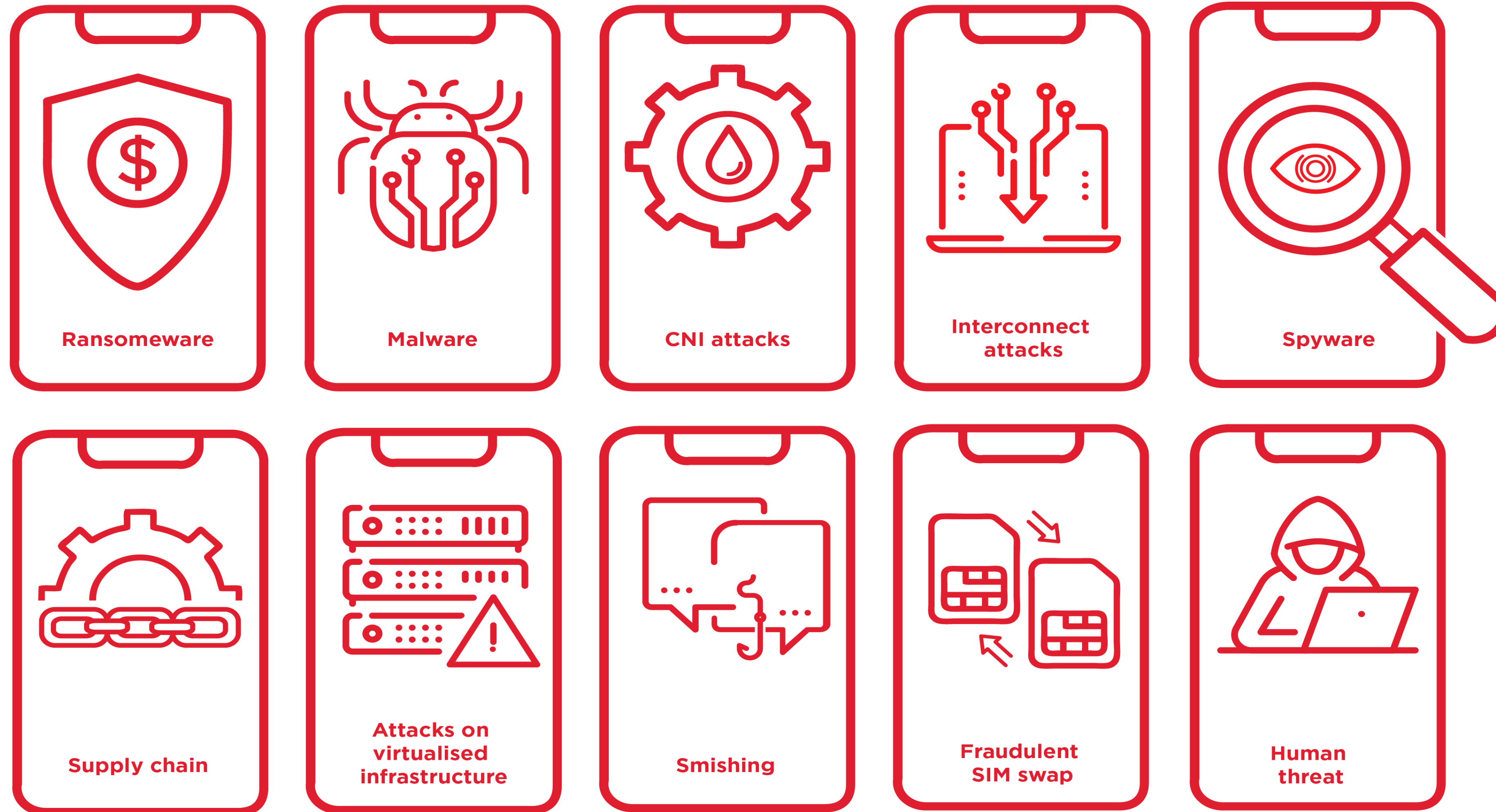
Cyberattacks: You could be the next target

The surge of cybersecurity breaches in India has raised concerns, inviting calls for overhauling weak preventive systems, greater awareness and a stringent legal and regulatory framework

Eastern European Governments Urge Tech Firms To Fight Disinformation

Is ChatGPT a cybersecurity threat?

Global Mobile Security Threats



Source: GSMA report: 'Mobile Telecommunications Security Landscape 2023'

Key Priorities for the Mobile Industry



**Enable safe
and secure
use of
products and
services**



**Test for
vulnerabilities
and deploy latest
technology**



**Comply with
laws and
regulations**



**Educate
customers
and raise
awareness**

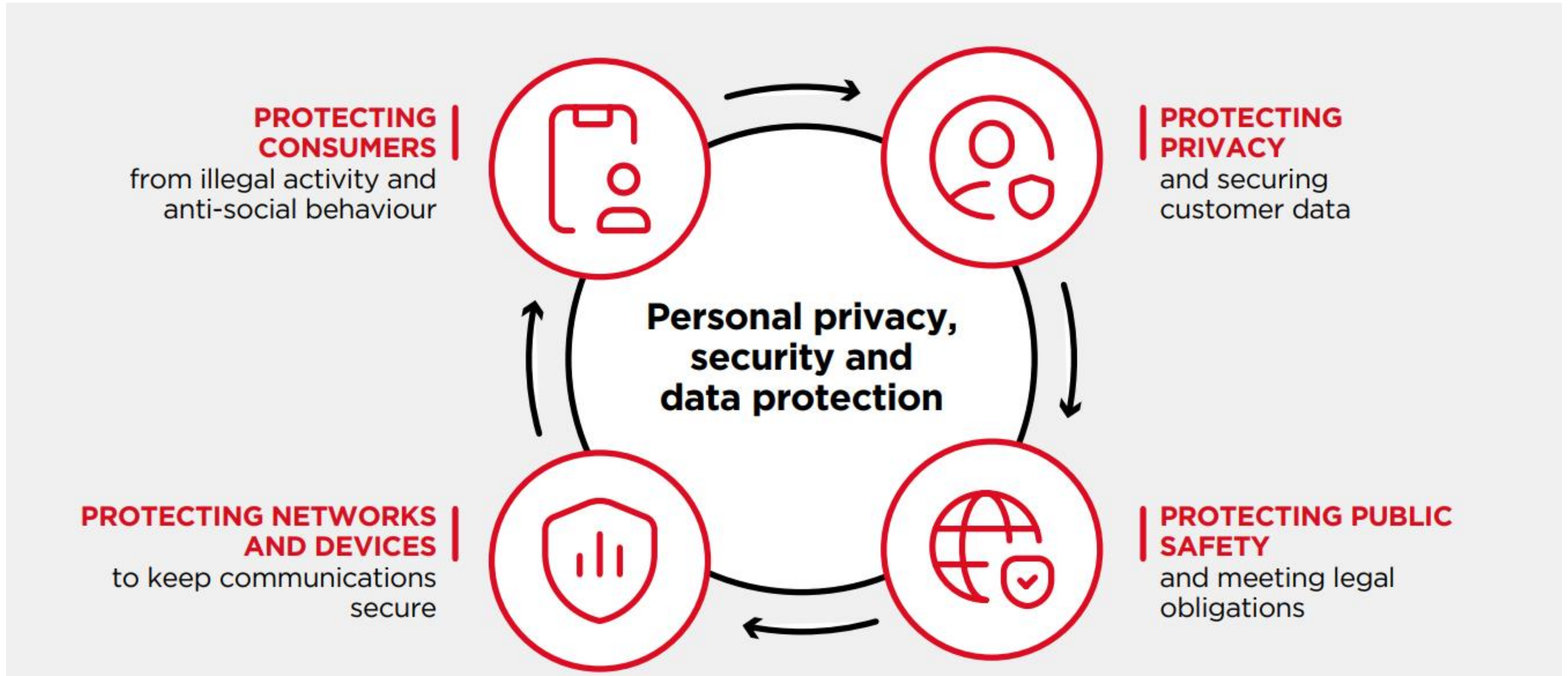


**Share best
practice and
threat
intelligence**



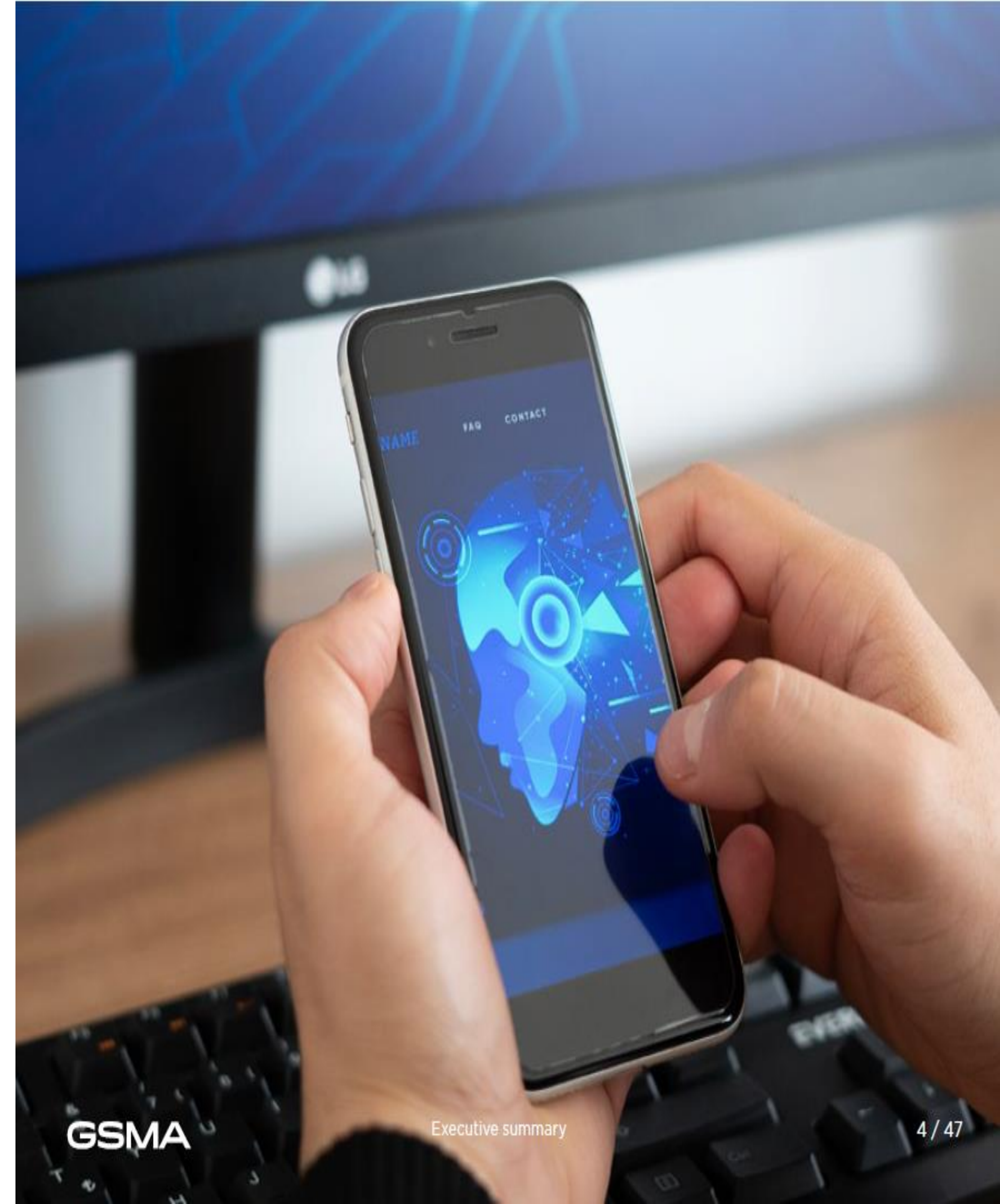
**Collaborate with
stakeholders in
the wider mobile
ecosystem**

GSMA Framework

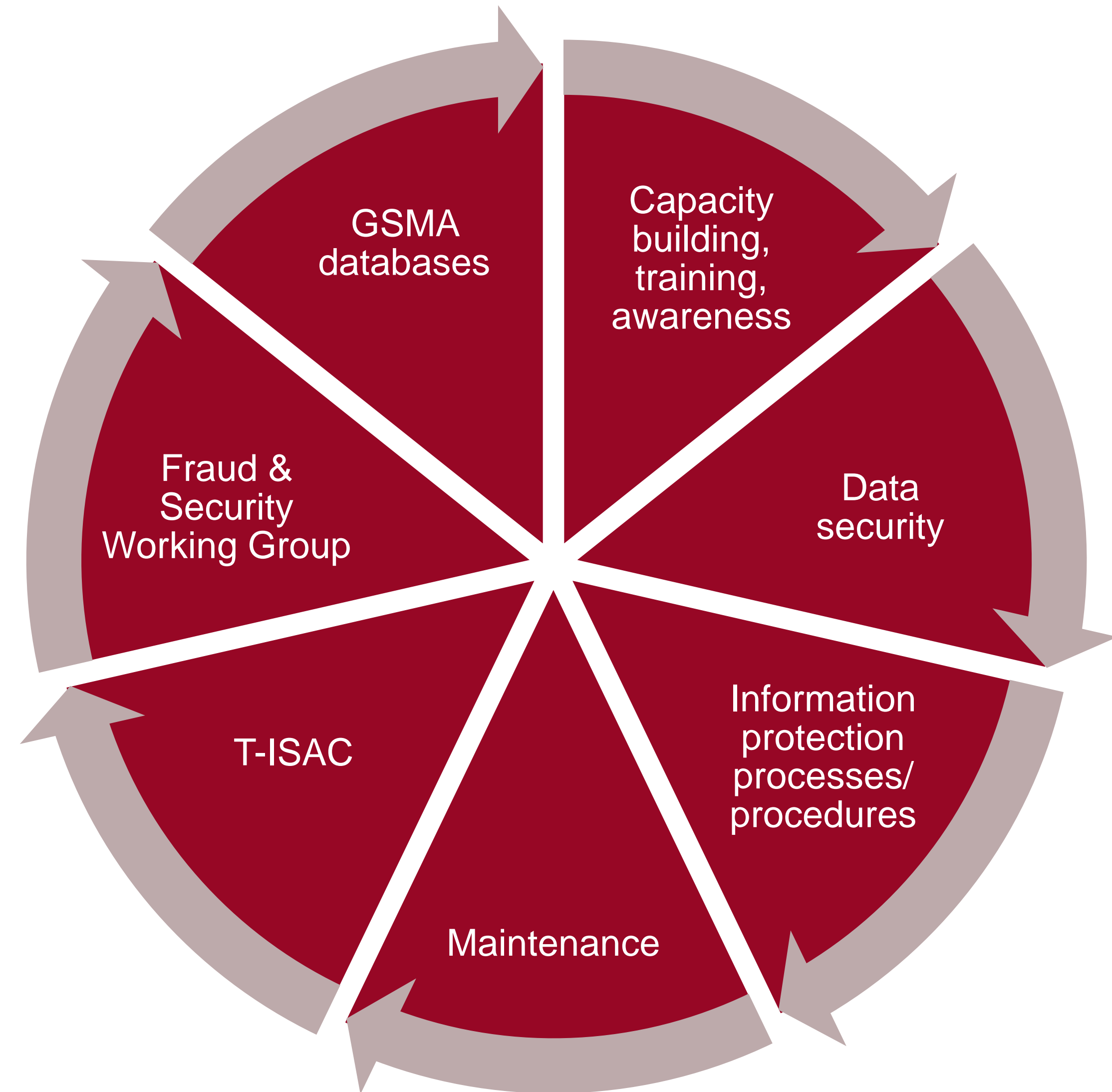


Protect against fraud

- Incorporate 'privacy by design' and 'secure by design'
- Implement best practice cybersecurity frameworks
- Collaborate with industry players to share intelligence
- Proactively educate customers
- Report data breaches and identity theft incidents



GSMA Intelligence Sharing



GSMA Fraud and Security Services

Device Check Device Registry	Coordinated Vulnerability Disclosure (CVD)	Type Allocation Code system (TAC)
eUICC Security Assurance (eSA)	Network Equipment Security Assurance Scheme (NESAS)	Security Accreditation Scheme (SAS)

GSMA Member Initiatives



Telecommunication Information Sharing and Analysis Center (T-ISAC)

- A central hub of information sharing for the telecommunication industry



Fraud and Security Group (FASG)

- Fraud and security intelligence-sharing for mobile operators



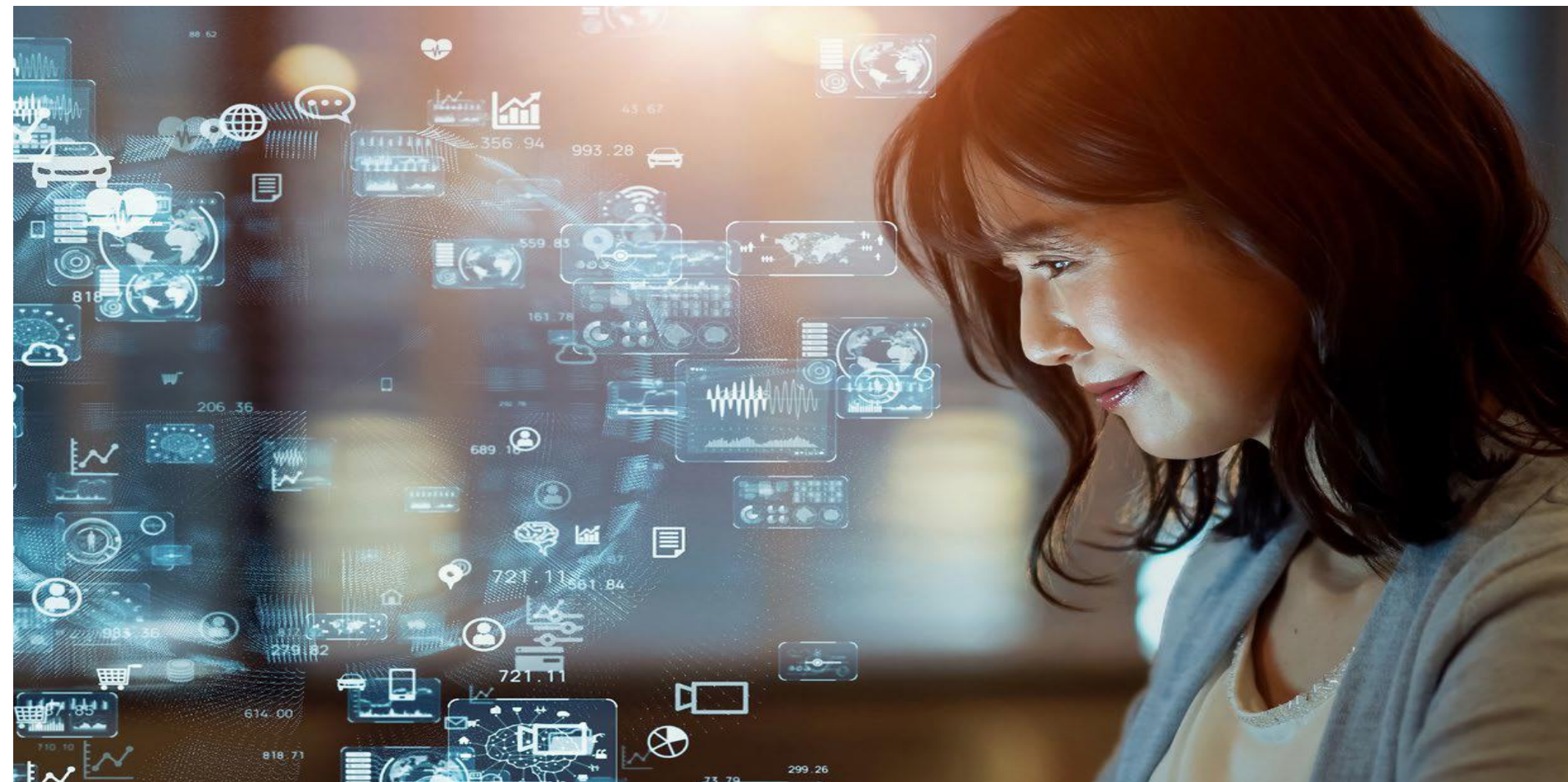
Industry can't do it alone

Promote skills training

- Increasing awareness among mobile customers
- Building digital skills by including cyber skills and Internet safety considerations

Protect the public from online harms

- Multi-stakeholder efforts needed to encourage safe and responsible use of mobile-based online services and devices
- Legal frameworks, resources and processes should be targeted at criminal behaviour



Smart data privacy laws and Implementation



GSMA

Smart Data Privacy Laws

Achieving the Right Outcomes for the Digital Age

Copyright © 2019 GSM Association



Introduction

Sensing the huge opportunity of digital transformation, governments are seen to establish a regulatory environment that supports data-centric economic policy while strengthening trust in technology. Many countries are therefore considering data privacy laws for the first time, while others are re-examining their existing approaches.

Organisations' use of personal data can no longer be contained or regulated in isolation within a single country. The future frameworks that will allow governments, businesses and, most importantly, individuals to benefit from the data revolution must respect national laws, traditions and cultures, but they must also coalesce around an emerging consensus that horizontal data privacy laws should protect the privacy of individuals while enabling efficiency and innovation.

This paper provides a guide for those involved in drafting and reviewing data privacy rules or legislation – distilling what has been learned from data privacy law implementation to date into guiding principles by which a proposal can be measured.

In brief, for a data privacy law to be successful, it must provide effective protection for individuals while allowing organisations the freedom to operate, innovate and comply in a way that makes sense for their businesses and can secure positive outcomes for society. The law should be guided by principles that put the responsibility on organisations to identify and mitigate risks while remaining flexible, technology- and sector-neutral and allowing data to move across borders easily.

Without these guiding principles, there is a serious risk that the resulting law or regulations will end up being too prescriptive, too rigid and too rapidly outdated. Conversely, if these guiding principles are adopted to, all stakeholders can win: organisations can prioritise their resources to achieve effective privacy outcomes while operating and innovating responsibly; supervisory authorities can target their resources to focus on prevention of harm; and governments and individuals can enjoy the economic and societal benefits of digital transformation safely.

An individual's privacy should be at the heart of any smart data strategy. People must be able to trust the data-driven businesses, governments and digital ecosystems that they engage with on a daily basis. If individuals trust the organisations that use their data, then governments and industries, including the mobile industry, can benefit through greater uptake of new technology and business ideas, increased economic activity and a thriving, digitally enabled population.

To achieve this, a smart approach to data privacy is needed, comprising four key areas:

- **Data privacy law** that empowers and protects individuals and encourages innovation to benefit society
- **Organisations with privacy practices** that focus on the minimisation of risk of harm to individuals
- **Supervisory authorities** that are able to prioritise their functions and resources to target the most pressing risks of harm – educating individuals and business, encouraging good practice and enforcing appropriately
- **Individuals** who are equipped with the information and tools they need to make informed choices about how their data may be used and to understand the value exchange they are engaged in

This paper focuses on the first of those areas and is intended as an aid to those who are involved in drafting or reviewing proposed rules relating to data privacy. It considers the drivers for and advantages of general data privacy laws and then sets out some guiding principles aimed at ensuring effective privacy outcomes for governments, organisations, society and, most important, individuals.

Risk-based

General data privacy laws should focus on the risk of harm to individuals. Obligations or duties that do not focus on the risk of harm result in checkbox approaches to compliance that bring little value to individuals and undermine the credibility of the law. For example, a requirement to consult the data protection authority whenever a certain type of data or technology is used does not take into account the context of the processing or the safeguards put in place by the organisation. It would therefore impose an unnecessary burden on organisations and it would swamp data protection authorities with unnecessary consultations. A risk-based approach would require an organisation to carry out its own risk assessment; to the extent consultation with the authority is included in the framework, it would be obliged to consult the authority only in exceptional circumstances. The same philosophy should be applied throughout the data privacy law.

A risk-based approach would also include the concepts of privacy-by-design and data privacy impact assessments. Privacy-by-design requires organisations to identify and mitigate risks throughout the lifecycle of a product, service or process. Data privacy impact assessments are a mechanism used by organisations to evaluate the impact on individuals of certain high-risk processing activities. It may be desirable to have these practices mandated by law, as they enable tailored approaches to privacy protection rather than a one-size-fits-all approach. This prevents the need for more prescriptive provisions set out in law.

Horizontal (sector- and technology-neutral)

General data privacy laws usually apply to any processing of personal data, regardless of sector or the technology used. This represents a positive for consumers, as it gives them a consistent level of protection without having to worry about what technology they are using, or whether the activity they are engaged in has specific rules or not.

A horizontal approach benefits all organisations that make use of personal data and defines a common baseline in the data economy, providing clarity and facilitating competition for all participants.

The introduction of a horizontal general data privacy law provides a useful opportunity for governments to review legacy sectoral rules. This is of particular relevance in the communications sector, which has always had a concern for privacy at its core. With communications now being possible over the internet and, increasingly, between objects connected to a variety of networks, a general data privacy law can provide the common rules that everyone must follow. A beneficial consequence of this is that redundant legacy rules concerning privacy in sectoral laws, guidance or telecom licence conditions can be reviewed and removed to avoid confusion.

In a modern, digital world, personal data should be subject to the same protections, regardless of whether it is collected via a website, a mobile application, a connected device, a retail establishment or a communications provider.

A smart data privacy law should:

- Adopt a risk-based approach throughout
- Ensure each provision targets the risk of harm to individuals
- Include privacy-by-design and privacy impact assessments

A successful data privacy law should:

- Apply horizontally to any processing of personal data regardless of the sector or the technology used
- Provide a common baseline for all actors in the digital ecosystem and data-driven economy
- Provide an opportunity for governments to review legacy privacy rules in sectoral laws, guidance or telecom licence conditions and, where possible, to remove them

Resource for Policymakers

When drafting, reviewing Or Implementing data privacy laws

Cuts through complexity

GSMA Smart Privacy Laws – full version

Latin America

Challenges

- Social engineering - phishing and malware (Argentina, Brazil, Chile, Colombia, Mexico, Peru)
- In Mexico and Guatemala - over 70% of mobile owners not using mobile internet reported safety and security concerns as an important barrier
- 38% in Mexico reporting it as the top barrier



Latin America



- Anatel's website contains information on the most common scams and how to prevent them

- FTC cooperation agreement with consumer protection authorities of Chile, Colombia, Mexico and Peru to combat unfair, deceptive and fraudulent practices

- Telefonica: Global Security Regulatory Framework and ISO22301 or ISO27001 certification in Argentina, Brazil, Ecuador and Peru (Colombia has SGI de Movistar)

Sub-Saharan Africa

Challenges

- M-Pesa fraud through social engineering
- Low consumer financial literacy rates
- 31% of mobile money account holders cannot use their account without help
- In 2022 South Africa saw 24% surge in reported digital banking fraud incidents (SABRIC)
- Theft of over R740 million from victims attributed to increasing fraud cases related to banking applications and online banking



Sub-Saharan Africa

Mozambique

- Collaboration between government authorities, mobile operators, internet service providers and financial institutions
- Standardised procedures for subscriber registration
- Central database for subscriber identification
- Risk centre to detect fraudulent activities
- Signatory to Malabo Convention



Operator Gateway Initiative

- Launched in 2023
- Standardises APIs by Mobile Network Operators
- Enhances security measures within banking applications and online banking platforms
- Implements robust fraud detection and prevention mechanisms
- Increases overall resilience of digital banking systems against cyber threats



Latin America

Brazil

- Claro, TIM and Vivo became the pioneer for GSMA Open Gateway
- Launched three anti-fraud network services: Number Verify / SIM Swap / Device Location.
- In March Claro recorded 3 million requests/month for the SIM Swap API



Sub-Saharan Africa

- Number Verify and SIM Swap APIs available in South Africa
- Help combat fraud and digital identity theft in sectors including banking / finance / insurance / retail
- Mobile operators are strategically placed to work with developers to help banks, financial institutions and commerce providers mitigate the risk and protect their customers





Thank you