DENTONS HPRP

Grow | Protect | Operate | Finance

Indonesia Launches eSIM Regulation: What It Means for Telecom Providers and Users

Prepared by:

Andre Rahadian (Partner), Mika Isac Kriyasa (Partner), and Steven Feriyanto (Associate)

On 11 April 2025, the Indonesian government took a significant step in modernizing its telecommunications landscape with the issuance of Regulation of the Ministry of Communication and Digital Affairs No.7 of 2025 (**MoCDA Reg. No. 7/2025**"), which was enacted on 10 April 2025 and took effect upon its promulgation according to Article 16. This regulation introduces a formal legal framework for the implementation of Embedded Subscriber Identity Module (eSIM) technology in Indonesia.

Designed to support the growth of next-generation connectivity, including Internet of Things (IoT) and machine-to-machine (M2M) communications, MoCDA Reg. No. 7/2025 lays down compliance requirements and technical standards that will govern how eSIM technology is deployed by both mobile cellular and mobile satellite network providers ("Providers") in Indonesia.

A Milestone in Digital Infrastructure

The adoption of eSIM technology is expected to enhance digital integration, enable device portability, and improve the overall security of telecommunications systems. Unlike traditional SIM cards, eSIMs are embedded within a device and can be remotely provisioned, offering significant benefits in terms of scalability, convenience, and data security.

In the context of IoT, eSIMs allow devices to interact and be controlled remotely, enabling real- time communication between connected systems such as smart meters, autonomous vehicles, surveillance equipment, and industrial machinery. This facilitates automatic data exchange between machines (M2M communication), eliminating the need for manual reconfiguration or physical SIM replacement—particularly important in hard-to-reach or high-volume deployments. As such, eSIM technology is critical for the future of remote device management and the automation of data- driven systems.

From a policy standpoint, this development aligns with Indonesia's broader ambition to build a secure, interconnected, and forward-looking digital economy. MoCDA Reg. No. 7/2025 underscores that eSIM implementation must also reinforce protections against digital threats such as spam, phishing, and identity fraud, while ensuring robust compliance with personal data regulations.

However, the very features that make eSIM attractive, such as remote access, seamless integration, and continuous data transmission, also introduce data security and privacy risks. The automatic collection and transfer of data between devices can expose sensitive information if not properly encrypted or secured. Unauthorized access or misuse could lead to serious issues, including identity compromise or other forms of data exploitation. Recognizing this, the regulation mandates that Providers implement strong encryption protocols, access controls, and audit mechanisms to ensure that data processed via eSIM-enabled devices remain secure and compliant with prevailing laws, including Indonesia's Personal Data Protection Law.

Key Compliance Obligations for Telecom Providers

To facilitate a secure and standardized transition, the regulation outlines seven core obligations that must be met by Providers intending to implement eSIM-based services:

1. **Provisioning System**
   Providers must establish and operate systems capable of managing local International Mobile Subscriber Identity (IMSI) numbers[1] and securely storing eSIM profiles.[2]
2. **Data Security and Certification**
   All eSIM provisioning systems must comply with data security accreditation schemes, covering encryption, personnel access, and network protections.[3]
3. **Standard Operating Procedures (SOPs)**
   SOPs must be adopted to safeguard customer data, personal information, and confidential communications in accordance with applicable laws.[4]
4. **Customer Registration**
   Providers must ensure that customer registrations comply with identity verification requirements and legal mandates for data integrity.[5]
5. **Subscription Management**
   Providers must operate subscription management systems utilizing both *Mobile Station International Subscriber Directory Numbers* (MSISDN, the phone numbers assigned to mobile users) and local IMSI numbers to support seamless service activation.[6]
6. **Third-Party System Requirements**
   If Providers collaborate with third-party provisioning vendors, those entities must be registered as *Electronic System Operators* (PSE) and comply with relevant standards.[7]
7. **Mandatory Reporting**
   Providers using MSISDN numbers for IoT/M2M services must report such utilization to the Directorate General of Digital Infrastructure by 11 October 2025.[8]

Sanctions for Non-Compliance

MoCDA Reg. No. 7/2025 provides for administrative sanctions against Providers and third parties that fail to meet their obligations. These include:

- **Written warnings** (up to three times within 30 working days each), and
- **Public disclosure** of violations on the Ministry's official website if non-compliance continues.[9]

Breaches related to customer registration, data protection, or numbering requirements may also trigger sanctions under applicable laws.[10]

Transition Period: April 2025 to April 2027

To facilitate industry adjustment, the regulation establishes a two-year grace period for Providers that are currently utilizing or intend to adopt eSIM technology. By 11 April 2027, all relevant systems, infrastructure, and operational protocols must be fully compliant with MoCDA Reg. No. 7/2025.[11]

This period offers Providers an opportunity to:

- Conduct compliance audits
- Review provisioning infrastructure
- Certify their systems under approved security frameworks
- Update internal policies and customer registration processes
- Reassess third-party partnerships and vendor contracts

Accreditation and Security Compliance

MoCDA Reg. No. 7/2025 places a strong emphasis on security accreditation. Provisioning systems and embedded UICCs must meet certification standards that cover:

- Information and physical security
- Key management and sensitive data handling
- Network infrastructure integrity
- Personnel and organizational controls
- Remote SIM provisioning safeguards

Providers are responsible not only for implementing secure systems but also for ensuring that third-party vendors meet the same standards if they are involved in provisioning operations.[12]

[1] Article 2(2)(a)
[2] Article 2(2)(d)
[3] Article 2(2)(g)
[4] Article 2(2)(f)
[5] Article 153 MCI Regulation No. 5 of 2021
[6] Article 2(3), Article 2(4)
[7] Article 3
[8] Article 11(a)
[9] Article 12
[10] Article 2(3)
[11] Article 14(2)
[12] Article 6

Strategic Considerations for Telecom Stakeholders

As the regulation comes into effect, telecom Providers operating in Indonesia will need to balance innovation with regulatory compliance. While the benefits of eSIM technology (such as greater efficiency, device flexibility, and operational scalability) are clear, the pathway to full adoption requires significant technical preparation, legal review, and security enhancement.

Key strategic actions for Providers may include:

- Mapping current infrastructure and identifying compliance gaps
- Engaging in early discussions with technology partners and vendors
- Reviewing customer onboarding procedures in line with regulatory standards
- Preparing documentation for PSE registration and MSISDN reporting

With eSIM technology likely to play an increasingly central role in consumer mobile services, industrial automation, smart cities, and digital identity frameworks, the decisions made during this transition phase may have lasting implications for competitiveness and regulatory standing.

* * * * *

MoCDA Reg. No. 7/2025 marks more than a technological shift, it reflects Indonesia's continued push toward a secure, standards-based digital ecosystem. For Providers, this is a timely opportunity to re-evaluate existing systems, adopt best practices, and future-proof their services in a fast-evolving connectivity landscape.

As the deadline for compliance approaches, clarity, preparation, and attention to regulatory detail will be essential to ensure a smooth and successful transition.

Looking ahead, the effective implementation of MoCDA Reg. No. 7/2025 could position Indonesia as a regional leader in digital connectivity and regulatory modernization.

How We Can Help

With the enactment of MoCDA Reg. No. 7/2025, telecom providers face a wide range of legal, technical, and compliance challenges. Our firm offers comprehensive advisory and regulatory compliance support tailored to the needs of telecom operators, equipment vendors, and technology partners navigating the new eSIM landscape.

We can assist with:

- **Regulatory Gap Assessments**: Evaluating current systems and policies against the new obligations set by MoCDA Reg. No. 7/2025.
- **Licensing and PSE Registration**: Advising on Electronic System Operator (PSE) registration and related licensing requirements for local and foreign providers.
- **Vendor and Contractual Review**: Reviewing and drafting agreements with third-party vendors to ensure they comply with provisioning and security obligations.
- **Customer Onboarding and Data Protection Compliance**: Aligning registration processes with identity verification and data privacy regulations, including the Personal Data Protection Law.
- **Security Accreditation Support**: Guiding clients through certification processes for provisioning systems, including alignment with international security standards.
- **Reporting and Audit Preparation**: Assisting with mandatory reporting obligations (e.g., MSISDN usage for IoT/M2M) and preparing for regulatory audits.
- **Strategic Advisory**: Supporting digital transformation strategies and helping providers future-proof their compliance and infrastructure investment plans.

Our team combines deep knowledge of Indonesian telecommunications law, digital infrastructure regulation, and cybersecurity frameworks. We stand ready to help industry stakeholders turn compliance requirements into opportunities for strategic growth and operational excellence.

- o0o -