Data Law Alert

Data Law



IT-Wallet and Cold Chain Cybersecurity

No.23 Issue 2026

Legance

Italy sets mandatory privacy safeguards for the IT-Wallet ecosystem

IT-Wallet is Italy's digital wallet system, designed to let users hold and present verified information about their identity and other personal details in digital form. The ecosystem brings together the organizations providing wallet solutions, those issuing credentials and those checking them to deliver a service. On 4 November 2026, the Italian Government announced the publication of the **Decree of the Head of the Department for Digital Transformation** (the "**Decree**") dated 29 September 2026, defining the technical and organizational measures applicable to personal data processing within the system, pursuant to Article 8(5) of the Prime Minister's Decree of 19 March 2026. The Decree makes the measures identified as mandatory in the IT-Wallet Technical Specifications a **minimum mandatory baseline**, rather than an exhaustive compliance checklist. Each participant remains responsible for its own processing and must adopt additional safeguards where its specific activities or technical configuration require them.

The rules apply to both public and private participants acting as controllers or processors, including wallet providers, credential issuers, verifiers and aggregators. **Participation does not give an organization the same privacy role for every activity**: the role depends on the particular processing, its purposes and the decision-making powers exercised. The safeguards cover data minimization, privacy by design and by default, limited retention, security and the logical separation of wallet data from other processing. They also require **measures to prevent unauthorized tracking or correlation of users' transactions and behavior**, while **preserving the traceability needed for security checks and incident management**. Where special categories of personal data are involved, enhanced safeguards must include selective, logged access and protection against unauthorized profiling or further processing.

Before providing a service through IT-Wallet, verifiers must document which attributes they request, why those attributes are necessary and proportionate, the applicable legal bases, retention periods and safeguards against excessive requests or incompatible further processing. The system-level data protection impact assessment provides a common reference, but participants must still assess, under Article 35 of Regulation (EU) 2016/679 (the "**GDPR**"), any additional, specific or local processing not covered by it, as well as changes to their processing that are likely to result in a high risk to individuals' rights and freedoms. Participants must also retain evidence of their decisions, periodically check the effectiveness of safeguards, train authorized staff and coordinate the handling of security incidents and personal data breaches. Organizations integrating the IT-Wallet should therefore define their respective responsibilities, document the data required for each service and establish procedures for retention, user requests and incident handling.

ACN warns food retailers and logistics operators as cold chain attacks reach Italy

On 3 November 2026, the Italian National Cybersecurity Agency ("**ACN**") **warned of cyberattacks affecting cold chain systems**, meaning the systems supporting temperature-controlled storage and distribution, **across several European countries**. Following earlier incidents involving French supermarket chains, the agency renewed its recommendations to food retailers, food logistics operators, industrial refrigeration businesses and maintenance providers. The warning also concerns Italy: ACN reported receiving a notification under the Network and Information Security (NIS) framework from a collective catering company in Tuscany and detecting an attack, not yet notified at the time of the announcement, against a frozen-food producer in Emilia-Romagna. The agency also intensified monitoring to identify further possible attacks.

The immediate priority is to check, with the utmost urgency, **whether control and remote-support systems are exposed to the internet** and **to segregate them within protected environments separated from corporate IT networks**. ACN also recommends **strengthening remote access through virtual private networks (VPNs) and multi-factor authentication**, checking privileged accounts and updating or replacing devices no longer supported by their manufacturers. These recommendations reach beyond conventional office IT: they expressly concern the systems used to control and remotely maintain refrigeration infrastructure, making the involvement of equipment operators and external maintenance providers particularly important.

Data Law Alert

Data Law



For further information, please contact:

Andrea Fedi
afedi@legance.it

Lucio Scudiero
lscudiero@legance.it

Martina Balzani
mbalzani@legance.it