Europol Calls for Stronger Data Laws to Combat Cybercrime

Criminals are exploiting encryption, anonymization and new technologies faster than regulators and law enforcement can adapt, creating a critical challenge in accessing data for investigations. This warning was delivered at Europol s 4th Annual Cybercrime Conference 2025, held last week at Europol headquarters in The Hague. The event gathered around 500 participants from across the world to examine one of the central dilemmas in modern law enforcement:
how to balance lawful access to data with the protection of privacy and digital rights.
At this year s Cybercrime Conference, we are confronting one of the defining dilemmas of our time: data as both a driver of innovation and the lifeblood of modern criminality, said Europol executive director, Catherine De Bolle. When digital evidence remains out of reach, children go unidentified, terrorist plots advance undetected and organized crime thrives in the shadows. EU Commissioner Calls for Stronger Cooperation Magnus Brunner, European commissioner for internal affairs and migration, delivered the keynote address, emphasizing the urgency of a coordinated European response. Cybercrime knows no borders, Brunner said. To protect people and businesses in the EU, we must mainstream security into all our policies, strengthen Europol s mandate and ensure lawful access to data. Under the theme Dissecting data challenges on the digital frontlines, the two-day event explored how the growing volume of digital information is reshaping cybercrime investigations and regulatory debates.
Read more on Europol s cybercrime initiatives and data access strategies: Europol Creates Violence-as-a-Service Taskforce Key Issues and Operations Highlighted Delegates examined five critical areas shaping today s cyber landscape: Balancing access and privacy in daily life and global strategy Improving cross-border data sharing through partnerships Updating laws to match rapid technological change Promoting cyber diplomacy between governments and industry Developing prevention strategies based on emerging technologies The conference

featured case studies such as Operation Eastwood, which disrupted pro-Russian hacktivist activity targeting European infrastructure, and Operation Ratatouille, which led to the arrest of a suspected administrator of a major Russian-speaking cybercrime platform. Strengthening Digital Resilience The conference followed a workshop with national Computer Security Incident Response Teams (CSIRTs), co-organized with the European Union Agency for Cybersecurity (ENISA). The session emphasized technical cooperation and information sharing between national and European bodies. Now in its fourth year, Europol s Cybercrime Conference has become a space for policymakers, investigators and industry representatives to exchange perspectives on cyber-threats, legal frameworks and the broader implications of data access in an interconnected world.