Global Threat Intelligence Report

Featuring Regulatory Insights

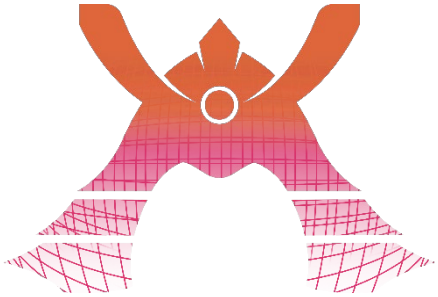
Volume 9 - January 2026

KDDI Europe

Cover Image: © Stuart Robertson (Senior Applications & Infrastructure Engineer, KDDI Europe). Photograph used with permission.

Table Of Contents

Introduction



Welcome to the Threat Report. The purpose of this document is to provide an overview of the latest cybersecurity threats, trends and regulations that could impact organisations worldwide. By analysing recent incidents and emerging threats, we aim to equip our team and customers with the knowledge and insights necessary to proactively defend against potential attacks.

At KDDI Europe, our dedication to protecting our clients and their systems is unwavering. We are continuously investing in security technologies and training our staff to enhance defences and respond swiftly to any threats. We are deeply committed to ensuring that our customers are protected in accordance with the highest standards of cybersecurity.

It is our belief that our success is linked to the success of our customers' businesses. By safeguarding your operations, we aim to provide a secure environment where your business can thrive and grow. Thank you for taking the time to review this report.

News

The Latest Cybersecurity news

ServiceNow to acquire Armis [1]

ServiceNow is acquiring Armis so that it can enter the cyber-physical security market and expand on cyber exposure management on their ServiceNow AI platform. This acquisition will cost ServiceNow $7.75 billion under the terms of the definitive agreement and in return it is expected to triple ServiceNow's market opportunity for security and risk solutions.

DDoS Attack disrupts France's Postal Service [2]

On Monday, the 22nd of December 2025, the national postal operator in France and it's banking division were on the receiving end of a cyber-attack with resulted in the unavailability of online services. Customers were reportedly turned away as service was unable to be provided with service and no group has yet claimed responsibility for the attack. This attack follows another which was targeted at the French Interior Ministry which occurred just days earlier.

Threat Insights

Why are DDoS Attacks Still Occurring?

A Distributed Denial-of-Service (DDoS) attack is one that uses incoming traffic from multiple hosts to flood a victims' network to make a resource unavailable thus disrupting a service. A simple analogy for this would be if someone booked all the tables in a restaurant for an entire evening and never showed up. The business would suffer financially because it would be unable to provide its services and legitimate customers would also be unable to patronise the restaurant.

The first attack of such a nature occurred in the 1996 and almost 30 years later, Denial-of-Service attacks are still used. Surely if we understand exactly how it occurs then we should have a permanent solution for preventing this attack and it should be a think of the past.

In this section we explore some reasons behind its continued existence despite the multitude of protective solutions, hardening techniques and awareness that exist surrounding DDoS attacks.

1. **Ease and efficiency**. The simplest reason for the continued use is that DDoS attacks are simply effective while at the same time easy to execute. The logic is straightforward, first, send an overwhelming amount of traffic to a network using tools that are already easily obtained on the internet, this prevents access resources on that network, then make a demand or release a statement to explain your motivation for doing so. This may be an oversimplification, but it is how an attack would work, is not difficult to understand and it works if proper safeguards are not in place.
2. **The commoditisation of DDoS**. Individuals with little skill and experience can purchase services that allow them to conduct DDoS attacks. The financial incentive to the service provider coupled with the nefarious intentions of the buyers of such services are the driving forces behind this supply and demand.

3. **The Internet of things (IoT)**. As the number of devices with internet connectivity increases, so does the number of improperly secured devices. The average home user may not possess the skills or knowledge required to properly secure their IoT devices and others may not even bother changing the default usernames and passwords. If an IoT device is running some version of Linux or an OS that supports networking and remote commands, then it can be used as part of a botnet to conduct DDoS attacks. Meaning attacks will have a continuous supply of devices to recruit for DDoS attacks.
4. **Faster Internet and networks speeds**. Speeds are faster now than they have ever been so more data can be sent in a shorter time. For example, over a 50 Mbps connection, you can send approximately 250,000 standard 1500-byte packets in one minute from a single device. However, since DDoS attacks use smaller byte packets, a larger number of packets can be sent. So, assuming the average botnet is made up of a few thousand devices we can imagine how much traffic can be sent and why it appeals to threat actors.
5. **Social consciousness and political motivations.** State actors and hacktivists have reasons likely extending beyond financial gain for wanting to cause the unavailability of a service. With current political tensions between countries and strong socially conscious movements it is clear why this method of attack would be of interest to threat actors, it allows them to disrupt services they believe are harmful to their nations interests or ideology.
6. **High cost of DDoS protection solutions**. For mid-market or enterprise level solutions such as Azure DDoS protection or AWS Shield Advanced, depending on the number of public IP addresses and networks that require protection, these can start from around $3,000 monthly. Prices like these can make it difficult for the wide adoption of DDoS prevention solutions.

Unfortunately, DDoS attacks may continue to exist while the points stated remain valid. In the meantime, best practices can be observed, and organisations can use the tools that they can afford to combat DDoS attacks.

Regulatory Insights

A Look Back at 2025 – How Cyber Security Laws across Europe Are Raising the Bar on Resilience, Data Governance and Accountability

With 2026 now underway, the EU and UK cyber regulatory landscape is still experiencing one of its most significant periods of transformation since the GDPR came into force. Governments are tightening rules, regulators are expanding their reach, and courts are redefining the boundaries of digital rights and liabilities. For businesses and individuals alike, 2026 will be a year of materially higher compliance expectations, greater exposure to regulatory enforcement, and a more mature ecosystem for incident preparedness across Europe.

KDDI has identified **5 major cyber security legislative developments in 2025 and their potential impact for the year ahead.**

1. The EU Digital Operational Resilience Act (DORA): a unified EU supervisory approach for ICT risk management in the financial sector.[3]

The entry into force of DORA on **17 January 2025**, marked a major regulatory shift for the financial sector. For the first time, banks, insurers, investment firms, and critical ICT providers were subject to a harmonised, EU-wide framework for digital resilience - from incident reporting to third-party risk oversight. Regulatory clarifications issued by supervisory authorities (EBA, ESMA, EIOPA) continued throughout the year.

Key Features of the Regulation:

- New ICT risk management obligations.
- Mandatory incident report.

- Mandatory threat-led penetration testing (TLPT).
- New contractual requirements for ICT third-party providers.

Impact for 2026

Financial firms and their cloud/tech suppliers will face contractual renegotiation, audit demands and potential direct oversight — vendors should expect more regulatory scrutiny and certification requests.

2. The UK Cyber Security and Resilience Bill [4][5]: a new era of mandatory cyber security standards.

The UK government introduced the Cyber Security and Resilience (Network and Information Systems) Bill to Parliament in **November 2025**. This legislation represents the most substantial overhaul of the UK's cyber regulatory framework since the original NIS Regulations in 2018.

Impact for 2026

In-scope organisations should **monitor the progress of the Bill through Parliament**, confirm they are in scope, look for sectoral authorities' guidance, and prepare to comply by improving their technical and organisational measures, such as patch management, network segmentation, incident management, multi-factor authentication and integration of threat intelligence in Security Operations. The Bill's emphasis on supply chain resilience means organisations will need to conduct more rigorous vendor assessments, negotiate contractual amendments to incorporate supply-chain security requirements and maintain auditable evidence of due diligence. **Entities should also ensure that board members are aware of the increased fines and, for critical sectors, of potential personal accountability.**

3. Litigation Risk Surges: no "de minimis" threshold for UK GDPR claims.

One of the most consequential legal developments of late 2025 comes from the UK courts. In **Farley v Paymaster** [6], 432 current and former Sussex Police officers sued Paymaster (Equiniti) after pension statements containing personal data were sent to wrong addresses, a clear GDPR

personal data breach. In August 2025, the Court of Appeal ruled that there is no “de minimis” threshold for UK GDPR non-material damages: claimants need not prove actual access or misuse; fear of misuse can suffice for compensation.

A permission to appeal has been lodged with the Supreme Court, but unless overturned, this ruling dramatically expands the scope for individual claims.

Impact for 2026

This precedent opens the door to:

- **More individual claims**, even for minor or technical personal data breaches.
- A surge in group litigation, particularly following data breaches.
- **Higher insurance premiums for cyber and data liability** coverage.

Organisations will need to invest more heavily in data governance, breach prevention and incident response, as even **small lapses may now trigger compensable claims.**

For individuals, the ruling strengthens digital rights and access to redress but may also contribute to rising service costs as organisations pass down to their customers increased insurance costs and litigation exposure.

4. AI Driven Cyber Regulation: the next frontier.

While not tied to a single legislative act, 2025 has seen regulators increasingly integrate AI specific considerations into cyber and data governance frameworks. As highlighted in industry analyses of 2025’s top data protection developments, AI related risks - from automated decision making to model security - are becoming central to regulatory agendas [7][8].

Key themes emerging

- **AI enhanced cyberattacks** are prompting regulators to require more robust anomaly detection and monitoring. Companies are ramping up their cyber-defence systems leveraging AI for vulnerability

identification, analysis and automation. **The use of AI for cyber defence is becoming increasingly a strategic necessity**.

- AI governance frameworks are converging with cyber resilience requirements.
- Data minimisation and transparency obligations are being reinterpreted in the context of large-scale model training.

Impact for 2026

Organisations should expect a growing patchwork of national AI laws - Italy led with its 2025 statute - along with EU AI Act secondary legislations and implementing guidelines. Two key dates in the EU AI Act timeline [9][10]:

1. Post-market monitoring for high-risk AI system must be active from **2 February 2026** onwards, including continuous monitoring.

2. Full high-risk AI obligations will trigger on **2 August 2026**, including but not limited to, **risk management, data governance, technical documentation, logging, human oversight, and cyber-security**.

Also, they will have to intensify their compliance work, from mapping AI use and assessing risks to reinforcing governance, ethics, safeguards, and monitoring. The following AI governance checklist, based on the AI Act requirements, is just one example of how organisations can structure this effort:

- Identify the role of the Organisation in respect to their use of AI (provider, deployer, distributor, user, etc.).
- Create an **AI system inventory** and assign accountable owners.
- Identify applicable laws, standards and guidelines.
- Adopt a **responsible AI Governance framework** (e.g., ISO/IEC 42001:2023).
- Establish code of conduct, **AI ethical principles, and lifecycle processes** (e.g. the Ethics Guidelines for Trustworthy AI issued by the EU Commission High-Level Expert Group on Artificial Intelligence [11]).
- Conduct **risk and data governance** assessments.
- Implement **human oversight**, safeguards, and technical testing.

- Manage third-party AI and contractual requirements.
- Provide transparency, user notices, and opt-outs.
- Monitor performance, audit independently, manage incidents, and retire systems responsibly.

5. Network and Information Systems (NIS) 2 Directive: moving from law into practice [12].

In 2025, ENISA and EU bodies published actionable guidance [13] clarifying technical and governance expectations under NIS 2, turning broad obligations into concrete controls and audit criteria.

Many countries in Europe have transposed the Directive into local legislation causing in-scope companies to ramp up their compliance efforts.

Impact for 2026

More countries, including Ireland and France, are expected to enact their NIS 2 law this year, potentially bringing tens of thousands of organisations into scope. International groups with subsidiaries across multiple EU jurisdictions, will need to monitor these developments closely. Much like the UK's Cyber Security and Resilience Bill, NIS 2 compliance will require organisations to step up their efforts to evidence risk management, incident reporting, security-awareness training, and supply-chain due diligence.

Conclusion: 2026 will be the year of mandatory cyber maturity.

The closing months of 2025 have set the stage for a regulatory environment in 2026 that demands higher standards, greater transparency, and stronger resilience. Businesses that treat cyber compliance as a strategic priority—not a box ticking exercise—will be best positioned to navigate the shifting landscape.

Cyber law is no longer a niche regulatory field—it is becoming the backbone of digital governance, and in 2026, its influence will be felt more than ever.

Column: Security Forefront

Insights from 'LAC Security Insight Vol.14 (Autumn 2025)[14]'

In this column, we share our perspective on the latest cybersecurity trends, drawing on a wide range of sources. For this edition, we reference insights from LAC's quarterly report, "LAC Security Insight," to highlight notable developments in advanced security practices.

Introduction of LAC

LAC Co., Ltd., a subsidiary of KDDI, is one of Japan's most trusted cybersecurity companies. Through its SOC (Security Operation Centre), LAC provides advanced threat intelligence and incident response services. Their quarterly 'LAC Security Insight' report is widely recognized for analysing real-world attacks targeting Japanese organizations.

URL: https://www.lac.co.jp/

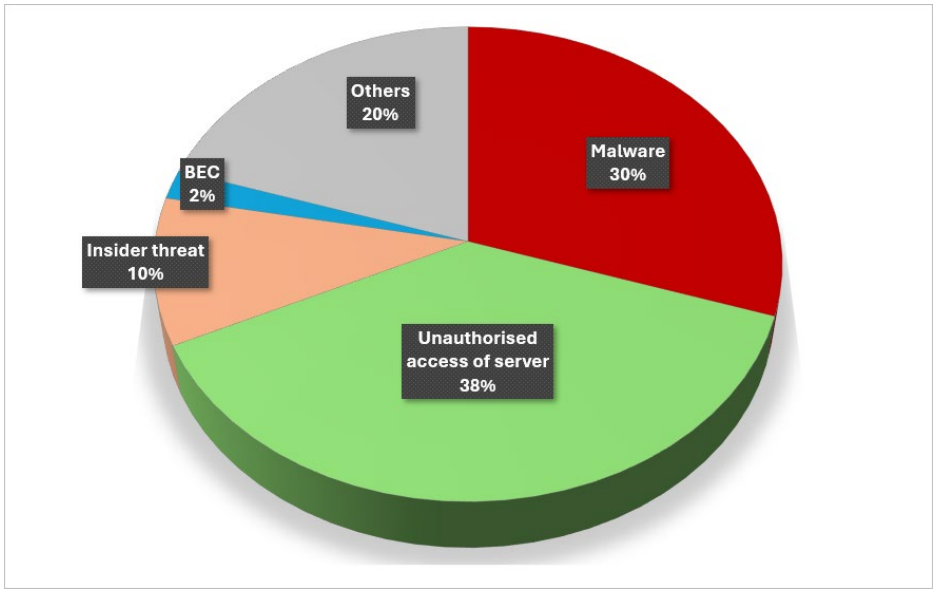
Key Topics

The topics we'll cover in this edition are as follows:

- Malware and server misuse dominate emergency incidents; Microsoft 365 account abuse is rising.
- Social engineering attacks against tourism sector using ClickFix.
- ToolShell exploit chain targets SharePoint servers for persistent access.

1. Incident Trends

Between July and September 2025, majority of the emergency responses was **malware** and **unauthorised access**. Ransomware remains the most common malware, although its share has declined. The most prominent increase in the trend is unauthorised access to Microsoft 365 accounts enabling attackers to carry out data theft and spam email campaigns.



Breakdown of deployment incidents from July to September 2025. [15]

*** Prepared using statistics based on LAC's incident response organization's record.**

Such unauthorised access can result in large-scale breach of your customer and employee data and reputational damage as we witnessed in the recent incidents (reference 2 – 3 incidents).

Many of these incidents share the common weakness. Cloud, access to corporate system through Cloud, identities and access in Cloud. Security in Cloud is a shared responsibility between the providers and us, users. Cloud is designed to accommodate multiple organisations with varied security postures, some prioritise security while others favour convenience. Although “secure by design” is not a new concept, it is not always implemented, making Cloud inherently vulnerable. While some neglects in security during the rapid development and adoption of Cloud in the midst of Covid-19 pandemic was understandable, as we began 2026,

nearly 3 years since WHO declared the end of the pandemic, the continued lack of security in Cloud is no longer acceptable.

The report makes it clear that the attackers prey on our negligence in remote access security, identity governance and monitoring of Cloud for their gain.

We recommend reviewing the following three points first:

- Your Cloud service is protected by **Multi-Factor Authentication**, especially Microsoft 365.
- Your remote access system is **patched regularly**.
- You are **monitoring** suspicious login and unusual file sharing.

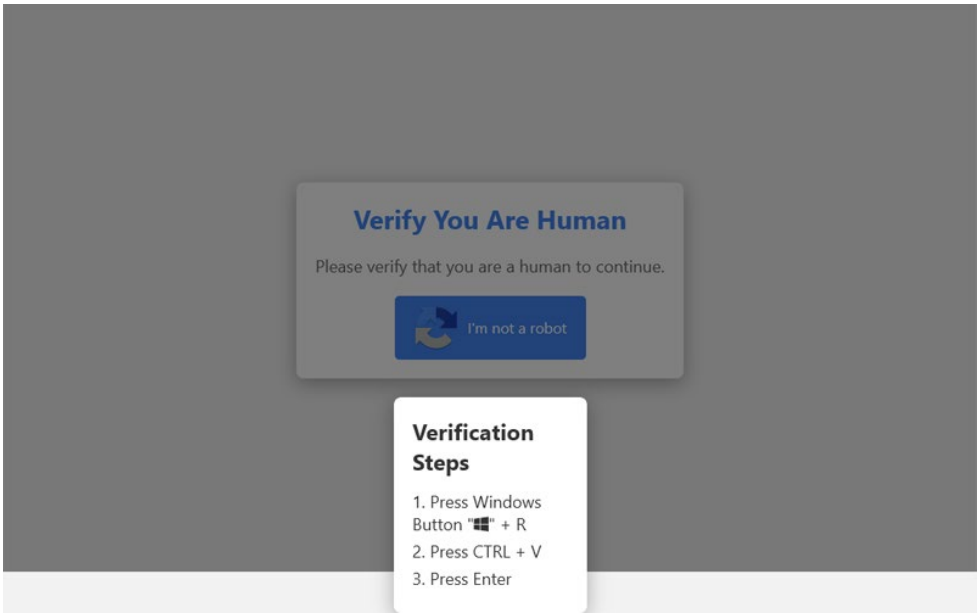
2. ClickFix Social Engineering Attack

For the hospitality and travel industry, the holiday season is a peak period that makes employees feel compelled to respond quickly and diligently to maintain customer satisfaction. The ClickFix attack we're about to introduce takes advantage of this sense of responsibility, using it as a lever to lure victims into malware infection.

A new technique called ClickFix is gaining traction among threat actors. It's deceptively simple: a fake CAPTCHA screen that looks legitimate enough to lower suspicion but hides a trap. When users follow the on-screen instructions and perform operations, they unknowingly trigger malware infection.

Attackers saw an opportunity to exploit human trust and impatience rather than technical flaws. They realised users instinctively follow prompts and trust system dialogs, making manual execution appear safe. This approach shifts responsibility to the user, and offers attackers a low-cost, high-success method for malware infection.

"



A fake screen disguised as a CAPTCHA page. [16]

What makes ClickFix particularly dangerous is its ability to bypass traditional security warnings. No suspicious downloads, no glaring red

flags—just a familiar CAPTCHA that feels routine. This is social engineering at its finest, and it's working. The hospitality and travel industry, the stakes couldn't be higher. Beyond operational disruption, the risk of data compromise and reputational damage is real. In an industry built on trust and customer experience, one breach can ripple far beyond IT.

We recommend reviewing the following three points first:

- Your endpoints are protected by **EDR** to detect suspicious behaviours and prevent exploitation.
- **Multi-Factor Authentication** is enforced across all SaaS platforms, not just Microsoft 365.
- Your **staff is trained** to identify fake CAPTCHA screens and unusual shortcut key requests before they act.

3. ToolShell Campaign

A surge in targeted exploitation campaigns against SharePoint environments has been observed. Among these, an attack technique known as ToolShell—an exploit chain that combines multiple vulnerabilities in SharePoint Server—stands out as one of the most critical threats. ToolShell emerged as attackers shifted focus from opportunistic web exploits to strategic compromise of collaboration platforms—systems that store sensitive business data and underpin remote work. This trend reflects a broader move toward exploiting high-value applications that organizations rely on daily, knowing disruption here creates maximum leverage.

This campaign abuses multiple SharePoint vulnerabilities to install webshells and steal encryption keys, enabling persistent access long after the initial compromise. What makes ToolShell particularly concerning is its use of CVE-2025-53770, a deserialization flaw that allows unauthenticated remote code execution. We highlighted this vulnerability in our Threat Report Volume 4 (August 2025), but its inclusion in ToolShell underscores a recurring issue: patching alone is not enough. Attackers are leveraging stolen keys and weak post-patch hygiene to maintain access, even in supposedly “secured” environments.

As IT ecosystems grow more interconnected and cloud-hybrid collaboration becomes the norm, attackers are exploiting complexity and trust relationships. Ignoring these realities is no longer an option.

We recommend reviewing the following three points first:

- **Microsoft patches** are applied immediately, and **machine keys are rotated without delay**.
- Monitoring for unusual **ASPX files** is in place and IIS logs are checked for suspicious access patterns, especially requests to **ToolPane.aspx**.
- SharePoint admin endpoints are protected with advanced detection and exploit prevention at an early stage by **EDR**.

Suggestions

Protection, Prevention and Takeaways

1. A quick positive note to start off the new year. Other recent news highlights several arrests of cyber criminals across the globe, this signals that law enforcement is actively and successfully combating cybercrime. The key takeaway? Despite frequent reports of cyberattacks and their impact, meaningful progress is being made, and the fight against cybercrime is working.

2. There are best practices you can implement to help safeguard your services from falling victim to a DDoS attack, often at no additional cost. Have you set time limits for how long your servers wait for a response? Do you maintain a blacklist of IP addresses associated with known botnets? Have you limited the number of requests per IP address, user, or API key within a defined time window? These simple actions, applied in your existing environment, can provide an added layer of defence.

3. Following the example of security vendors who continuously expand their offerings through acquisitions or partnerships, businesses must also consider leveraging multiple tools to enhance protection in areas that may otherwise remain vulnerable. Cybersecurity is a vast domain, and no single solution can provide complete coverage across all its facets. Key areas such as Endpoint, Email, Identity, and Cloud Security, along with Data Loss Prevention (DLP), Vulnerability Management, and Network Security, are distinct yet interconnected. Because of this complexity, organisations should regularly assess their security posture to identify gaps in critical areas that could expose them to risk. Implementing a layered approach is essential to achieving comprehensive protection.

Common Vulnerabilities and Exposures (CVEs)

Every month a CVE is selected at the discretion of the report's author to be discussed. This report will also include the EUVD ID as well. This month it is a vulnerability affecting multiple versions of Microsoft Office.

CVE-2025-62554 | EUVD-2025-202218 [17]

Vendor	Microsoft
Product	Microsoft Office 2016, 2019, LTSC 2021, LTSC 2024, Microsoft Office for Android. Microsoft 365 Apps for Enterprise
Publish Date	09-12-2025
Platform	32-bit and 64-bit editions
CVSS (v3.1)	8.4

Description

Access of resource using incompatible type ('type confusion') in Microsoft Office allows an unauthorized attacker to execute code locally.

What does this mean for you?

An attacker can send a malicious link via email and in a worst-case scenario code execution can occur simply by previewing a malicious document.

What should you do about it?

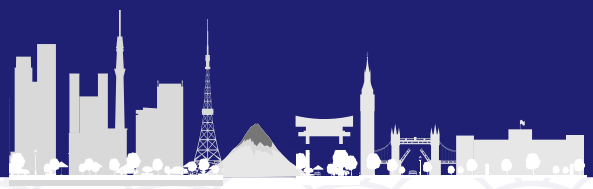
Install security updates released by Microsoft on the 9th of December 2025 for all affected systems.

Links & References

1. ServiceNow (2025) ServiceNow to acquire Armis to expand cyber exposure and security across the full attack surface in IT, OT, and medical devices for companies, governments, and critical infrastructure worldwide. Available at: https://newsroom.servicenow.com/press-releases/details/2025/ServiceNow-to-acquire-Armis-to-expand-cyber-exposure-and-security-across-the-full-attack-surface-in-IT-OT-and-medical-devices-for-companies-governments-and-critical-infrastructure-worldwide/default.aspx (Accessed: 2 January 2026).
2. Euronews (2025) Cyberattack knocks France's postal service and its banking arm offline. Available at: https://www.euronews.com/2025/12/22/cyberattack-knocks-frances-postal-service-and-its-banking-arm-offline (Accessed: 2 January 2026).
3. European Insurance and Occupational Pensions Authority (EIOPA) (2026) Digital Operational Resilience Act (DORA). Available at: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en (Accessed: 7 January 2026).
4. UK Government (2026) Cyber Security and Resilience Bill. Available at: https://www.gov.uk/government/collections/cyber-security-and-resilience-bill (Accessed: 7 January 2026).
5. Information Commissioner's Office (ICO) (2026) Information Commissioner's response to the Cyber Security and Resilience Bill. Available at: https://ico.org.uk/about-the-ico/information-commissioner-s-response-to-the-cyber-security-and-resilience-bill/ (Accessed: 7 January 2026).
6. UK Supreme Court (2026) Case UKSC 2025/0185. Available at: https://www.supremecourt.uk/cases/uksc-2025-0185 (Accessed: 7 January 2026).
7. European Union Agency for Cybersecurity (ENISA) (2025) ENISA Threat Landscape 2025. Available at: https://www.enisa.europa.eu/sites/default/files/2025-12/ENISA%20Threat%20Landscape%202025_v1.1.pdf (Accessed: 7 January 2026).
8. Information Commissioner's Office (ICO) (2026) Guidance on AI and data protection. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/ (Accessed: 7 January 2026).
9. European Commission (2025) Commission publishes guidelines on prohibited artificial intelligence (AI) practices as defined in the AI Act. Available at: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act (Accessed: 8 January 2026).
10. European Parliamentary Research Service (EPRS) (2025) AI Act implementation timeline. Available at:

https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/772906/EPRS_ATA(2025)772906_EN.pdf (Accessed: 8 January 2026).
11. High-Level Expert Group on Artificial Intelligence (AI HLEG) (2019) Ethics Guidelines for Trustworthy AI. Available at: https://www.europarl.europa.eu/cmsdata/196377/AI%20HLEG_Ethics%20Guidelines%20for%20Trustworthy%20AI.pdf (Accessed: 8 January 2026).
12. European Commission (2025) NIS2 Directive: securing network and information systems. Available at: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive (Accessed: 8 January 2026).
13. European Union Agency for Cybersecurity (ENISA) (2025) NIS2 Technical Implementation Guidance. Available at: https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance (Accessed: 8 January 2026).
14. LAC Co., Ltd. (2025) LAC Security Insight Vol.14 (Autumn 2025). Available at: https://www.lac.co.jp/lacwatch/pdf/20251113_lsi_vol14.pdf (Accessed: 17 December 2025).
15. LAC Co., Ltd. (2025) LAC Security Insight Vol.14 (Autumn 2025), translated by Hiroki Morishita, KDDI Europe Limited, page 5. Available at: https://www.lac.co.jp/lacwatch/pdf/20251113_lsi_vol14.pdf (Accessed: 17 December 2025).
16. LAC Co., Ltd. (2025) LAC WATCH, translated by Hiroki Morishita, KDDI Europe Limited. Available at: https://www.lac.co.jp/lacwatch/alert/20250519_004380.html (Accessed: 18 December 2025).
17. European Union Agency for Cybersecurity (ENISA) (2026) EUVD. Available at: https://euvd.enisa.europa.eu/enisa/EUVD-2025-202218 (Accessed: 8 January 2026).

Let’s Secure the Future — Together



KDDI Europe is the European headquarters of the Fortune Global 500 KDDI Corporation, delivering cutting-edge ICT and cybersecurity solutions with the precision and reliability Japan is known for.

With over 70 years of global expertise, we empower businesses across industries — from finance and retail to manufacturing and education — with secure, scalable infrastructure and 24/7 protection.

Whether you’re looking to strengthen your cybersecurity posture or scale your global operations, **we are your partner, your enabler, your platformer.**

Security of Tomorrow, Today.

Contact Information

Telephone Number	+44 20 7507 0001
Email Address	info@uk.kddi.eu

Website

LinkedIn

Enquiry