










Infobrief – April 2026

 Germany – legal and regulatory updates	2
Germany tightens action against organised crime.....	2
BaFin flags rising AML/CFT risks across payments, crypto and sanctions evasion.....	2
New reporting rules for suspicious activities since 1 March 2026.....	3
BaFin updates high-risk countries list.....	3
 EU and international – legal and regulatory updates	4
AMLA sets out strategic priorities for 2026-2028.....	4
AMLA opens consultations on AML/CFT standards.....	4
AMLA opens consultations on group-wide requirements and business-wide risk assessment	5
EU updates non-cooperative tax jurisdictions list	5
FATF adds Kuwait and Papua New Guinea to list of jurisdictions under increased monitoring	6
US National Money Laundering Risk Assessment published	6
 AML/CFT investigations and enforcement action	7
Police search Deutsche Bank over money-laundering suspicions	7
Investigation at EFG bank in Luxembourg	7
FINMA winds up MBaer Merchant Bank over money laundering.....	7
 Financial crime and cybercrime investigations	8
Europol-led global operation shuts down 373,000 dark web sites	8
 Terrorist and extremist financing	8
EU strengthens terrorist listing rules.....	8
Global terrorism declines to decade low despite rising risks in West.....	9
 Sanctions.....	9
German criminal sanctions law to be tightened.....	9
EU court clarifies scope of sanctions: asset freezes extend to controlled companies	10
EU imposes new sanctions on Iran over protest suppression	10

 Other AML/CFT research reports	11
Council of Europe flags virtual asset risks.....	11
CPI 2025: Global corruption decline deepens.....	11
London's role in Iran's financial networks.....	12
 Crypto assets	12
Media reflects doubts about Bitpanda	12
Chainalysis: Crypto crime hits record levels as state actors expand on-chain activity	13
FATF warns on offshore virtual asset service providers.....	13
 Information security and data protection	14
EU Commission proposes stronger cybersecurity framework.....	14
EU Council imposes sanctions over cyber-attacks on member states and partners.....	14
ChatGPT vulnerability exposed sensitive data risk.....	15
 Media Recommendations	15
 Coming soon	16

Germany – legal and regulatory updates

Germany tightens action against organised crime

The German government on 25 February 2026 announced that it had approved a new action plan to intensify the fight against organised crime. The plan aims to improve cooperation between the relevant authorities, speed up the sharing of information, and make better use of modern technology in investigations. It also allocates additional staff and stronger legal, technical and organisational resources to the customs service (Zoll) and the Federal Criminal Police Office (BKA).

Financial crime is a key focus of this plan: officials intend to target illicit proceeds more consistently and seize assets more quickly when criminal origin is suspected. The government says the measures were designed to address money laundering, drug trafficking and related criminal structures more effectively. Finance Minister Lars Klingbeil described the approach as 'following the money' and making it harder for criminals to benefit from illegal gains.

Link:

[Aktionsplan der Regierung. Besser organisiert gegen die Organisierte Kriminalität \(Tagesschau, 25 February 2026\)](#)

BaFin flags rising AML/CFT risks across payments, crypto and sanctions evasion

BaFin at the beginning of the year published its priorities for 2026, which focus on the risks arising from inadequate money laundering and terrorist financing prevention measures. BaFin underscored that the AML/CFT risks remained high for market participants, due to geopolitical tensions, fragmented payments systems, and the growth of cryptocurrencies.

Notably, BaFin stressed that terrorist financing required separate attention from money laundering, as illicit funds may originate from legitimate sources and involve very small transactions. The authority noted that obliged entities often failed to give sufficient weight to terrorist financing risks and needed to strengthen controls such as transaction-purpose checks and adverse media screening. BaFin also highlighted growing concerns about sanctions circumvention schemes, particularly those involving Iran, where the risks have increased significantly since the reimposition of sanctions in September 2025.

In addition, the regulator warned that cryptocurrency transactions could be used to obscure identities and move illicit funds quickly, making them attractive for both money laundering and terrorist financing. Payment service providers remain under close scrutiny, particularly as online commerce and card use are increasing the importance of customer identification and counterparty risk assessment.

In 2026, BaFin plans to conduct at least 75 special audits and intends to maintain a strict supervisory stance, focusing on suspicious transaction monitoring, business with high-risk countries, compliance with the Travel Rule and agents of EU payment institutions deemed to be high risk.

Links:

[Risiken aus unzureichender Prävention von Geldwäsche und Terrorismusfinanzierung \(BaFin\)](#)

[Gemeinsamer Einsatz zur Bekämpfung der internationalen Geldwäsche \(BaFin, 16 April 2026\)](#)

New reporting rules for suspicious activities since 1 March 2026

A new regulation on suspicious activity reports (SARs) under the Anti-Money Laundering Act came into force on 1 March 2026. It is intended to increase the uniformity and quality of reports to Germany's Financial Intelligence Unit (FIU). Since the regulation came into force, SARs and subsequent amendments must be submitted electronically in a structured, machine-readable format, such as XML, with attachments in formats that can be automatically processed and searched.

The regulation also establishes minimum content requirements, such as the reporting person's case reference, details of potential criminal complaints or official investigations, and one or more justification for the filing of the report – drawn from the FIU's predefined categories.

Link:

[Verordnung über die Form von und die erforderlichen Angaben in Meldungen an die Zentralstelle für](#)

[Finanztransaktionsuntersuchungen nach § 43 Absatz 1 und § 44 des Geldwäschegesetzes \(GwG-Meldeverordnung — GwGMeldV\) \(Bundesgesetzblatt, 1 September 2025\)](#)

BaFin updates high-risk countries list

On 30 March 2026, BaFin published an updated list of third countries with strategic deficiencies in their anti-money laundering and counter-terrorist financing systems.

The list cites FATF concerns about North Korea's failure to address major AML/CFT deficiencies and related proliferation financing risks. As noted in United Nations Security Council Resolution 2270, North Korea is believed to increasingly use front companies, shell companies, joint ventures and complex, opaque ownership structures to circumvent sanctions. With regard to Iran, the FATF reiterated its call for countermeasures to be applied due to the ongoing threat of terrorist financing and proliferation financing originating from the country.

The circular also defines a list of enhanced due diligence obligations that apply to business relationships and transactions with North Korea and Iran, including heightened beneficial ownership checks and additional safeguards.

Links:

[Rundschreiben 03/2026 \(GW\) \(BaFin, 30 March 2026\)](#)

[High-Risk Jurisdictions subject to a Call for Action \(FATF, 13 February 2026\)](#)

EU and international – legal and regulatory updates

AMLA sets out strategic priorities for 2026-2028

On 4 February 2026, the EU's Anti-Money Laundering Authority (AMLA) published its first Single Programming Document for the period 2026-2028. This document defines the Authority's priorities and timelines as it transitions from its founding phase to full operational capacity. The plan sets out the scheduled mandates for 2026 and defines three strategic objectives: completing the Single Rulebook, advancing supervisory convergence and strengthening cooperation among financial intelligence units.

These objectives have been broken down into five workstreams, which cover core regulatory mandates, direct supervision, operationalising the FIU framework, indirect supervision and oversight and AMLA's risk frameworks. According to AMLA, the document is intended to provide clarity to the market on upcoming requirements and support preparation through public consultations.

The Authority also plans to expand its operational capacity by increasing its workforce, improving its IT infrastructure and strengthening its internal structures in order to fulfil its mandate. According to AMLA, workforce numbers are expected to rise from 120 at the end of 2025 to 432 by the end of 2027. Chair Bruna Szego said the document sets out a path towards full operations, while maintaining technical excellence and cooperation.

Link:

[AMLA sets strategic priorities with 2026-28 Single Programming Document \(AMLA, 4 February 2026\)](#)

AMLA opens consultations on AML/CFT standards

On 18 February 2026, AMLA launched consultations on three regulatory technical standards (RTS) that will shape how money laundering and terrorist financing risks are addressed across the financial and non-financial sectors. Market participants are being encouraged to contribute to the consultation process, given that the standards will apply directly to private-sector firms in Germany once finalised.

The first RTS concerns criteria for identifying business relationships, occasional transactions, linked transactions and lower thresholds under the new EU AML rulebook. The second RTS sets out customer due diligence requirements, including how firms should assess risk and apply controls in practice. The third RTS covers supervisory measures, administrative sanctions and periodic penalty payments, including the methodology for coercive fines.

The consultation period for the first and the second RTS lasts until 8 May 2026, while the shortened deadline for the third RTS already ended on 9 March 2026.

The consultation fits into the broader EU AML reform, which created AMLA as a central authority and is designed to harmonise prevention standards more closely across member states. The process is part of a wider 2026 regulatory transition, with firms expected to prepare early for more unified EU requirements and tighter

oversight (see also [Infobrief 17 of December 2025](#)). AMLA will still need the European Commission's approval before the standards can enter into force.

Links:

[AMLA konsultiert Standards zur Prävention von Geldwäsche und Terrorismusfinanzierung \(BaFin, 18 February 2026\)](#)

[Overview of AMLA Regulatory Instruments](#)

[Press Release: AMLA to launch data collection exercise to test risk assessment models for the financial sector \(AMLA, 26 January 2026\)](#)

AMLA opens consultations on group-wide requirements and business-wide risk assessment

On 16 April 2026, AMLA initiated public consultations on two draft instruments aimed at enhancing the management of money laundering and terrorist financing risks.

The draft guidelines on business-wide risk assessment under AMLR Article 10(4) set out minimum expectations for all obliged entities in the financial and non-financial sectors. The guidelines promote proportionality based on size, business model and risk profile, and are intended to support informed, risk-based decision-making.

The draft regulatory technical standards (RTS) on group-wide requirements, pursuant to AMLR articles 16(4) and 17(3), establish minimum standards for AML/CFT frameworks, including cross-border operations and third-country activities, providing groups with a consolidated view of risk.

These measures are intended to ensure that organisations adapt their policies, procedures and controls to comprehensively address ML/TF risks across their operations. AMLA has invited stakeholder feedback, particularly from the non-financial sector, in any EU language via the consultation links (see below). Public hearings are scheduled for 20 May 2026 (draft RTS) and 28 May 2026 (draft guidelines), both from 10:00–12:00 CET.

Links:

[AMLA consults on group-wide requirements and business-wide risk assessment \(AMLA press release, 16 April 2026\)](#)

[Public Hearing on the draft RTS on group-wide minimum requirements and additional measures for subsidiaries and branches in third countries \(AMLA, 16 April 2026\)](#)

[Public Hearing on the draft Guidelines on business-wide risk assessment \(AMLA, 16 April 2026\)](#)

EU updates non-cooperative tax jurisdictions list

Following its latest review, the Council of the European Union in February 2026 updated its list of non-cooperative jurisdictions for tax purposes. The revised Annex I now includes the following ten jurisdictions: American Samoa, Anguilla, Guam, Palau, Panama, the Russian Federation, the Turks and Caicos Islands, the US Virgin Islands, Vanuatu and Vietnam.

Fiji, Samoa and Trinidad and Tobago have been removed from the Annex I list after addressing relevant tax-related issues. According to the Council, the update reflects ongoing screening based on tax transparency, fair taxation and the implementation of OECD anti-BEPS standards.

In parallel, Annex II — the EU's “grey list” of jurisdictions under review — was updated and now includes nine jurisdictions: Belize, the British Virgin Islands, Brunei Darussalam, Eswatini, Greenland, Jordan, Montenegro, Morocco and Turkey. According to media and professional tax briefings, Antigua and Barbuda and Seychelles were removed from Annex II, while Brunei was given more time to implement reforms.

Link:

[EU list of non-cooperative jurisdictions for tax purposes \(Council of the European Union, 17 February 2026\)](#)

FATF adds Kuwait and Papua New Guinea to list of jurisdictions under increased monitoring

The Financial Action Task Force (FATF) added Kuwait and Papua New Guinea to its list of jurisdictions under increased monitoring at its February 2026 Plenary. No countries were removed from the list.

The Plenary also adopted mutual evaluation reports for Austria, Italy and Singapore, which are expected to be published in spring 2026. Additionally, the Plenary approved new strategic publications on cyber-enabled fraud and virtual assets.

Links:

[Outcomes FATF Plenary, 11-13 February 2026 \(FATF, 13 February 2026\)](#)

[Jurisdictions under Increased Monitoring \(FATF, 13 February 2026\)](#)

US National Money Laundering Risk Assessment published

On 6 March 2026, the US Department of the Treasury published its 2026 National Money Laundering Risk Assessment (NMLRA).

The assessment noted that illicit trade continued to generate billions of dollars in profits, and stated that the primary money laundering threats remained linked to fraud, drug trafficking, cybercrime, human trafficking, human smuggling and corruption. The NMLRA emphasised that these threats were increasingly enabled by professional money launderers, including Chinese money laundering networks, which were found to be scaling up and professionalising criminal activity. According to the report, technological change has intensified the risk, particularly through social media, encrypted messaging, digital assets and artificial intelligence (AI).

The NMLRA further highlighted the substantial increase in high-value fraud cases, with the report noting that median losses in convicted money laundering cases had risen considerably over the past five years. The assessment also highlighted the growing use of AI in fraudulent communications, identities and websites, enabling scams to be carried out more quickly and on a larger scale, and making them harder to detect. Investment fraud was identified as a leading source of illicit funds, and the report attributed much of the recent

increase to digital asset investment and cross-border scams. It also warned that criminals continued to exploit banks, legal entities, cash channels and digital assets to hide illicit funds amid legitimate financial flows.

Link:

[Department of the Treasury: 2026 National Money Laundering Risk Assessment \(6 March 2026\)](#)

AML/CFT investigations and enforcement action

Police search Deutsche Bank over money-laundering suspicions

German investigators on 28 January 2026 searched the offices of Deutsche Bank in Frankfurt and Berlin on suspicion of money laundering. The operation was carried out by the Frankfurt special prosecutor's office for economic crime, in collaboration with the Federal Criminal Police Office (BKA). The authorities said that the searches were intended to secure additional evidence.

The investigation reportedly concerns unnamed individuals at the bank. It is linked to earlier business relationships with foreign companies suspected of being used for money laundering. The raids took place on the eve of the bank's announcement of its results for 2025. Deutsche Bank has faced repeated scrutiny over alleged weaknesses in its anti-money laundering controls. The bank stated that it was cooperating with the authorities while the investigation continued.

Link:

[Deutsche Bank: Razzia wegen Geldwäsche in der Zentrale in Frankfurt \(Tagesschau, 28 January 2026\)](#)

Investigation at EFG bank in Luxembourg

Media reports in February indicated that EFG's Luxembourg subsidiary is under investigation for suspected money laundering and terrorist financing, as well as possible breaches of reporting and cooperation duties. On 24 February 2026, the bank's premises were searched as part of the evidence-gathering process.

The investigation reportedly pertains to – among other issues – alleged weaknesses in customer due diligence and internal controls. EFG confirmed that the local authorities had been present at its Luxembourg offices and stated that it was cooperating fully. The investigation is ongoing.

Link:

[Raid at EFG in Luxembourg \(Finews, 27 February 2026\)](#)

FINMA winds up MBaer Merchant Bank over money laundering

MBaer Merchant Bank AG on 27 February 2026 announced that it had entered liquidation, after it withdrew its appeal against the revocation of its banking licence by Switzerland's financial regulator FINMA. The regulator had on 6 February revoked the license and ordered MBaer's liquidation following enforcement proceedings concerning violations of anti-money laundering regulations. FINMA claimed that the bank committed serious

and systematic breaches of anti-money laundering rules, and had actively helped clients to circumvent asset freezes and sanctions.

The bank's decision to withdraw its appeal was made one day after the US financial crime watchdog FinCEN threatened to exclude Mbaer from the US financial system. FINMA described the case as exceptionally serious, stating that the organisational and risk management shortcomings were so severe that a rescue was no longer feasible. Mbaer Merchant Bank reportedly managed CHF 4.9 billion for nearly 700 clients at the end of 2025, with just over 60 employees.

Links:

[FINMA-Verfahren: Mbaer Merchant Bank AG in Liquidation \(FINMA, 27 February 2026\)](#)

[Finanzaufsicht wickelt Mbaer Merchant Bank wegen Geldwäsche ab \(Handelsblatt, 27 February 2026\)](#)

Financial crime and cybercrime investigations

Europol-led global operation shuts down 373,000 dark web sites

On 9 March 2026, Europol reported that a major international law enforcement operation had disrupted one of the largest dark web fraud networks to date. Carried out with the help of authorities from 23 countries, the operation resulted in the shutdown of over 373,000 dark web sites, the identification of the perpetrator operating the central dark web platform and 440 customers worldwide, and the seizure of 105 servers.

Europol stated that the network had been used to advertise child sexual abuse material and cybercrime-related services. Investigators linked the scheme to wider organised criminal infrastructure. The operation is part of an ongoing effort to combat online fraud and other cybercrimes.

Link:

[Global cybercrime crackdown: over 373 000 dark web sites shut down \(Europol, 9 March 2026\)](#)

Terrorist and extremist financing

EU strengthens terrorist listing rules

On 26 February 2026, the Council of the EU announced that it had expanded the scope of the EU's list of terrorist organisations and individuals, and confirmed that all existing listings would remain in place.

According to the Council, the updated rules broaden the listing criteria, enabling the EU to target leading members of listed groups and entities that play a pivotal role in the planning, facilitation, preparation or execution of terrorist acts. The new framework also permits the imposition of restrictive measures on individuals, groups and entities associated with those involved in terrorist activities, including financing, training or recruitment.

Alongside the existing asset freeze and ban on providing funds or economic resources, the Council has introduced a travel ban for listed individuals. The Council stated that the intention was to reinforce the EU's counterterrorism sanctions regime and enhance its capacity to respond to emerging threats.

Link:

[EU sanctions against terrorism: Council strengthens the scope of the EU Terrorist List and maintains all existing links \(European Council, 26 February 2026\)](#)

Global terrorism declines to decade low despite rising risks in West

The London based Institute for Economics and Peace on 19 March 2026 published its Global Terrorism Index (GTI) for 2025. According to the report, terrorism-related deaths have decreased by 28 percent worldwide, with 5,582 fatalities recorded in 2025, marking the lowest number since 2007. However, Western countries experienced a 280 percent surge in fatalities, reaching 57 in 2025, largely driven by antisemitism, Islamophobia and politically motivated violence.

Pakistan was ranked the most terrorism-affected country for the first time, with 1,139 deaths and 1,045 incidents recorded – its highest level since 2013. Sub-Saharan Africa remained the global epicentre of terrorism, with six of the ten most impacted countries located in the region, accounting for over half of all terrorism-related deaths.

The report highlighted a sharp increase in youth radicalisation, with minors representing 42 percent of terrorism-related investigations in Europe and North America. Investigations involving young individuals have tripled since 2021, with online platforms accelerating radicalisation timelines to just a few months. The Islamic State and its affiliates were found to be the deadliest terrorist network, being responsible for almost 17 percent of global attacks. Notably, lone actors were responsible for 93 percent of fatal attacks in the West.

Geopolitical developments, particularly the escalating conflict in Iran, were identified as key risk factors. There are concerns that state instability could foster new terrorist safe havens and militia activity. Border regions are being increasingly affected, with more than 76 percent of attacks occurring within 100km of international borders – more than double the proportion recorded in 2007. Overall, the report warned that deteriorating economic conditions, political polarisation and the weakening of international norms could undo recent progress in countering terrorism.

Links:

[Measuring the Impact of Terrorism: Global Terrorism Index 2026 \(pdf\)](#)

[Measuring the Impact of Terrorism: Global Terrorism Index Briefing 2026 \(pdf\)](#)

Sanctions

German criminal sanctions law to be tightened

On 15 January 2025, the German Bundestag passed the Act “on the adaptation of criminal offences and sanctions for breaches of European Union restrictive measures”, which came into force on 6 February 2026. The act transposes the long-awaited provisions of the “EU Directive (2024/1226) on the definition of criminal offences and sanctions for breaches of European Union restrictive measures” into German law, fundamentally reforming German criminal sanctions law in the process.

Key provisions have been significantly tightened, noticeably increasing the risk of criminal penalties and fines for companies and their management found in to be breach of sanctions. A minimum upper limit for fines is provided for companies, based either on global annual turnover (1 percent or 5 percent) or on specific monetary amounts of EUR 8 million or EUR 40 million, depending on the nature of the underlying breach.

Notably, the amendment stipulates that numerous infringements that could previously only be punished as administrative offences will now incur mandatory criminal penalties in cases of intentional infringement. This applies in particular to infringements of certain transaction and financial services prohibitions.

An important change relates to infringements concerning the trade in dual-use goods, i.e. goods that can be used for both civilian and military purposes. In future, mere recklessness will suffice to render such acts punishable. This shift will increase the criminal liability risks for companies that export or import such goods, as well as for logistics companies.

Links:

[Gesetz zur Anpassung von Straftatbeständen und Sanktionen bei Verstößen gegen restriktive Maßnahmen der Europäischen Union \(Bundesgesetzblatt, 05 February 2026\)](#)

[EU-Richtlinie \(2024/1226\) zur Definition von Straftatbeständen und Sanktionen bei Verstoß gegen restriktive Maßnahmen der Europäischen Union](#)

EU court clarifies scope of sanctions: asset freezes extend to controlled companies

The Luxembourg-based Court of Justice of the EU has ruled that the assets of a company not listed under EU sanctions may be frozen if it is controlled by an individual subject to sanctions.

In its ruling on Case C-84/24, the Court confirmed that a 50 percent shareholding created a presumption of control, which extended to both the company itself and its funds and economic resources. The case originated when Lithuanian banks froze the assets of EM System due to a sanctioned Belarusian national holding exactly 50 percent of its shares.

The court emphasised that sanctions must be applied broadly to prevent circumvention, requiring an expansive interpretation of “ownership”, “holding” and “control”, including indirect influence. The ruling also highlights that this presumption can be challenged, and both the sanctioned individual and the affected company must be given the opportunity to contest and potentially overturn the asset freeze.

Link:

[Press Release 32/26 \(Court of Justice of the European Union, 12 March 2026\)](#)

EU imposes new sanctions on Iran over protest suppression

On 16 March 2026, the EU Council announced a new sanctions package targeting 16 individuals and three entities for serious human rights violations in Iran linked to the violent suppression of anti-government protests in January 2026. These measures address the regime's response, which resulted in thousands of civilian casualties and more than 16,500 arbitrary arrests.

The list of sanctioned individuals include Iran's Deputy Minister of the Interior Ali Akbar Pour-Jamshidian, IRGC commanders and local Revolutionary Guard branches responsible for brutal crackdowns. Judiciary members involved in forced confessions, unfair trials and harsh sentences against protesters, activists and journalists also face sanctions.

The package imposes asset freezes, travel bans and prohibitions on EU entities providing funds or resources to those listed. It brings the total number of individuals and entities covered by the EU's Iran human rights regime to 263 and 53, respectively.

Link:

[New EU sanctions package targets Iran human rights violations \(ICLG, 18 March 2026\)](#)

Other AML/CFT research reports

Council of Europe flags virtual asset risks

On 10 February 2026, the Council of Europe's MONEYVAL committee published a new report on the misuse of virtual assets and service providers for the purposes of money laundering, terrorist financing and evading sanctions.

Reflecting the rapid evolution of crypto-related technologies and their use in illicit finance, the report was based on input from 25 jurisdictions. While it acknowledged progress in licensing and supervision in many countries, it also highlighted persistent weaknesses in enforcement against unlicensed operators.

The report also highlighted the incomplete implementation of the Travel Rule as an ongoing concern. Emerging threats identified in the review included sanctions evasion and fraud. MONEYVAL stated that further operational and regulatory action was required to mitigate these risks.

Links:

[Practice of Using Virtual Assets, Virtual Asset Service Providers in the Laundering of Criminal Property, Financing of Terrorism, and the Evasion of Sanctions. Typologies report, December 2025](#)

[New report on the use of virtual assets for money laundering and terrorist financing \(Council of Europe, 10 February 2026\)](#)

CPI 2025: Global corruption decline deepens

Transparency International's 2025 Corruption Perceptions Index (CPI) – published on 10 February 2026 – highlighted that corruption remains a serious global problem. For the first time in over a decade, the average score fell to 42 out of 100, reflecting a worsening overall corruption picture.

The index covers 182 countries and territories, using 13 independent data sources to assess perceived public-sector corruption. According to the report, 122 countries scored below 50, indicating that the majority of governments are still struggling to control corruption. The report suggested that the decline was driven by weakened democratic checks and balances, pressure on civil society and limited accountability.

The report linked stronger anti-corruption outcomes to independent courts, free media, civic space and transparent institutions. It also noted that improvements that relied on authoritarian control rather than

genuine accountability could be fragile. Overall, the 2025 CPI presented a mixed picture, showing limited progress but a clear global trend towards weaker integrity and a higher risk of corruption.

Link:

[CPI 2025: Findings and insights \(Transparency International, 10 February 2026\)](#)

London's role in Iran's financial networks

Transparency International UK on 12 March 2026 published an article highlighting London's long-running significant role in financial networks linked to Iran's regime and associated individuals.

The article highlighted that more than GBP 200 million-worth of UK property had been identified as having been purchased by individuals connected to the Iranian regime. It argued that these assets demonstrated how international financial centres could be exploited to move and store wealth associated with sanctioned or politically exposed networks.

The article emphasised the relevance of this issue, given the ongoing high level of enforcement pressure and geopolitical scrutiny surrounding Iran. It also suggested that greater transparency and stronger controls were essential to reduce the misuse of the property market and wider financial system.

Link:

[London's role in Iran's financial networks — and why it matters now \(Transparency International UK, 12 March 2026\)](#)

Crypto assets

Media reflects doubts about Bitpanda

According to an investigative report published by Tagesschau on 29 January 2026, internal documents suggest that crypto platform Bitpanda faces significant regulatory and organisational weaknesses within its German-licensed operations.

The company, which presents itself as a model fintech, received a BaFin licence in 2022 through its subsidiary Bitpanda Asset Management GmbH. During a special review in 2023, BaFin reportedly identified 16 issues, including serious problems relating to risk management, IT and outsourcing. According to Tagesschau, five of these were classified as severe, while the rest were rated as material, medium or minor. Internal audit documents seen by journalists also reportedly criticised the quality of documentation and control processes.

According to the report, Bitpanda informed BaFin that it would address the shortcomings by March 2025. BaFin reportedly acknowledged the company's efforts, yet still issued a formal warning letter. The company stated that the review was a routine supervisory examination following the granting of a licence. BaFin did not publicly comment on the specific findings.

Link:

[Erfüllt Bitpanda die Vorgaben der Finanzaufsicht? \(Tagesschau, 29 January 2026\)](#)

Chainalysis: Crypto crime hits record levels as state actors expand on-chain activity

Blockchain data platform Chainalysis' 2026 Crypto Crime Report, published on 17 December 2025, revealed that illicit cryptocurrency activity reached record levels in 2025, partly due to the increasing participation of nation-states in on-chain ecosystems. The report emphasised that the adoption of cryptocurrency continued to expand rapidly, with stablecoins demonstrating a high demand for fast, low-cost cross-border transactions that are available 24/7.

A key structural shift identified in the report lies in blockchain transparency, which enables the real-time tracing of transactions and provides an unprecedentedly transparent, immutable and publicly accessible financial record. This transparency enables financial institutions and authorities to analyse value flows, detect patterns and improve compliance frameworks more effectively than in traditional, fragmented financial systems.

Despite these advantages, illicit activity has become increasingly professionalised, with criminal organisations operating sophisticated infrastructures to support money laundering and other illegal services across borders. Notably, nation-states are now leveraging these networks or building their own systems to evade sanctions on a large scale, which significantly raises the risk to both consumer protection and national security.

The report identified the Chinese cybercrime ecosystem as a central hub for large-scale scams, human trafficking, underground banking and money laundering. It also highlighted that illicit crypto activity is becoming deeply interconnected with geopolitical dynamics, reflecting a convergence of organised crime and state interests.

Link:

[The Chainalysis 2026 Crypto Crime Report \(Chainalysis, 17 December 2025\)](#)

FATF warns on offshore virtual asset service providers

On 11 March 2026, the FATF published a report on the risks posed by offshore virtual asset service providers (VASPs), focusing on how these providers can exploit regulatory gaps across jurisdictions.

According to the report, these providers may facilitate money laundering, terrorist financing and sanctions evasion by operating without a meaningful physical presence or by serving customers abroad from loosely supervised locations. It emphasised that illicit actors could exploit offshore structures to conceal ownership, transfer funds swiftly and complicate supervision and enforcement.

The FATF also cited cases in which offshore VASPs had been associated with fraud networks, ransomware-related activity, and the transfer of funds for terrorist activities. In order to mitigate these risks, the report recommended stronger licensing or registration regimes, more effective supervision and enhanced international cooperation between relevant authorities. It also emphasised the role of banks and regulated VASPs in identifying and avoiding relationships with unlicensed providers.

Link:

[Understanding and Mitigating the Risks of Offshore Virtual Asset Service Providers \(oVASPs\) \(FATF, 11 March 2026\)](#)

Information security and data protection

EU Commission proposes stronger cybersecurity framework

On 20 January 2026, the European Commission proposed a new cybersecurity package aimed at strengthening the EU's resilience and capabilities in the face of growing cyber and hybrid threats. The proposals include revising the Cybersecurity Act to enhance the security of Information and Communication Technologies (ICT) supply chains.

The proposals also aim to simplify and streamline the certification process for digital products and services used in the EU. The changes are intended to ease compliance with existing EU cybersecurity regulations. According to the Commission, the measures will further support the EU Agency for Cybersecurity (ENISA) in helping member states manage cyber threats. The proposals will be examined by the European Parliament and the Council before they can take effect across the EU.

Link:

[Commission strengthens EU cybersecurity resilience and capabilities \(European Council, 20 January 2026\)](#)

EU Council imposes sanctions over cyber-attacks on member states and partners

The Council of the European Union has adopted restrictive measures against three entities and two individuals responsible for cyber-attacks targeting EU member states and partners. These measures include asset freezes and travel bans, thereby expanding the EU's horizontal cyber sanctions regime.

Among the entities listed is Integrity Technology Group, a China-based company that supplied products used to compromise and access devices in multiple EU member states and beyond. Between 2022 and 2023, the company provided the technical and material support that enabled the hacking of over 65,000 devices in six EU member states.

Another company based in China, Anxun Information Technology, provided hacking services targeting the critical infrastructure and functions of EU member states and other countries. The two Chinese individuals listed by the Council are the company's co-founders and were responsible for cyber-attacks affecting EU member states.

The third entity, Iranian company Emennet Pasargad, unlawfully gained access to a French subscriber database and advertised its contents for sale on the dark web. The company also compromised advertising billboards to spread disinformation during the 2024 Paris Olympic Games and compromised a Swedish SMS service, impacting a large number of EU citizens.

The Council's decision is based on the EU cyber-sanctions framework, which was established in 2019 and allows for targeted restrictive measures in response to cyber-attacks that constitute an external threat to the EU or its member states.

Link:

[Cyber-attacks against the EU and its member states: Council sanctions three entities and two individuals \(European Council, 16 March 2026\)](#)

ChatGPT vulnerability exposed sensitive data risk

Media reports on 2 April 2026 indicated that a recently disclosed security flaw in AI platform ChatGPT had briefly allowed sensitive conversation data to be extracted without the knowledge or consent of users. According to Check Point Research, the vulnerability exploited a hidden DNS-based communication path, which could also expose uploaded content and AI-generated summaries.

ChatGPT developer OpenAI has since fixed the problem. The report stated that the vulnerability was fully resolved on 20 February 2026, and that there were no signs of exploitation. Nevertheless, the case highlights that AI platforms can still be vulnerable in ways that are not fully covered by built-in safeguards. For organisations, the incident underscores the need to protect sensitive information shared with AI tools with the same care as data handled in cloud or computing environments.

Link:


[Schwachstelle in ChatGPT ermöglicht Zugriff auf sensible Daten \(Netzwoche, 2 April 2026\)](#)

Media Recommendations




OSINT techniques for foreign-language research (Episode 22, 11 March 2026)

In this latest episode of Integrity Insights, host Filip Brokes is joined by Skip Schiphorst of i-Intelligence, a specialist in multilingual open-source intelligence (OSINT) and online research. Skip manages the company's language-focused OSINT courses, including Chinese, Russian, and Arabic.

 [Listen to the episode here](#)


The evolution of open-source intelligence: a conversation with Nico Dekens (Episode 21, 11 February 2026)

In this episode, Filip talks with Nico Dekens, a recognised authority in the world of OSINT. Nico shares his insights into the evolving OSINT landscape, the tools and techniques he uses, and the ethical considerations of this critical field. They dive into how OSINT has changed over the years, with new technologies such as AI revolutionising the process, but also the complexities of using these tools responsibly.

 [Listen to the episode here](#)


AML in Transition: What 2025 meant for compliance in Europe (Episode 20, 26 January 2026)

In this episode of Integrity Insights, Filip is joined by Jennifer Hanley-Giersch to review the biggest AML/CFT developments of 2025. They discuss why the year marked a shift from incremental updates to structural change, driven by AMLA's launch, preparation for the EU Single Rulebook, tougher sanctions expectations and a renewed focus on terrorist financing.

 [Listen to the episode here](#)

Belgium leading the way in the fight against money laundering in European football (Episode 19, 17 December 2025)

In this episode of Integrity Insights, host Filip Brokes is joined by Professor Niels Appermont, a professor of economic law at Hasselt University in Belgium, and an expert in sports law. Niels discusses his research into money laundering in football, with a particular focus on Belgium's fight against corruption and the broader challenges of enforcing anti-money laundering (AML) regulations in the sport.

 [Listen to the episode here](#)



Bad Banker – Geständnisse eines Geldwäschers

Over two episodes, money launderer Ali C. tells his life story and describes how he handled banking transactions for drug dealers in Hamburg.

[ZDF-Mediathek](#)

Coming soon

Anniversary Conference: 10 Years ACAMS Germany Chapter (6 May 2026 in Berlin)

On the occasion of its 10th anniversary, the ACAMS Germany Chapter invites compliance professionals to the conference "Transnational Threats: The EU AML Regulation as a Weapon Against Mafia Networks, Organized Crime Structures, and Terrorist Financing Network".

The event is hosted in cooperation with Mafia Nein Danke e.V. and Counter Terrorism Project Germany, and will take place on 6 May 2026 at 13.00.

The event will focus on the question of which measures can truly be effective in the fight against organised crime. Particular attention will be given to Italy's experience in combating mafia structures, the role of the new European AML framework, the recent German Action Plan to fight organised crime and the lessons that can be drawn for Germany and Europe. Recent developments have pushed terrorist organisations to rely more heavily on criminal sources of funding and organised crime structures – something that needs to be closely monitored. The evening reception at the Italian Embassy includes a key note by Bruna Szego, Chair of AMLA, on "The European Anti-Money Laundering Authority: Shaping the Future of EU AML/CFT".

Link:

[Programme and registration](#)

ACAMS: Assembly Europe (12-13 May 2026 in Frankfurt am Main)

This ACAMS conference provides a deep dive into the recent developments of European nations protecting their economies from illicit activity, aligning with the EU's Single Rulebook standards and getting a grasp on how the AMLA is reshaping compliance. The program will also explore AI-driven threats and defences, the Digital Euro, virtual underground banking, and strategies to combat fraud and sanctions evasion.

Link:

[The Assembly Europe \(ACAMS website\)](#)

Imprint

ALL AML GmbH
Hamburger Bahnhof 1
10557 Berlin
www.allaml.eu/

Amtsgericht Charlottenburg HRB 219815
Managing Directors: Dr. Carsten Giersch, Jennifer Hanley-Giersch

For more information see: <https://allaml.eu/impressum/>

Right of objection and data protection notice

You are receiving this information letter because you are either a client or an interested or associated party.

This newsletter aims to keep you informed about the latest developments in the area of anti-money laundering and terrorist financing. For this purpose, we process your personal data on the basis of Art. 6 (1) p. 1 lit. f) DSGVO or, in case you have given your consent, on the basis of Art. 6 (1) p. 1 lit. a) DSGVO.

If you no longer wish to receive this newsletter, you can opt-out at any time by sending us an e-mail at newsletter@allaml.eu.

For more information on data protection and your rights, please refer to the data protection notice on our website at <https://allaml.eu/datenschutz/>.