

The Legal Quality Standard of Ireland



SEPTEMBER 2026 - ARTICLES & ITEMS OF INTEREST

AML - RED FLAGS & PRACTICAL RISK MITIGATION FACTORS WHERE FUNDS ORIGINATING IN CHINA ARE BEING USED IN AN IRISH TRANSACTION

In the August/September 2026 edition of the Law Society Gazette, Ciara McQuillan, AML executive and solicitor in the AML Section of the Law Society's Regulation Department, has written an article titled 'Chinese Burn'. In this article Ciara McQuillan examines the steps an Irish Solicitor should take where funds originating in China are being used in an Irish transaction.

Chinese controls - China's foreign exchange controls are administered by the State Administration of Foreign Exchange (SAFE). These controls apply to both individuals and corporate entities. In the case of individuals, the central feature of the regime is the annual foreign exchange quota of US\$50,000 or its equivalent in other currencies. Each Chinese citizen may, through the authorised banking system, purchase foreign currency up to that limit in a calendar year. The quota is intended to meet ordinary personal needs, such as travel, overseas-education fees, and medical expenses. It is not, in the ordinary course, a lawful mechanism for overseas property investment. Chinese banks are accordingly required to verify the stated purpose of the foreign exchange purchase.

Circumventions - Practitioners should be alert to the principal methods by which value may be moved out of China in circumvention of capital controls. Each method carries distinct AML and evidential risks.

- One method is splitting.
- Another route is underground banking.
- Trade-based manipulation is another route.
- Cryptocurrency may also be used
- Third-country routing creates a further difficulty.

These are all discussed in detail with the concerns and issues of the methods also documented.

Red flags - The following indicators, individually or combined, should alert the solicitor to the possibility that funds from China have been moved in circumvention of capital controls or through underground banking channels:

- Multiple transfers from different named individuals who are not parties to the transaction, with no obvious relationship to the client,
- Funds arriving from third-party personal or corporate accounts without satisfactory explanation.
- Funds routed through intermediate jurisdictions, particularly Hong Kong, Macau, or Southeast Asian countries.
- A client's inability to provide a clear, consistent, and documented explanation of how the funds were accumulated and transferred out of China,
- Bank statements, tax returns, employment records, or other documents that cannot be independently verified or appear inconsistent,
- An amount grossly disproportionate to the client's declared income, occupation, or business activities,
- Source of wealth involving cash intensive businesses where income is difficult to verify,
- Reluctance or inability to provide original Chinese-language documents with certified English translations,
- Funds arriving from a corporate account where the client is not a director or shareholder,
- A structure that appears designed to avoid reporting thresholds or obscure the trail of funds.

The article then sets out the **practical risk mitigation** factors that Solicitors and firms handling transactions involving funds from China should take.

To view this article in full see [Gazette Magazine](#)

AML - NEW SOLICITORS (MONEY LAUNDERING AND TERRORIST FINANCING) (AMENDMENT) REGULATIONS 2026

In the August/September 2026 issue of the Law Society Gazette, Niall Connors, Director of regulation and Registrar of Solicitors has issued a practice note in relation to the new Solicitors (Money Laundering and Terrorist Financing)(Amendment) Regulations 2026 (SI 367 of 2026). These regulations took effect on 1 September 2026.

He states - The new regulations amend the Solicitors (Money Laundering and Terrorist Financing) Regulations 2020 to incorporate the legislative changes brought about by the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2021.

The new regulations do not impose any new obligations on solicitors regarding their statutory AML obligations, nor do they confer any new powers on the Law Society regarding its statutory role as the competent authority for solicitors (in the context of monitoring and securing their compliance with AML obligations).

Solicitors are reminded of their obligations under the current anti-money-laundering legislation, the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (as amended). Solicitors must be able to demonstrate that they have policies, controls, and procedures in place for the prevention and detection of money-laundering and terrorist-financing offences.

AML compliance is assessed by the Law Society's investigating accountants during their routine inspections. Solicitors are reminded that failure to comply with the Solicitors (Money Laundering and Terrorist Financing) Regulations 2020, as amended, may result in one or more of the following courses of action:

- Requirement to take remedial action,
- Requirement to attend a meeting of the Regulation of Practice Committee to explain failure to comply,
- Requirement to undertake professional training in AML/CFT,
- Requirement to undertake an independent AML audit pursuant to regulation 5(10)(c) of the Solicitors (Money Laundering and Terrorist Financing) Regulations 2020,
- Referral to the Legal Practitioners Disciplinary Tribunal.

To view this practice note see [Gazette Magazine](#)

AML COMPLIANCE IS AN ONGOING OBLIGATION

On the 7 September 2026, the Law Society of Ireland top stories published an article titled "Solicitors' AML compliance 'ongoing obligation'".

Niall Cawley in his presentation to the DSBA webinar *Focus on Clients: Care, Complaints, GDPR and AML Considerations* suggested that AML compliance should be treated as an ongoing practice-management obligation, rather than simply a matter of producing a policy for an inspection.

Some of the items discussed in the article include: -

- **AML Business Risk Assessment** - practitioners are reminded of the deadline for the Law Society's anti-money-laundering (AML) thematic review of business-risk assessments is 30 September.

A business-risk assessment (BRA) under regulation 6 should consider the risks arising from the particular nature of the practice, its clients, services, transactions, and geographical exposure.

Factors that may increase risk include:

- One-off or unfamiliar clients,
- Clients based outside the EU,

- Complex or unusual transactions,
- Transactions involving funds or parties from outside the jurisdiction, and
- Circumstances in which the solicitor has limited visibility of the client or the source of funds.
- **Third party funds** - Cawley suggested that practices should consider appropriate safeguards on third-party payments and, where appropriate, require funds to be transmitted through the solicitor acting for the other side, rather than directly from a third party.
- **Document Your Thought Process Forms** - Cawley suggested that practices could record whether the matter presented a low, medium, or high risk and briefly explain the basis for that assessment. The approach should reflect the circumstances of the individual matter. A straightforward probate involving a long-established family home, for example, may present a very different risk profile from an unusual transaction involving an unfamiliar client, overseas parties, or unexplained funds.
- **Suspicious Transactions Reports** - Practices that might need to make suspicious-transaction reports should be familiar with the GoAML reporting facility operated by the Financial Intelligence Unit (FIU), Cawley advised. Registration with the FIU ensures that a practice is set up to make a report if required.

To view this article in full, see [Solicitors' AML compliance 'ongoing obligation'](#)

DPC FINES HSE €645,000

On the 2 September 2026 the Data Protection Commission (DPC) announced its final decision following an inquiry into the HSE's processing of personal data contained in paper records, which were found rotting and covered mould in disused hospitals by urban explorers. The DPC's decision fined the HSE a total of €645,000 and imposed a reprimand and a number of corrective orders.

The DPC's findings identified data protection failings concerning the physical conditions of HSE document storage facilities and the integrity of the documents held within those facilities.

The retention of records by the HSE in an insecure manner beyond the period where they should be retained gives rise to an ongoing significant risk of unauthorised access to and disclosure of sensitive medical information by third parties. There is also the risk of records not being available for other medical care or other legal or regulatory reasons.

The DPC's decision found that the HSE:

- Infringed the principle of integrity and confidentiality of Article 5(1)(f) GDPR and infringed Article 32(1) GDPR by:
 - Failing to ensure appropriate security of the personal data contained in paper records stored and retained by the HSE in its external facilities;
 - Failing to implement appropriate technical and organisational measures, including proper records management processes, mechanisms and controls, to ensure a level of security appropriate to the risk.
- Infringed the principle of storage limitation of Article 5(1)(e) GDPR by failing to retain personal data contained in paper records in a form which permits identification of data subjects for no longer than is necessary.

- Infringed Article 33(1) GDPR by:
 - Failing to notify a breach to the DPC without undue delay, and within 72 hours of becoming aware of it, in respect of St. Loman's Hospital;
 - Failing to notify a breach to the DPC without undue delay, and within 72 hours of becoming aware of it, in respect of the personal data contained in paper records stored and retained in the basement of St. Loman's Hospital.
- Infringed Article 34(1) GDPR by failing to communicate to the data subjects, the personal data breaches which occurred at St. Loman's Hospital and St. Conal's Hospital.

To view this news item in full see [Data Protection Commission announces Final Decision following Inquiry into the Health Service Executive \(HSE\) | 02/09/2026 | Data Protection Commission](#)

WHAT EMPLOYERS NEED TO CONSIDER WHEN IMPLEMENTING SYSTEMS USED IN EMPLOYMENT

The Workplace Relations Commission (WRC) has been designated as a market surveillance authority (MSA) under the EU AI Act and will supervise certain high-risk and prohibited AI systems used in employment.

The WRC has published a note explaining its new role as a Market Surveillance Authority (MSA) and outlining what employers should consider when implementing AI in the workplace, particularly where AI systems are used in employment, recruitment and workplace decision-making.

To view this note, see [WRC Role under EU AI Act - Workplace Relations Commission](#)

DPC PUBLISHES AI INSIGHTS REPORT

On the 25 September 2026 the Data Protection Commission published a new report detailing the DPC's supervision of Artificial Intelligence products and services between 2021 and 2025. The report details a significant increase in AI-related engagements, driven in part by the rapid development of Generative AI in recent years.

This report presents the insights gathered by the Data Protection Commission's Technology Multinational Supervision Unit within the DPC's Supervision Function. Key findings highlight that innovation and rigorous data protection are not mutually exclusive. Through a large number of engagements involving different AI such as Large Language Models and recommender systems, the DPC Supervision Function has secured significant improvements in data protection compliance in the areas of lawful basis, transparency, data minimisation, and the protection of children.

The report demonstrates a number of critical areas of focus for the DPC, particularly the application of Legitimate Interests as a legal basis for AI training, and the necessity of robust Transparency for what is novel technology, often involving opaque and complex processing operations.

While the majority of AI engagements resulted in recommendations being issued, the report also demonstrates the DPC's readiness to urgently intervene where risks to individuals' rights are unsatisfactorily mitigated.

Ultimately, this report serves as both a record of the DPC's actions in regulating emerging technologies such as AI, and as guidelines for controllers, signifying that early regulatory engagement is the most effective path to sustainable, responsible, and data protection and privacy-centric innovation.

To view this report, see [Data Protection Commission publishes AI Insights Report | 25/09/2026 | Data Protection Commission](#)