JENNER & BLOCK

The EU Anti-Corruption Directive: What You Need to Know

Client Alerts

July 7, 2026
By: Christine Braamskamp, Joshua Kell, André Nwadikwa

Directive (EU) 2026/1021 (the Directive) is the most far-reaching development in European anti-corruption law in more than two decades. It harmonises the criminal anti-corruption laws of the participating Member States by establishing a single set of criminal offences, penalties, and prevention duties.[1]

The Directive entered into force on 31 May 2026, but Member States have until 1 June 2028 to transpose its core criminal provisions into law. As the Directive only sets a minimum standard, a degree of divergence between national regimes is expected, with some Member States choosing to impose stricter rules than the Directive requires (so-called 'gold-plating').

In this client alert, we explain what the Directive changes, who is in scope, and the steps that organisations should take before new legislation takes effect.

I. What the Directive Does

The Directive replaces the 1997 Convention on the fight against corruption involving EU officials and the Council Framework Decision 2003/568/JHA on corruption in the private sector, and amends Directive (EU) 2017/1371 on the fight against fraud to the Union's financial interests by means of criminal law. In their place, it imposes a single, harmonised set of criminal offences resting on common definitions.

The harmonised offences cover:

- Bribery in the public and private sectors;
- Misappropriation;
- Trading in influence;
- The unlawful exercise of public functions;
- Obstruction of justice;

- Enrichment from corruption; and
- Concealment.

The offences involve deliberately broad concepts of ‘public official’ and ‘undue advantage’, which extend the Directive’s reach well beyond conduct that most existing national regimes would capture.

Two features stand out:

1. **The broad concept of an ‘undue advantage’**: An ‘undue advantage’ may be tangible or intangible and pecuniary or non-pecuniary, but an advantage is not treated as ‘undue’ where it is permitted by law or limited to a minimal or very low-value gift. The Directive fixes no monetary threshold for this, however, so what counts as a permissible low-value courtesy will vary from one Member State to another. For public sector bribery, there is no need to show that the official acted in breach of duty–the distinction between lawful and unlawful acts becomes relevant only at sentencing–whereas the private sector offence does require a breach of duty.
2. **The broad definition of the concealment offence**: It captures crypto assets and other digital instruments, and may be committed by any person–including a company itself–where tainted property passes through its treasury, M&A, joint-venture, or supply-chain arrangements.

II. The New Offence to Watch: Trading in Influence

The Directive’s most significant innovation is a standalone offence of trading in influence, for which there is no equivalent in most national regimes and no discrete counterpart in either the UK Bribery Act or the US Foreign Corrupt Practices Act (FCPA). The offence criminalises giving or receiving an ‘undue advantage’ (directly or through an intermediary) in order to exert improper influence over the decision-making of a ‘public official’, regardless of whether the influence is real, is actually exercised, or in fact succeeds. The corrupt bargain is itself sufficient: the influence-peddler does not need to be an official, nor to have possessed any influence at all.

III. Who Is in Scope: Jurisdictional Reach

Each Member State must establish jurisdiction where:

- The offence is committed wholly or partly within its territory; or
- The offender is one of its nationals.

A Member State may also extend jurisdiction to conduct committed abroad, for example where:

- The offender is habitually resident there;
- The offence is committed against one of its nationals or residents; or

- The offence is committed for the benefit of a company established in, or doing business in, its territory.

Territorial jurisdiction may also reach misconduct carried out through information systems used within a Member State, regardless of where the underlying infrastructure sits – a potentially significant 'digital nexus' for groups that run centralised or cloud-based IT. The practical effect is broad: companies headquartered outside the European Union, but with EU operations or commercial links, may face enforcement in one or more Member States even for conduct occurring elsewhere.

Enforcement is also likely to become far more robust. Member States must ensure that investigators have access to special investigative tools of the kind used against organised crime and other serious crime, and that authorities can trace, identify, freeze, and confiscate the instruments and proceeds of the offences. Given the scope for cooperation among the European Public Prosecutor's Office, the European Anti-Fraud Office, Europol, and Eurojust, businesses should prepare for the prospect of parallel, multi-jurisdictional enforcement, with conflicts of jurisdiction resolved through Eurojust.

IV. Penalties and Corporate Liability

Corporate liability arises under the Directive on two bases: first, where an offence is committed for the company's benefit by a person in a leading position; and second, where a lack of supervision or control by such a person made the offence possible. The second basis imports a 'failure to prevent' logic familiar from the UK Bribery Act, and represents a material change for those Member States whose existing regimes do not already provide for it.

The financial exposure is also substantial. Member States must set maximum corporate fines at no less than:

- 5% of total worldwide turnover, or €40 million, for bribery and misappropriation; and
- 3% of total worldwide turnover, or €24 million, for trading in influence, obstruction of justice and enrichment.

As these fines are assessed against total worldwide turnover, they will raise the stakes considerably, particularly for large multinational groups.

Beyond fines, the Directive imposes a range of additional sanctions, including:

- Debarment from public tenders and funding;
- Disqualification from business activities;
- Withdrawal of permits;

- Contract annulment;
- Judicial supervision; and
- Winding-up.

V. Compliance Programmes

The Directive formally recognises a genuine, effective, and independently assessed compliance programme, together with prompt cooperation and self-disclosure, as a mitigating factor, whether the programme was in place before or implemented after the conduct came to light.

Two contrasts with the regimes our clients know well are worth emphasising. First, the Directive itself treats an effective compliance programme only as a mitigating factor. It is not, as adequate procedures are under the UK Bribery Act's failure-to-prevent offence, a complete defence, although the Directive leaves Member States free to go further and treat an effective programme as a ground for excluding liability where their national law already does so, as some, such as Italy, do. Companies will therefore need to be able to demonstrate, rather than merely assert, that a programme works in practice, but they should not assume that doing so will defeat liability altogether across the European Union. Second, unlike the United States and the United Kingdom, where deferred prosecution agreements are central to enforcement, the Directive does not harmonise negotiated resolutions, leaving each Member State to develop its own approach, or none at all. The route to, and value of, self-disclosure will accordingly differ markedly across the EU footprint.

VI. Next Steps for Companies

For organisations with a mature UK Bribery Act 2010 or FCPA programme, the Directive calls for recalibration rather than a rebuild. Existing frameworks already address much of the substance of the EU bribery offences, so the priority is to close the gaps–above all on trading in influence–and align policies to the harmonised definitions across the EU footprint. Companies should consider the following steps as a minimum:

- **Run a gap analysis**: Benchmark the existing programme against the Directive's offences and its effectiveness expectations, and identify where policies, procedures, controls, and training must be supplemented. Trading in influence is the first priority, as most existing regimes do not capture it.
- **Map and stress-test trading-in-influence exposure**: Carry out an inventory of every lobbyist, government-affairs adviser, consultant, and intermediary who interacts with public officials in EU markets, and confirm that each provides bona fide, properly documented services. Scrutinise payment arrangements in particular–success or contingent fees tied to government

outcomes, bonuses triggered by contract awards, and open-ended retainers where the value lies in proximity to officials rather than substantive expertise.

- **Strengthen third-party due diligence**: Extend risk-based, documented diligence and ongoing monitoring across agents, distributors, joint-venture partners, intermediaries, and public-sector counterparts, with particular care around state-owned enterprises, privatised utilities, and public-private partnerships.

- **Revisit gifts, hospitality, and codes of conduct**: Review these against the broad 'undue advantage' concept, bearing in mind the absence of a clear de minimis threshold and the variation in what each Member State will treat as a permissible low-value courtesy, and tighten registers and approval thresholds.

- **Map the 'leading position' population**: Identify the individuals whose conduct can trigger corporate liability, and ensure that training, oversight, and controls are proportionate to the risk those individuals create.

- **Widen speak-up channels**: The Directive extends the EU Whistleblower Directive protection to all the offences it creates, so expand internal reporting to capture the full catalogue–trading in influence and concealment included–rather than only the conduct previously covered.

- **Make the programme demonstrably effective**: Ensure it is documented, resourced, tested, and independently assessed, with clear protocols for investigation, escalation, remediation, and voluntary disclosure, and refresh enterprise risk assessments across operations, business lines, procurement, and M&A targets to reflect the longer limitation periods in diligence and provisioning. Given the Directive's extraterritorial reach and the authorities' growing use of data analytics, prepare for cross-border enforcement and coordinated, cross-jurisdictional incident response.

The core criminal provisions must be transposed by 1 June 2028, but the standards the Directive sets are already clear. Companies with EU operations or connections should use the time before then to review their anti-corruption programmes and monitor how each Member State implements the new rules.

Footnotes

[1] The Directive binds all Member States save for Denmark, which does not participate by virtue of its opt-out from EU justice and home affairs measures.

Related Attorneys

Christine Braamskamp
Managing Partner, London
cbraamskamp@jenner.com
+44 330 060 5445

Joshua Kell
Associate
jkell@jenner.com
+44 330 060 5472

André Nwadikwa
Associate
anwadikwa@jenner.com
+44 330 060 5464

Related Capabilities

Anti-Corruption and FCPA

Investigations, Compliance, and Defense

Stay Informed →