TerraLex

EU Update

Legal Insights from Europe's Capital

September 2026 | Edition #4

*This monthly EU newsletter for TerraLex member firms has been put together by **Gecić Law**'s EU Law practice in Brussels, staffed by partner [Anne MacGregor] and associate [Nina Raluca Bucătaru]. The aim is to provide an overview of EU legislative and policy developments and other relevant insights likely to impact TerraLex firm clients globally who do business in the EU market of some 450 million consumers in 27 Member States.*

1. THE THIRD FILING: FOREIGN INVESTMENT SCREENING BECOMES PART OF EU DEAL PLANNING

Foreign investment screening, previously a secondary issue in European M&A, has become a core element of deal planning.

Historically, companies acquiring European businesses concentrated on merger control. The introduction of the Foreign Subsidies Regulation brought additional scrutiny for larger transactions involving foreign financial contributions. Now, FDI screening is emerging as the third key component of regulatory analysis.

In June 2026, the EU adopted a new Foreign Investment Screening Regulation, replacing the 2019 framework. The revised regime aims to create greater consistency across Member States and to prevent transactions involving strategically sensitive European assets from avoiding review due to narrower national rules.

From Cooperation to Mandatory Screening

The EU already operates a foreign investment screening framework, but the current system gives Member States significant discretion. This has led to divergent thresholds, procedures, and timelines across jurisdictions.

The new Regulation reduces that fragmentation by requiring every Member State to maintain a screening mechanism meeting common minimum standards. These include an initial review, generally within 45 calendar days, the possibility of an in-depth investigation, safeguards against circumvention, and powers to review certain transactions after completion.

The Regulation does not establish a single Brussels-based FDI authority similar to EU merger control. National authorities will continue to make screening decisions, but the system will be significantly more harmonised across Europe.

A Common List of Sensitive Sectors

A key change is the introduction of a common minimum scope. Member States must now require prior authorisation for certain foreign investments involving particularly sensitive European businesses. These include:

- companies developing, producing or commercialising dual-use items and defence-related technology;
- businesses involved in semiconductor and quantum technologies and certain artificial intelligence technologies;
- activities involving strategic raw materials;
- certain financial-market infrastructure;
- electoral systems, and
- critical entities in the energy, transport and digital infrastructure sectors.

Member States can still apply their own domestic rules to screen a broader range of transactions.

The Investor May Look European

The revised rules also broaden the ownership analysis. Screening now extends beyond acquisitions where the immediate purchaser is established outside the EU.

The framework also captures investments made through EU entities that are ultimately controlled by third-country investors. Parties must therefore assess the ultimate ownership and control structure, not just the immediate acquisition vehicle.

Therefore, a European holding company does not, by itself, take a transaction outside the FDI screening framework.

The Third Filing

For cross-border transactions, regulatory planning increasingly requires three parallel assessments: merger control, the Foreign Subsidies Regulation and national FDI screening.

Each regime applies different jurisdictional tests and examines a different risk: competition, foreign financial support, and security or public order.

Not every transaction will trigger all three. However, acquisitions involving European targets in sectors such as technology, infrastructure, defence, energy and financial services increasingly require FDI analysis from the outset, alongside merger control.

The Regulation took effect on 16 July 2026. Most substantive provisions will apply from 17 January 2028, allowing Member States time to align their national regimes with the new requirements.

2. THE 24-HOUR CLOCK: EU CYBER INCIDENT REPORTING STARTS IN SEPTEMBER

A new EU cybersecurity deadline takes effect on 11 September 2026, when reporting obligations under the Cyber Resilience Act (CRA) begin to apply.

From that date, manufacturers of products with digital elements must report certain actively exploited vulnerabilities and severe security incidents. An initial notification must be submitted within 24 hours of becoming aware of the event, followed by a fuller notification within 72 hours.

The deadline comes more than a year before the CRA applies in full on 11 December 2027, making incident reporting one of the first significant operational requirements under the new framework.

What is the CRA?

The CRA is the EU's horizontal cybersecurity framework for products with digital elements. Its scope is broad, covering hardware and software made available on the EU market.

The aim of the Regulation is to make cybersecurity part of product compliance.

Once fully applicable, manufacturers will have to meet essential cybersecurity requirements throughout the design, development and maintenance of their products, address vulnerabilities during the support period and provide users with relevant security information. Compliant products will ultimately bear the EU conformity mark.

What Must Be Reported?

The CRA sets out reporting requirements for two main types of events.

The first is an **actively exploited vulnerability**: a vulnerability with reliable evidence of unauthorised exploitation by a malicious actor.

The second is a **severe security incident:** an incident that seriously affects the availability, authenticity, integrity, or confidentiality of a product's data or functions.

The reporting timeline begins when the manufacturer becomes aware of the relevant vulnerability or incident.

Manufacturers are required to submit an initial notification through the Single Reporting Platform without undue delay and in any case within 24 hours. A more detailed report must be provided within 72 hours. For actively exploited vulnerabilities, a final report is due no later than 14 days after a corrective or mitigating measure is available. For severe security incidents, the final report must be submitted within one month of the 72-hour notification.

For manufacturers used to conduct internal investigations before deciding on notification, these deadlines allow limited time for assessment. Within 24 hours, companies must determine whether the CRA applies, evaluate the event and coordinate both legal and technical responses.

The Practical Challenge

For manufacturers, the main challenge is not just identifying a cyber incident. It is also determining, without delay, whether the incident falls under the CRA reporting requirements.

This assessment often requires answering several questions at once. Companies must determine if the affected product is covered by the Regulation, which group entity is the manufacturer, whether the event meets the reporting threshold, and who is responsible for submitting the notification.

The analysis does not stop with the CRA. The same incident may also trigger separate obligations under NIS2 or sector-specific cybersecurity rules.

Many see the CRA as a 2027 compliance issue, since most substantive requirements apply from December next year. For incident reporting, though, the key date comes much sooner.

From 11 September 2026, manufacturers supplying covered products to the EU will need to make these decisions within hours, not days.

3. PACKAGING UNDER SCRUTINY: NEW EU RULES TAKE EFFECT

Since 12 August 2026, the EU's Packaging and Packaging Waste Regulation (PPWR) has applied across the Single Market.

The Regulation sets out a directly applicable framework for packaging, but a less obvious effect is how it assigns responsibility. Under the PPWR, a company can be treated as the 'manufacturer' of packaging even if it does not physically produce the box, bottle, or wrapper.

Responsibility may instead fall on the company that places the packaged product on the market, depending on how the packaging is designed, branded, and used.

Who is the Manufacturer?

The PPWR defines 'manufacturer' as including more than just the business that physically produces the packaging.

If packaging or a packaged product is designed or manufactured under a company's own name or trademark, that company may be considered the manufacturer. For sales and grouped packaging, responsibility can also attach to the operator that performs the final processing steps, such as filling or sealing.

This approach can lead to outcomes that are not immediately intuitive. A cosmetics company may outsource both the manufacture of its product and its packaging, but still qualify as the manufacturer where the packaged product is produced under its brand. A retailer using generic transport packaging may simply be a user of that packaging. If the same packaging is produced under the retailer's name or trademark, responsibility may shift.

Likewise, a non-EU manufacturer selling packaged goods into Europe cannot assume that responsibility for the packaging sits with the supplier that physically produced it.

The key practical question is not just who made the packaging, but under whose name it was designed, produced, and placed on the market.

Why the Classification Matters

This distinction brings with it substantive obligations. Manufacturers must ensure that packaging complies with the applicable PPWR requirements, carry out the required conformity assessment, maintain technical documentation and draw up an EU declaration of conformity.

For businesses that have treated packaging as a procurement or logistics issue, this introduces a new layer of product compliance requirements.

The complexity increases when multiple types of packaging are used in a single supply chain. A single shipment may involve sales, grouped, and transport packaging, with responsibility potentially assigned to different operators.

Companies may need to map both the supplier of each packaging component and the entity that legally qualifies as manufacturer for each type.

The Terminology – Producers VS Manufacturers

The PPWR further complicates matters by distinguishing between 'manufacturer' and 'producer.'

The manufacturer is responsible for ensuring the packaging itself is compliant. The producer is the operator with extended producer responsibility obligations in the Member State where the packaging will become waste.

An importer, distributor or direct seller may therefore assume producer obligations in a Member State even where another entity remains the manufacturer of the packaging.

A Difficult Start

The complexity of the new framework has already prompted the European Commission to issue further clarification.

Ahead of the 12 August application date, the Commission issued detailed guidance on how to allocate responsibilities between economic operators and how to treat packaging already circulating in the market.

It also stressed that implementation should avoid unnecessary disruption to trade flows and supply chains. Where authorities identify certain forms of non-compliance, the PPWR provides for corrective action before considering more restrictive measures, such as withdrawal or recall.

This does not amount to a formal grace period. It does, however, indicate that enforcement is expected to be proportionate, particularly during the transition to the new system.

This matters because the PPWR applies to a wide range of businesses, many of which may not have previously considered themselves regulated packaging operators.

The Product Is Only Half the Question

For companies selling into Europe, the practical lesson is that they now need to assess the packaging alongside the product itself.

A perfectly compliant bottle of wine, electronic device or cosmetic product can arrive surrounded by several layers of packaging, each carrying its own regulatory questions.

END