*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. CHILD PROTECTION ONLINE: A COMING OF AGE IN THE EU RULEBOOK

The protection of children online is becoming a central issue in digital regulation globally. Regulators are moving beyond treating it as a platform safety concern, creating new compliance requirements for social media, messaging services, gaming platforms, marketplaces, app stores, advertisers and technology vendors.

In the European Union, legislators are advancing on multiple fronts: age verification, child sexual abuse material, addictive design and potential limits on minors' access to social media. The key point is that regulators are shifting from removing illegal content after the fact to asking whether platforms are built and managed to prevent foreseeable harm to children.

A Global Concern

The issue is global.

In March 2026, a court in New Mexico found that Meta had violated state consumer protection law by misleading users about teen safety and designing its platforms in ways that put young users at risk. The jury awarded the state $375 million in civil penalties, determining that Meta had engaged in unfair or deceptive trade practices and did so wilfully.

New Mexico is among 40 states that filed lawsuits against Meta in 2023, alleging that the company's algorithms and engagement-driven design features were intended to increase usage among minors.

Australia has taken a legislative route, passing measures to restrict social media access for users under 16. These developments have informed ongoing debates in Europe, where policymakers are weighing the introduction of age verification requirements for certain online services.

The EU Legal Basis

In the EU, the Digital Services Act (DSA) is the principal EU framework for regulating online intermediaries and platforms.

The DSA covers a broad range of services, such as social networks, marketplaces, content-sharing platforms, and app stores. Article 28 requires platforms accessible to minors to adopt appropriate and proportionate measures to protect children's privacy, safety, and security. The EU has also published more detailed guidelines on how platforms should protect minors.

Very large online platforms have even stricter rules. They must assess and address systemic risks related to how their services are designed and used.

The European Commission has already launched investigations under the DSA against several major platforms. In February 2026, it issued a preliminary finding that TikTok violated the DSA by using design features like infinite scroll, autoplay, push notifications, and personalized recommendations that may encourage addictive use. The European Commission is also looking into X and Grok to see if they have taken steps to address illegal content, including manipulated sexual images and possible child sexual abuse material. Meta is also facing scrutiny after a preliminary finding that it failed to stop children under 13 from accessing Instagram and Facebook.

The Digital Markets Act (DMA) sits alongside this wider enforcement push, targeting the market power of large digital "gatekeepers". In April 2025, the Commission issued its first DMA non-compliance decisions, fining Apple over App Store steering restrictions and Meta over its "pay or consent" model.

The Emerging Toolkit

- **Age verification and social media thresholds.** On 15 April 2026, European Commission President Ursula von der Leyen and Executive Vice-President Henna Virkkunen announced that a European age-verification app is ready for rollout. The app is intended to help online services confirm users' ages. It does not, however, set a minimum age for social media access. That question is still under review, with an expert group preparing recommendations on online child protection. For now, there is no EU-wide minimum age for social media, but individual Member States are moving ahead. Greece plans to ban social media use for children under 15 from 2027, while France is pushing for a possible "digital age of majority". The app has also drawn scrutiny after researchers reportedly bypassed a demo version in less than two minutes, underlining the difficult balance between child protection, privacy and cybersecurity.
- **Child sexual abuse material.** A proposed EU regulation on child sexual abuse material is moving in parallel. Recent negotiations have focused on the scope of covered

material and providers, as well as how removal and cross-border enforcement would work in practice. One option under consideration is a delisting order, which would require search engines and platforms to keep illegal content out of search results and recommendation feeds. The most difficult question is how to detect this material, especially in private communications.

- **Addictive design.** The European Commission is also preparing a draft Digital Fairness Act. Von der Leyen has said it will target harmful and addictive design practices, including attention-capturing features, complex contracts and subscription traps.

The Brussels Effect

The EU has a long record of exporting regulatory standards to the rest of the world. The GDPR is the classic example. A similar "Brussels effect" may emerge in child online safety.

While social media, messaging, dating and other user-facing platforms will be most directly affected, advertisers, payment providers, telecoms and other businesses supporting online platforms are likely to also be impacted.

2. TERRITORIAL SUPPLY CONSTRAINTS ARE MOVING UP THE EU POLICY AGENDA

Territorial supply constraints (TSCs) are becoming a new pressure point in the push to enhance the functioning of the EU's single market.

At its core, the problem is that retailers in one EU country can be blocked from buying products in another, even when cross-border sourcing would lower costs and benefit consumers. This is at odds with the EU principle that goods must be able to move freely across intra-EU borders.

According to a European Commission study published in July 2020, eliminating these restrictions could cut retailer purchase prices by nearly 9% and lower consumer prices by over 7%, unlocking an estimated EUR 14.1 billion in consumer savings.

The European Commission has now moved the issue onto its list of legislative priorities. In its Single Market Strategy released on 21 May 2025, it committed to developing new tools to tackle what it calls 'unjustified' territorial supply constraints, with a draft law expected by the end of 2026.

What are Territorial Supply Constraints?

TSCs are restrictions imposed by suppliers on wholesalers, retailers or other downstream buyers, limiting where products can be sourced or resold within the EU.

In practice, they are often associated with large brand owners or multinational manufacturers that organise supply along national markets. The restrictions may be direct, such as refusing supply, limiting quantities or imposing geographic restrictions.

They may also be indirect. Differences in packaging, product formats or product content can make cross-border resale more difficult, even where there is no express territorial ban.

Enforcement Lacuna under EU Competition Law

In the absence of specific rules, this problem has been tackled at EU level by competition law, but with only partial success. Competition law applies where there is either an agreement between companies or a dominant market position. As a result, unilateral TSCs imposed by large but non-dominant suppliers often fall outside its scope.

The European Commission has acted where those thresholds were met. In 2019, it fined AB InBev €200 million for abusing its dominant position on the Belgian beer market. The European Commission found that the company had restricted cheaper imports of beer from the Netherlands into Belgium, including by limiting supply to Dutch purchasers and changing packaging to make resale in Belgium harder.

In 2024, the European Commission fined Mondelez €337.5 million for restricting cross-border trade in chocolate, biscuits and coffee products. The case involved both anticompetitive agreements and abuse of dominance and confirmed that the European Commission will pursue market-partitioning conduct where existing competition rules apply.

The difficulty lies outside those cases. A supplier may have enough commercial leverage to influence sourcing and resale, but not enough market power to meet the legal test for dominance. That is the enforcement gap now attracting attention.

The Case for New Rules

The European Commission is therefore now considering whether targeted legislation is needed to deal with unjustified territorial supply constraints.

This would follow a familiar EU pattern. Some practices that are difficult to capture through competition law alone are later addressed through sector-specific or targeted legislation. The food supply chain is one example, where unfair trading practices eventually became subject to a dedicated EU framework.

The European Commission has said it is looking at four different policy options: self-regulation by multinationals, guidelines for national authorities, legislation based on the concept of economic dependence, which would take aim on a case-by-case basis at constraints of trade resulting from unilateral decisions by a multi-national manufacturers and legislation identifying prohibited practices.

A clear prohibition would give retailers and authorities a stronger tool, but could also interfere with legitimate supply-chain management. A case-by-case approach would be more flexible, but potentially harder to enforce.

On 5 March 2026, the European Commission launched a call for evidence on unjustified TSCs, with submissions due by 2 April 2026. A broader public consultation is expected in Q2 2026, with targeted surveys and interviews involving companies, trade associations, consumer organisations and other stakeholders. The European Commission's current indicative timetable points to Q4 2026 for the next formal step.

3. COOKIES CRUMBLE UNDER THE EU'S DIGITAL OMNIBUS

Few features of EU digital regulation are as familiar to internet users as the ubiquitous cookie banner.

In November 2025, the European Commission proposed its Digital Omnibus package, aimed at simplifying parts of the EU's digital regulatory framework. The package includes targeted changes to several major laws, including the GDPR, the ePrivacy Directive, the Digital Services Act, the Data Act and the AI Act.

One of the most practical changes concerns cookies and similar tracking technologies. The goal is to reduce "cookie consent fatigue", i.e. the endless pop-ups that users often accept or reject without real engagement.

What Are Cookies?

Cookies are small text files placed on a user's device when they visit a website. They are processed and stored by the user's browser and can perform essential functions, such as keeping a user logged in, remembering language preferences or maintaining items in an online shopping basket.

However, they can also be used to track users across websites, build profiles and support targeted advertising. This is why cookie rules are closely linked to privacy, data protection and advertising rules.

Cookies are usually divided into two categories. First-party cookies are placed by the website the user is visiting. Third-party cookies are placed by another entity, such as an advertising network, analytics provider or social media plug-in.

The Current Rules

Cookie compliance currently sits between two legal frameworks: the ePrivacy Directive and the GDPR.

The ePrivacy rules govern access to, and storage of, information on a user's device. This includes cookies, tracking pixels, local storage and similar technologies. The GDPR then applies where the information collected or processed qualifies as personal data.

Article 5(3) of the ePrivacy Directive requires users to receive clear and comprehensive information and, in most cases, to give consent before information is stored on or accessed from their device. The rule protects the user's device, or "terminal equipment", and applies whether the information stored is personal data or not.

In practice, this layered structure has made compliance complex. Businesses must navigate both device-access rules and data-protection rules, while users are confronted with repeated consent banners that often do little to improve real choice or understanding.

What the Digital Omnibus Would Change

The Digital Omnibus would simplify the current structure by moving certain cookie and terminal-equipment rules into the GDPR. In practice, this would create a more centralised framework for consent when personal data is accessed or stored on a user's device.

The most visible change would be browser-level consent. Instead of responding to cookie banners website by website, users could express their preferences through one-click choices at browser level. Organisations would then need to respect those choices for a defined period.

For businesses, this could reduce compliance friction and improve the user experience. For users, it could make privacy choices more consistent and less repetitive. However, if users can reject tracking more easily and centrally, consent-based targeted advertising may become harder to sustain.

The Digital Omnibus has also triggered a broader debate about the GDPR definition of "personal data". Under the European Commission's proposal, information would not automatically be treated as personal data simply because someone, somewhere, could identify the individual. The proposed change was intended to clarify the scope of the GDPR, but it quickly became controversial.

The European Data Protection Board and the European Data Protection Supervisor warned that the change could narrow the GDPR's scope and weaken individual rights. Reports indicate that Member States have moved to remove the proposed change from the compromise text.

The European Commission presented the Digital Omnibus package on 19 November 2025, and the proposal still needs to be negotiated by the European Parliament and the Council. Businesses affected by the proposed changes should use this window to engage with the co-legislators and ensure that their concerns are reflected before the final text takes shape.

END

Disclaimer: This newsletter contains summaries of general principles of EU law. It is not a substitute for specific legal advice and should not be relied upon in relation to the application of the law or subject matter covered. For further advice on the topics included or any aspect of EU law, please contact Anne McGregor, Partner at Gecić Law in Brussels. Specific member firms can provide advice on the implementation of EU law in their respective jurisdictions – you can find member firms on the TerraLex website: https://www.terralex.org/firms