Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: Tomorrow's Affairs Staff

EU digital rules collide with reality

In November 2025, the European Commission departed from its usual approach to digital policy.

Instead of introducing new, comprehensive regulation, it presented a proposal called the Digital Omnibus, which aims to intervene within the existing regulatory framework.

This package introduces changes to several current digital regulations, intending to remove overlaps, simplify procedures, and reduce the administrative burden for companies and public institutions.

The Commission justifies this approach by citing the need to improve the practical application of the rules and to increase the competitiveness of the European economy without introducing new obligations as such.

This issue does not concern the content of a single regulation but rather the European Union's ability to manage and enforce the regulatory system it has created.

The European economy has long faced low growth, increased security spending, and growing dependence on technologies developed outside the Union. In such circumstances, any additional regulatory burden has immediate economic consequences.

If the Digital Omnibus results only in superficial changes, without real simplification and clearer application rules, the Union will further undermine economic confidence in its regulatory policy.

Conversely, an excessively aggressive reduction of obligations risks weakening existing data protection mechanisms and other fundamental rights that have been embedded in the European legal framework for years.

It is precisely this balance between the system's manageability and the preservation of standards that makes this package politically sensitive and explains why the debate surrounding it extends beyond technical legislative issues.

The seriousness of this proposal is evident in the response of the institutions responsible for data protection.

The EDPB (European Data Protection Board), which brings together national supervisory authorities, and the EDPS (European Data Protection Supervisor), responsible for the institutions of the European Union, published a joint opinion on the Digital Omnibus on 11 February.

In that document, they supported the intention to make the rules simpler and more applicable but clearly warned that reducing the administrative burden must not lead to a weakening of existing guarantees of privacy and other fundamental rights.

Their message is clear: technical corrections are acceptable only if they do not alter the essence of the protection system already in place.

Formal compliance without legal certainty

The essential issue that the Digital Omnibus raises is not normative but operational.

The European regulatory system has reached a point where formal compliance no longer guarantees legal certainty, either for companies or for supervisory authorities.

Overlapping rules, varying deadlines, inconsistent definitions, and parallel oversight regimes have created an environment where mistakes occur not due to negligence, but because of the system's complexity.

> The reason the Union has reached this stage lies in the way digital regulation has been conducted over the past decade

This is precisely where the Commission seeks

to intervene – not by changing the political objectives of the regulation, but by attempting to re-establish control over how these rules are implemented in practice.

The reason the Union has reached this stage lies in the way digital regulation has been conducted over the past decade.

Regulations were adopted more quickly than institutional and technical capacities were developed for their consistent application.

The result was not greater legal certainty but increased complexity of the system, with overlapping requirements and responsibilities dispersed among multiple supervisory bodies.

Effects on the economy and citizens

For much of the economy, this has meant a continual rise in compliance costs, especially for medium-sized companies that lack the resources for permanent legal and technical adaptation.

The same events or risks are often subject to different reporting obligations, with varying deadlines and criteria, complicating planning and increasing regulatory risk.

From the perspective of citizens, the consequences of this process are evident in their daily interactions with digital services.

> Instead of giving users real control over their own data, in practice they have become a routine of automatic acceptance

The number of mandatory notifications users must receive or confirm has grown significantly, from messages about data processing and cookie consent to notifications about changes to terms of use.

These notifications are often lengthy, legally complex, and similar to one another, as they stem from different regulations requiring the same information to be communicated in multiple ways.

Instead of giving users real control over their own data, in practice they have become a routine of automatic acceptance, reducing both understanding and the effectiveness of the protection the rules formally guarantee.

Data protection as a central point of contention

The Digital Omnibus is primarily an attempt to make the regulatory system functional again, not a signal to abandon regulation.

The European Commission states that the aim of the proposal is to simplify the application of existing rules, making them more predictable, so that harmonisation ceases to be a source of continuous costs and legal uncertainty.

Such an approach requires a significant revision of the existing framework, as the proposed changes affect regulations that form the core of European data protection policy and digital rights.

The joint opinion of the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) clearly states that the Digital Omnibus introduces changes to the General Data Protection Regulation (GDPR), the ePrivacy Directive, and several regulations governing data management and cyber security.

The most sensitive aspect of this package concerns data

protection, as the GDPR has, over the years, become a central normative pillar of European digital policy

Because of its broad scope, the proposal is significant beyond technical harmonisation and raises the question of how to simplify the system without weakening the standards on which it is based.

The most sensitive aspect of this package concerns data protection, as the GDPR has, over the years, become a central normative pillar of European digital policy.

Its implementation has established high standards, but it has also created numerous practical problems, particularly where it intersects with rules on the privacy of electronic communications and with new obligations in data management and cyber security. It is precisely in these areas of overlap that the greatest legal uncertainty has arisen.

Efforts to reduce this uncertainty inevitably acquire a political dimension. Any intervention in definitions, legal bases for processing, or exceptions to the general rules is interpreted as a potential deviation from the current level of protection.

This is why the competent regulatory bodies responded immediately and publicly. Their opinion serves as a clear warning to legislators that simplification can only be accepted if it does not undermine the basic principles of data protection on which the entire system is built.

Artificial intelligence, cyber security and competitiveness

Another politically sensitive point for the Digital Omnibus is its intersection with the AI Act. Within European institutions, there has been a debate for months about whether the regulatory pace has been too rapid at a time when global competition in artificial intelligence is intensifying.

While the United States and China promote development through capital, infrastructure, and industrial policy, the European framework is increasingly viewed in terms of costs and implementation risks.

In this context, delaying the deadlines for the strictest rules on high-risk artificial intelligence systems is more important than just changing the schedule.

For some, it is an attempt to give European companies time to adapt and prevent further loss of competitiveness. For others, it signals a concession to industry pressure and an acknowledgement that the existing regulatory framework is too ambitious for the market's real capacities.

The Commission, however, maintains that this is not about abandoning the basic rules but about adjusting their application so that the system remains viable and practical.

Discussions about the Digital Omnibus often overlook a key problem. The debate is often reduced to simplistic divisions between alleged leniency towards big tech companies and the defence of citizens' interests, although the real issue lies elsewhere.

The European Union faces a risk that is not political but managerial. When a regulatory system becomes too complex and inconsistent, its ability to produce predictable and fair outcomes is weakened.

> The Digital Omnibus should be seen as an attempt to remove practical obstacles that have accumulated in the application of European digital rules

In such a setting, the most resourceful actors benefit, not those the regulation is meant to protect. Large companies can absorb the costs of constant legal adjustment and navigate a complex system without major consequences.

In contrast, medium-sized enterprises, new technology firms, and public institutions face ongoing uncertainty and rising costs, as they

lack the capacity to continuously interpret and apply rules whose complexity is ever increasing.

The Digital Omnibus should be seen as an attempt to remove practical obstacles that have accumulated in the application of European digital rules.

These obstacles are not of a single nature. Part of the problem is legal, part is administrative, and part concerns system security. In the field of cyber security, this is particularly evident.

Parallel incident reporting regimes, with different deadlines, criteria, and competent authorities, can slow down the response in a crisis rather than speed it up.

When an organisation, at the moment of an attack, must consider to whom, how, and under which rule to report an incident, formal compliance becomes more important than operational efficiency.

The difference between these approaches often determines whether an incident remains under control or escalates into a wider disruption.

The legislative and political test of the Digital Omnibus

At the same time, this package has broader political significance because it directly affects the Union's relationship with its own citizens.

For years, European policy has rested on the claim that high standards of privacy protection are not opposed to innovation but rather represent its normative basis. The Digital Omnibus puts that claim to the test.

If simplification is reduced to the weakening of protective mechanisms, citizens' trust in the European model will be seriously undermined.

If, however, it proves possible to remove unnecessary complexity without affecting the substance of the law, the Union could demonstrate that it is capable not only of enacting ambitious rules but also of keeping them functional in practice.

At this stage, the legislative procedure, which is just entering its most sensitive phase, plays a crucial role.

The European Commission's proposal represents the starting point, while the actual content of the package will be shaped through negotiations between the European Parliament and the member states.

> European companies are heavily dependent on American platforms, chips, and investment capital

The joint opinion of the EDPB and the EDPS has already set clear boundaries for the discussion, especially regarding privacy protection, which will carry significant weight in the Parliament, where these issues are politically sensitive in the long term.

Simultaneously, strong pressures outside the legislative framework itself will drive the process. The shaping of the final text is also influenced by external economic and political factors, primarily the relationship between the European Union and the American technological market.

Much of the global AI infrastructure is being developed in the United States, while European companies are heavily dependent on American platforms, chips, and investment capital.

Therefore, issues of deadlines and the scope of obligations in the field of artificial intelligence will inevitably be considered through the prism of the competitiveness of European companies in relation to American ones.

This explains why regulatory decisions in this area are not viewed exclusively as an internal legal issue but also as part of the broader economic relationship between the EU and the US.

From stricter privacy oversight to regulatory functionality

It is certain that the Digital Omnibus will remain on the agenda and that the legislative process will be completed, but it is unlikely that all parts of the proposal will pass without significant amendments.

Areas directly related to privacy protection, primarily regimes based on the GDPR and rules on the privacy of electronic communications, will be subject to stricter supervision and additional tightening.

The parts of the package related to reducing the administrative burden and better harmonising procedures have a much higher chance of being accepted - European Commission

The reason for this is not exclusively political but stems from the institutional logic of the Union. At a time when the EU is already facing criticism for lagging in the development and application of artificial intelligence, a loss of credibility in the field of data protection would represent a serious political and normative setback.

Conversely, the parts of the package related to reducing the administrative burden and better harmonising procedures have a much higher chance of being accepted.

Where it is apparent that the same requirements produce multiple obligations, there is agreement among different actors.

The economy sees a reduction in costs and legal uncertainty, the public administration sees simpler implementation of regulations, and citizens see fewer formalities that offer no clear additional protection.

More broadly, the Digital Omnibus indicates a change in the way the European Union understands its own regulatory role. The focus shifts from the constant expansion of the normative framework to the question of its functionality.

In this context, the rules are no longer a political symbol but an operating system that must be stable and applicable.

When that system ceases to function in practice, the protection it offers becomes available primarily to those who have the resources to navigate it, while the rest remain burdened by rules that formally exist but do not achieve their basic goal.