MARCH – APRIL 2025

#DeRisk Newsletter

DLA PIPER

Contents

ESG

Veronica Bertocci, Giulia Rodio, **Corporate Sustainability Due Diligence Directive: A new legal framework for sustainable business conduct..... 3**

Cyber

Giulia Zappaterra and Edoardo Bardelli, **Seconds matter: Understanding DORA's real-time response requirements..... 4**

Reinsurance

Francesco Cerasi, Mauro Carretta, **Retrospective reinsurance in portfolio transfers..... 7**

Case law

Valentina Grande, Giulia Indragoli, **Italian Supreme Court – Failure to adopt an adequate technical defense might breach the insured's duty to mitigate..... 8**

Valentina Grande, Giulia Indragoli, **Italian Supreme Court, Third Section, Judgment No. 8224/2025: Liability regimes for defective products coexist, but parties can't combine them..... 10**

The Editorial Team, **Civil Court of Bari issues order on retroactive application of Article 2407 of the Italian Civil Code..... 11**

ESG

Corporate Sustainability Due Diligence Directive: A new legal framework for sustainable business conduct

Veronica Bertocci, Giulia Rodio

On 25 July 2024, Directive (EU) 2024/1760 (known as Corporate Sustainability Due Diligence Directive or CSDDD) entered into force.

The directive presents a new, ambitious regulatory framework that advances responsible business conduct with regard to human rights and environmental protection across global value chains. Member states have to transpose the directive into national law no later than 25 July 2026.

Large companies incorporated in the EU and specific non-EU companies operating in the EU are subject to the directive. The new responsibilities affect enterprises with more than 1,000 employees and a total worldwide revenue of over EUR450 million. Parent organizations of groups that meet these thresholds are also affected.

In the EU marketplace, the same criteria apply to non-EU enterprises that have large revenues. Businesses can also be included depending on earnings from royalties and aggregate turnover across the EU if the business operates via licensing or franchise arrangements in the EU.

Micro-enterprises and Small and Medium-sized Enterprises (SMEs) are explicitly excluded from the immediate application of the directive. But if they operate in value chains, they could be included in larger business partners' compliance protocols.

The directive introduces a thorough due diligence duty, requiring companies to incorporate human rights and environmental considerations into internal policies and risk management frameworks. Companies should pinpoint and gauge actual or potential negative repercussions. They also have to undertake preventative and corrective courses of action, keep watch over action effectiveness, and publish due diligence statements every year.

The directive obliges companies to develop and implement a climate transition plan to ensure they align with the Paris Agreement and broader sustainability objectives as it coordinates with the obligations arising from the Corporate Sustainability Reporting Directive (CSRD).

Companies have to assess and frequently revamp their governance structures, risk oversight protocols and reporting habits to adhere to these new mandates. The legal and insurance sectors are expected to play a key role. They will help businesses create adherence blueprints, handle lawsuit threats, and customize indemnity offerings for new accountability classifications, especially regarding ESG issues and corporate leadership vulnerabilities.

Domestic regulators will supervise and have the capability to undertake inspections and probes and administer penalties for infractions capped at 5% of the firm's worldwide net revenue. The directive establishes a right to civil remedy for victims of corporate contraventions of human rights and environmental benchmarks as it augments avenues to justice and elevates potential litigation vulnerabilities.

The directive will be enacted progressively according to company size and revenue:

- Corporations with over 5,000 employees and EUR1.5 billion in turnover from 26 July 2027.
- Companies with over 3,000 employees and EUR900 million in turnover from 26 July 2028.
- Every other organization included from 26 July 2029. These businesses have over 1,000 personnel and EUR450 million in revenue.

We advise businesses to prepare for these regulatory changes by reviewing current due diligence frameworks and being proactive with respect to stakeholder engagement and sustainability governance. They should also assess the hardiness of their value chains. Taking action promptly will reduce legal and financial hazards and strengthen companies' standing and enable them to succeed in an ever more ESG-centric worldwide market.

Adopting these compliance measures also serves as a strategic safeguard to prevent and manage potential liabilities, including criminal ones, throughout the supply chain. Recent legal cases involving Italian companies have shown that control systems are essential when dealing with third parties.

Cyber

Seconds matter: Understanding DORA's real-time response requirements

Giulia Zappaterra and Edoardo Bardelli

What is DORA?

On 17 January 2025, Regulation (EU) 2022/2554, commonly referred to as DORA (Digital Operational Resilience Act), finally came into effect.

The financial and insurance sectors' increasing reliance on digital technologies makes operational resilience a critical area for regulators. In response, the EU introduced DORA to establish a comprehensive and unified regulatory framework.

The aim of DORA is to ensure that all financial/insurance entities within its scope can withstand, respond to, and recover from ICT-related disruptions and threats.

One of DORA's most impactful components is its structured approach to incident reporting. Beyond the primary regulation, the Regulatory Technical Standards (RTS) – developed by the European Supervisory Authorities (ESAs) – have introduced detailed guidance on how incidents have to be classified, reported and communicated to authorities. This article explores these requirements and what organizations need to do to comply.

Why incident notification matters

In today's interconnected digital ecosystem, a single cyber incident can have a cascading effect across markets, institutions, and even national economies. Quickly and effectively communicating incidents is essential not only for the individual institution's crisis management, but also for systemic risk containment and regulatory oversight.

DORA mandates a consistent and timely process for reporting significant ICT-related incidents, promoting greater situational awareness and regulatory coordination across the EU.

Incident notification requirements under DORA

Under DORA, financial and insurance entities have to:

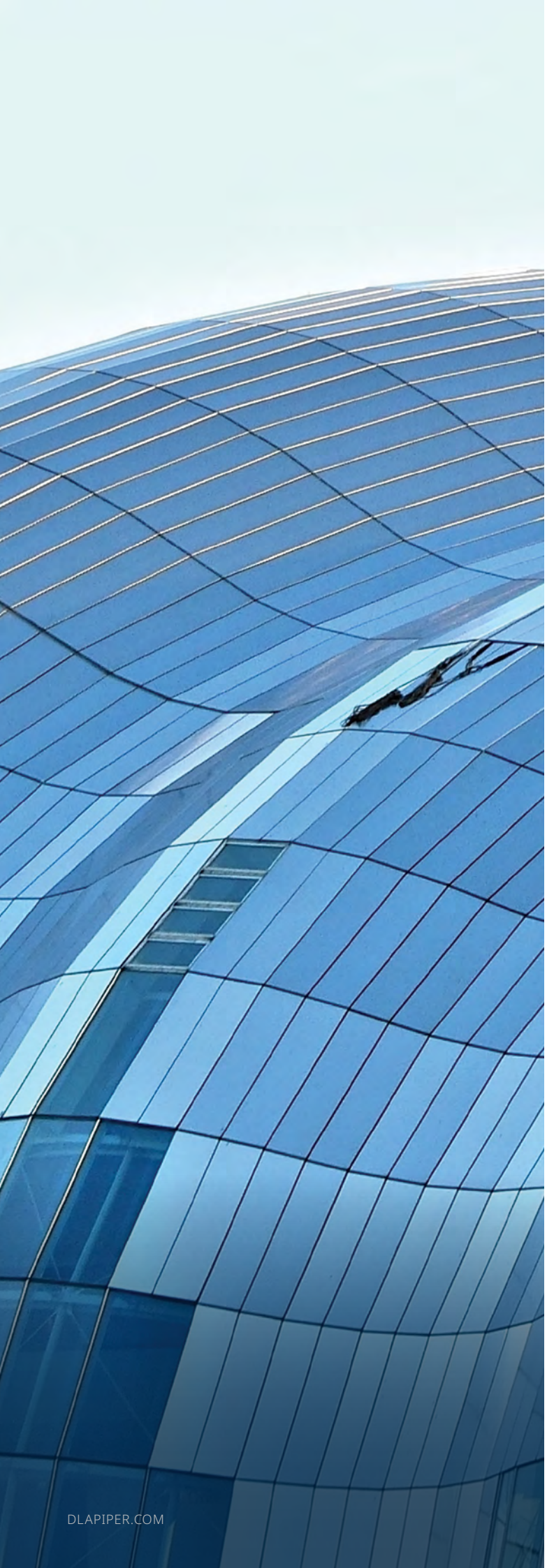
- identify and classify ICT-related incidents;
- report major incidents to competent authorities; and
- share information where relevant with clients and stakeholders, especially if the incident could impact their operations.

The key innovation of DORA is the introduction of a standardized, multi-step incident notification process, enhanced by the RTS for accuracy, timeliness and comparability across institutions.

Classifying major ICT incidents

According to the RTS, a major ICT-related incident is one that meets one or more criteria across several dimensions, including:

- **Client impact:** Affects a large number of users.
- **Duration and service downtime:** Disrupts normal operations for a prolonged period.
- **Geographical spread:** Affects a wide area, spreading in other member states.
- **Economic impact:** Causes material losses.
- **Data losses:** Involves disruption of the availability, authenticity, confidentiality or integrity of data.
- **Criticality of services affected:** Concerns the entity's critical infrastructure.



Entities have to implement an internal classification methodology aligned with the impact assessment thresholds defined in the RTS. This is essential to determine whether an incident qualifies as "major" and is therefore notifiable. When an incident is the result of successful, malicious and unauthorized access, it always qualifies as a major incident, regardless of other thresholds.

Once the incident has been identified as major, DORA establishes a three-stage incident reporting system:

1. **Initial Notification** – Within four hours of determining that an incident is major and no later than 24 hours from the discovery of the incident, the entity has to send an initial report to the competent authority. It should include basic facts: type of incident, services affected, estimated impact, and initial mitigation actions.
2. **Intermediate Report** – Within 72 hours of the initial notification, entities have to provide more detailed information. This includes root cause analysis (if available), full impact scope, and ongoing recovery measures.
3. **Final Report** – Within 1 month, or as soon as a full post-incident review is complete, the entity has to submit a final report. It should contain:
   - root cause and incident timeline
   - recovery effectiveness
   - lessons learned
   - preventative and corrective measures

Entities have to ensure they comply with these timings even if they don't have all the requested information or if the situation hasn't changed between submitting one report and another. In these circumstances, DORA requires entities to submit additional updated reports as soon as the missing information becomes available or the situation changes.

Financial entities can outsource their incident reporting obligations to a third-party ICT service provider. Though they will still be responsible for the obligations.

Interaction with other legal frameworks

DORA's incident notification obligations are designed to complement existing frameworks, such as:

- **NIS2 Directive** (on critical infrastructure cybersecurity) – which doesn't really apply to insurance companies
- **GDPR** (on personal data breach notifications)
- **EBA Guidelines on ICT and security risk management**

Entities subject to multiple regimes have to ensure they have harmonized and coordinated reporting mechanisms to avoid duplication and reporting fatigue. The RTS encourages financial firms to use automated tools and centralized internal systems to detect, classify and report incidents.

The practical impact of DORA on financial entities

DORA has serious ramifications for insurance companies and financial institutions.

To be "DORA-ready," insurance and financial institutions should focus on:

- **Incident response planning:** Ensure existing frameworks align with DORA's definitions, thresholds, and timelines.
- **Tooling and automation:** Adopt systems capable of real-time incident detection and report generation.
- **Staff training:** Operational, IT, and compliance teams have to understand their roles in the notification workflow.
- **Testing and simulation:** Regularly test response and reporting capabilities through tabletop exercises or cyber drills.

While January 17 has already passed, having a full operational system is not something to take for granted. Companies have to constantly improve their overall structure, especially with regard to security and incident notification.

Reinsurance

Retrospective reinsurance in portfolio transfers

Francesco Cerasi, Mauro Carretta

Adverse loss development reinsurance, often referred to as Adverse Development Cover (ADC), is a specialized form of reinsurance designed to protect insurers against unexpected increases in their loss reserves.

This type of reinsurance is particularly valuable for managing the financial risks associated with historical claims, providing a safety net for insurers facing adverse reserve development.

Adverse loss development occurs when the actual losses from past underwriting years turn out to be higher than initially estimated. This can happen for various reasons – changes in the legal environment, unexpected inflation or new information about claims that were previously underestimated. When these losses exceed the reserves set aside by the insurer, it can lead to significant financial strain.

ADC transfers the risk of adverse loss development from the insurer to the reinsurer. This gives the insurer financial stability, allowing them to focus on core operations, without the looming uncertainty of past claims. It also allows the insurer to reallocate capital to more productive uses. And it can enhance an insurer's market value by reducing the uncertainty associated with historical claims.

ADC contracts can be structured in various ways, depending on the insurer's needs. They may attach above, at, or below the booked reserves. And they have to exit above the booked reserves to ensure effective risk transfer.

The attachment point and limit of the ADC determine the extent of coverage provided.

While ADC provides significant benefits, it also comes with challenges.

The first one regards modelling uncertainty. Pricing and reserving ADC involves complex actuarial calculations to ensure the coverage is both adequate and cost-effective. This process requires a deep understanding of loss trends and the ability to model uncertainties accurately. Predicting future loss development is inherently uncertain. Actuaries have to account for various factors, such as changes in legal environments, economic conditions, and claim behaviours, which can affect the accuracy of their models.

Then there are regulatory considerations. ADC contracts must comply with regulatory requirements, which can vary by jurisdiction. Insurers and reinsurers need to navigate these regulations to ensure their ADC contracts are legally sound.

The cost of ADC can also be substantial, especially for insurers with a high risk of adverse loss development. Insurers have to weigh the benefits of ADC against its cost to determine if it's a viable option for their risk management strategy.

One kind of ADC is Loss Portfolio Transfer (LPT). It is a first-euro ADC that transfers the entire portfolio of losses to the reinsurer, provides comprehensive coverage and is often used when an insurer wants to achieve economic finality on its back book.

It's often used in portfolio transfer in combination with a business transfer agreement.

The portfolio transfer process can take time to complete. The LPT agreement provides economic finality as of the date of signing of the business transfer agreement, which provides legal finality only when certain conditions precedent occur, such as regulatory approvals.

To transfer the economic risk and benefits of the targeted portfolio as at the signing date, the transferor and the transferee will enter into a reinsurance agreement. Under this agreement the transferee will reinsure the transferor's liabilities in full under the portfolio. The transferor's direct liability to the policyholders won't transfer to the transferee on signing. This liability will only transfer on completion of the regulatory transfer process or once legal finality is reached.

The LPT reinsurance agreement is a transitional arrangement pending approval of the transfer process and will terminate when the process is complete.

The premium can be a cash sum or possibly investment assets equal to the estimated liabilities as at the accounting reference date. The premium amount will be trued up post signing so that the actual assets transferred are equal to the actual liabilities transferred as at the date of signing. It can also be paid on a funds withheld basis.

Transaction legal documents will also usually include a transitional service agreement for managing claims. The transferor will outsource the administration of the targeted portfolio and claims handling to the transferee, again until legal finality is reached.

Case law

Italian Supreme Court – Failure to adopt an adequate technical defense might breach the insured's duty to mitigate

Valentina Grande, Giulia Indragoli

Factual backgrounds

The case originated when a civil court convicted an anesthetist for medical malpractice after an operation on a newborn child resulted in serious permanent damage.

The trial ended with a compensation order against (among others) the anesthetist. The court didn't accept the defense argument based on the anesthetist's objection to continuing the surgery, giving more weight to the medical records, which hadn't been formally challenged for falsity at any stage of the proceedings.

Later, the anesthetist (Insured) took legal action against her insurer to have the validity of the civil liability insurance policy recognized and to obtain the insurer's payment of the coverage.

First and second instance proceedings

Both the Court of First Instance and the Court of Appeal recognized the Insured's right to compensation, rejecting the objection raised by the insurer that the Insured's defensive conduct constituted a breach of the duty to mitigate provided for by Article 1914 of the Italian Civil Code (ICC).

The insurer challenged the doctor's failure to take, during the indemnity proceedings, specific defensive initiatives, including filing a formal challenge for falsity (*querela di falso*) against the medical records. According to the insurer, the gaps and errors in the defense strategy would have been relevant under the provision, since they could potentially prejudice the insurer's liability exposure.

Conversely, the Court of Appeal held that the duty to mitigate only concerns conducts that could prevent or reduce the damage caused to the third party. Since the alleged procedural mistakes occurred after the damage had already materialized, they were deemed irrelevant in terms of forfeiting the right to compensation, as they didn't fall within the causal chain of the harm suffered by the third party.

The Supreme Court decision (no. 10725/2025)

The insurer appealed to the Supreme Court, claiming the breach and false application of Article 1914 of the ICC, by failing to consider the insured party's insufficient diligence in managing its legal defense.

The Supreme Court upheld the appeal. The court clarified that the duty to mitigate doesn't end with merely preventing the damage, it also extends to conduct subsequent to its occurrence, including conduct aimed at containing or reducing the extent of the damage. As such, the Insured's procedural conduct in liability proceedings brought by the injured third party falls within the scope of application of Article 1914 of the ICC.

The ruling addresses a narrow and traditional reading of the institution, previously confined to tangible actions of prevention or containment. The court recognized that containing legal expenses incurred to resist the injured party's claim falls within the scope of Article 1914 of the ICC. In this sense, the duty to mitigate may even involve abstaining from legal defense if no concrete benefit can be derived from the latter.

More generally, the court specified that the defensive strategies adopted during the action for damages must also be characterized by the diligence of a "reasonably prudent person." So any negligence in the technical defense (such as omitting a formal challenge for falsity, ie *querela di falso*) could be considered a breach of the duty to mitigate, affecting the insured's right to compensation, provided they're not attributable to the insurer or to counsel appointed by the insurer.

Conclusion

This ruling significantly broadens the scope of the duty to mitigate, extending its applicability to procedural behavior. By formulating a clear and innovative principle of law, the Supreme Court confirmed that the duty set forth in Article 1914 of the ICC also applies to how the insured conducts litigation, imposing a standard of diligence and responsibility in managing legal proceedings. This results in a heightened duty of cooperation on the insured, who now has to adopt all measures, including procedural measures, to avoid or minimize the financial consequences of the damage.

Italian Supreme Court, Third Section, Judgment No. 8224/2025: Liability regimes for defective products coexist, but parties can't combine them

Valentina Grande, Giulia Indragoli

Factual background

A leading international biopharmaceutical company was sued to ascertain its civil liability pursuant to Articles 2043 and 2050 of the Italian Civil Code (ICC). A patient was given a flu vaccine that allegedly caused a severe form of encephalomyelitis. The patient subsequently died.

The action was based on the assumption that the drug was placed on the market without adequate prior testing to exclude the risk of serious adverse effects, like those that occurred. The defendant claimed that no liability profile existed, asserting that the vaccine wasn't dangerous, since it had passed all required safety checks and regulatory approvals, and pointing to the previous medical conditions of the injured party.

First and second instance proceedings

The court of first instance partially upheld the plaintiff's claims. It asserted the company's product liability under the Consumer Code because the vaccine was found to be defective due to the lack of adequately conducted clinical studies on the subjects most affected.

Both parties appealed the decision. But the Court of Appeal rejected the appeals, upholding the first instance ruling in its entirety. The Court of Appeal reaffirmed "the existence of a product defect, consisting in the lack of up-to-date and necessary clinical studies on the effects of the vaccine in the elderly individuals with co-morbidities such as diabetes, heart disease and discopathies" and therefore the existence of a causal link between damage suffered and the company's conduct.

The Supreme Court decision

The pharmaceutical company appealed to the Supreme Court, alleging infringement of Articles 117, 118 and 120 of the Consumer Code. It complained that the Court of Appeal had applied a plurality of criteria of judgement, creating an impermissible overlap.

The territorial court initially attributed the case under the product liability rules, which are based on specific assumptions, ie the consumer must prove the damage, the defect in the product and the causal link. Subsequently, its decision was based on the assumptions of Article 2050 ICC (which regulates tort liability in dangerous activities), generating a mixture between the two regulations. The company further objected to how the burden of proof was handled, arguing that defectiveness and causation were presumed.

The court noted that, in cases of harm resulting from administering a vaccine, the legal system allows recourse to different liability regimes, as confirmed by Article 127 of the Consumer Code. It's possible to invoke product liability regime governed by Articles 114–127 of Legislative Decree No. 206/2005, extra-contractual liability pursuant to Article 2043 ICC, and "objective" liability for dangerous activities under Article 2050 ICC. Nevertheless, the court emphasized the impossibility of combining these regimes, each of which is based on its own rationale and distinct criteria of attribution of liability. The overlap of the relevant rules leads to an error of legal classification (subsumption).

Although the Court of Appeal claimed to apply the regime of extra-contractual liability under Article 2043 ICC, it introduced a burden of proof not provided for by that provision; the realising proof of the damaging party.

The ruling effectively ends up altering the nature of product liability rules, bringing it unduly closer to the model set forth under Article 2050 ICC, which entails a duty of ongoing scientific monitoring even after the product has been placed on the market. While the legal system permits the alternative use of different liability regimes, it's essential to emphasize the inadmissibility of combining them. Each regime has to be applied independently and consistently with its own underlying principles and attribution criteria.

The Supreme Court concluded by overturning the second instance ruling and clarifying that, although the injured party is entitled to choose from the various liability regimes provided by the legal system, once the choice has been made, the judge has to apply exclusively the rules specific to the chosen regime, without overlapping criteria derived from other models of liability.

Civil Court of Bari issues order on retroactive application of Article 2407 of the Italian Civil Code

The Editorial Team

On 12 April 2025, Law No. 35/2025, amending Article 2407 of the Italian Civil Code, came into force. It introduces:

- limits on the liability of internal auditors based on remuneration; and
- a five-year limitation period for bringing liability actions running from the date of filing the auditors' report attached to the financial statements for the financial year in which the damage occurred.

As we discussed in previous DeRisk articles, several doubts have been raised as to the retroactive application of this provision.

The case at issue concerns a preventive seizure requested by the bankruptcy receiver of a company against former directors and statutory auditors. According to the bankruptcy receiver, the company had been in a state of decline since 2017: the directors had unlawfully continued the company's activities for years, violating the obligation to provide a true and fair view in the financial statements since 2017, with particular reference to the value of shareholdings, and receivables and payables. The statutory auditors, despite the irregularities ascertained since 2015, hadn't correctly fulfilled their supervisory obligations. They'd failed to report the matter pursuant to Article 2409 of the Italian Civil Code and hadn't requested the liquidation of the company pursuant to Article 2485 of the Italian Civil Code.

In upholding the application for preventive seizure filed by the receiver, the Court of Bari noted the following with regard to amended Article 2407 of the Italian Civil Code:

- With regard to the limits on the liability of auditors, "... it is considered that the new text of paragraph 2 of Article 2407 of the Italian Civil Code also applies to events prior to the entry into force of the law itself, as it is a procedural provision in the broad sense because it merely indicates to the judge a criterion for quantifying the damage (maximum limit), without such an interpretation affecting the very existence of the right to compensation for damage, limiting only the amount with respect to persons who are in any case jointly and severally liable with the directors."
- In reaching this conclusion, the Court of Bari referred to orders nos. 2552/2024 and 8069/2024, in which the Court of Cassation held that the criterion for quantifying damages based on the "difference in net assets" referred to in Article 2486(3) of the Italian Civil Code also applies to proceedings pending at the time of entry into force of that provision of 2019.
- In calculating the ceiling on the liability of auditors, the reference in Law 35/2025 to "remuneration received" means that the net annual remuneration received by the statutory auditor must be taken into consideration.
- With regard to the limitation period, retroactive application has been excluded, since "... the provision on the limitation period governs a substantive legal institution and the legislator has not provided for the applicability of the new legislation to pending proceedings..." Article 11 of *Preleggi* contained in the Italian Civil Code provides that "the law does not provide for the future."

Following the entry into force of Article 2407 of the Italian Civil Code, several scholars have questioned whether the provision can also apply to external auditors. Amendments are being discussed on this and on the retroactive application of the new provision.

In the meantime, we will be monitoring the upcoming court rulings.

Authors

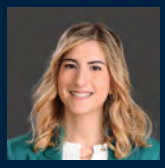
Francesco Cerasi
Partner
T +39 06 68 880 1
francesco.cerasi@dlapiper.com

Veronica Bertocci
Legal Director
T +39 02 80 618 1
veronica.bertocci@dlapiper.com

Mauro Carretta
Legal Director
T +39 02 80 618 1
mauro.carretta@dlapiper.com

Giulia Zappaterra
Legal Director
T +39 02 80 618 1
giulia.zappaterra@dlapiper.com

Edoardo Bardelli
Lawyer
T +39 02 80 618 1
edoardo.bardelli@dlapiper.com



Valentina Grande
Lawyer
T +39 02 80 618 1
valentina.grande@dlapiper.com

Giulia Rodio
Intern
T +39 02 80 618 1
giulia.rodio@dlapiper.com

Giulia Indragoli
Intern
T +39 02 80 618 1
giulia.indragoli@dlapiper.com

dlapiper.com