Newsletter

EHLO, our ICT, IP, media and data protection news - SEPTEMBER 2024

Information technology

Data protection

Intellectual property

Trade Marks & Copyright 2024 - Luxembourg

Digital operational resilience: DORA's implementation roadmap

What happened?

On 16 January 2023, the Digital Operational Resilience Act (DORA) [1] entered into force, after two years of meticulous concoction by the European Union's legislator. DORA's primary objective is to increase the ICT security of financial entities. By harmonising the rules across the EU, DORA is to ensure that the European financial sector remains resilient when confronted with operational disruptions.

In Luxembourg, the Commission de Surveillance du Secteur Financier (CSSF) had already implemented many rules regarding ICT and security risk management. [2] The CSSF has been actively preparing for the upcoming entry into application of DORA by monitoring by anticipation the readiness of Luxembourg financial institutions to comply with DORA's requirements.

In-scope entities and date of application

DORA will apply to most EU financial entities, including credit institutions, payment institutions, electronic money institutions, investment firms, (UCITS) management companies, alternative investment fund managers (AIFMs), insurance companies as well as ICT third-party service providers (including providers of cloud computing services, software, data analytics services and data centres).

To take into account the variety of players involved, their diverse nature and size, DORA provides for a proportionality principle.

In-scope entities will have to be digitally and operationally resilient by **17 January 2025**.

Definition of digital operational resilience

DORA extensively defines digital operational resilience as "the ability of a financial entity to build, assure and review its operational integrity and reliability, either directly or indirectly through the use of services provided by ICT third-party service providers, the

full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions". [3]

In other words, digital operational resilience means the ability to produce, possess and adapt, directly or with the help of ICT third-party service providers, safe, reliable and strong procedures about ICT risk management.

Key obligations imposed by DORA

Based on existing ICT risk management rules, DORA strengthens certain roles and responsibilities of in-scope entities through five pillars, as follows.

1. ICT risk management – governance and organisation

Management bodies of financial entities will play an important role in ensuring compliance with DORA's requirements as they will be responsible for establishing and overseeing internal risk governance and control frameworks. They must ensure the effective and prudent management of ICT risk through a sound, comprehensive and well-documented framework.

2. ICT-related incident management, classification and reporting

Financial entities will have to define, establish and implement ICT-related incident management processes to detect, manage and report ICT-related incidents. Financial entities must be prepared to ensure the integrity and resilience of their processing systems through the recording or classifications of ICT-related incidents and significant cyber threats. The reporting of significant cyber threats and incidents will be harmonised at the EU level through the establishment of a single EU Hub for major ICT-related incidents reported by financial entities.

3. Digital operational resilience testing

Financial entities will have to conduct appropriate testing to ensure the resilience of their ICT systems, at least annually. When identifying potential weaknesses, financial entities will have to fully address potential vulnerabilities. Entities designated by the national competent authority as meeting certain threshold of systemic importance and maturity will have to conduct "advanced" threat-led penetration testing every three years.

4. Managing of ICT third-party risk

As an integral part of their ICT risk management framework, financial entities will have to

manage the risks linked to third-party service providers. Financial entities will have to assess the resilience of their critical service providers. They will also have to ensure that their contractual arrangements for the use of ICT services meet DORA's requirements, while remaining responsible for ICT third-party risk strategies, policies for critical or important functions and register of all such contractual arrangements. Contractual arrangements on the use of ICT services of third-party service providers will have to include certain key contractual provisions. [4] Financial entities will have some obligations to notify regulators with respect to critical or important functions. [5]

5. Information-sharing arrangements

Financial entities may exchange amongst themselves cyber threat information and intelligence to the extent that such sharing aims to enhance the digital operational resilience of financial entities, subject to DORA's conditions.

Anticipation of DORA by the CSSF

On 3 April 2023, the CSSF addressed a compliance preparation survey to a certain number of investment fund managers, enquiring about the gaps identified and mitigation plans for each pillar of DORA. This survey had to be completed and returned by 15 June 2023.

On 5 January 2024, the CSSF published its Circular 24/847 on ICT-related incident reporting framework [6] and the related FAQ. That circular expands the range of ICT incidents to be reported to the CSSF, which was previously limited to "frauds and incidents due to external computer attacks." In this context, Circular 24/847 is set to repeal and replace Circular CSSF 11/504 on frauds and incidents due to external computer attacks as of 1 April 2024. Supervised entities will be required to classify ICT-related incidents based on the criteria indicated in Circular 24/847 and notify major or significant incidents to the CSSF.

Circular 24/847 will enter into force on 1 April 2024 for all supervised entities and on 1 June 2024 for management companies and AIFMs.

The interplay between DORA, the GDPR and NIS 2

While DORA will not supersede the data protection rules set out under the General Data Protection Regulation 2016/679 (GDPR), it is not intended to operate in isolation. As such, DORA complements the GDPR as both regulations share common goals: ensuring the security, confidentiality and integrity of (personal) data and monitoring third-party service providers processing (personal) data on behalf of a principal. The GDPR focuses on 'personal' data protection whereas DORA addresses resilience. The challenge for in-scope entities will be to integrate ICT risk management and (personal) data protection principles

into one comprehensive decision-making process.

On 18 September 2023, the European Commission published its Guidelines on the application of Article 4(1) and (2) of Directive (EU) 2022/2555 (NIS 2). [7] According to Article 4(1) of NIS 2 [8] , where sector-specific legal acts of the EU require essential or important entities to adopt cybersecurity risk-management measures or to notify significant incidents and where those requirements are at least equivalent in effect, the relevant provisions of NIS 2, including the provisions on supervision and enforcement, shall not apply. These guidelines consider DORA as a sector-specific law covering NIS 2, emphasising the fact that DORA applies as lex specialis for financial entities.

Conclusion

To best prepare for January 2025, entities and third-party service providers active in the financial sector must first assess if they fall within the scope of application of DORA (and possibly be designated as having systemic importance and maturity). In-scope entities must assess as soon as possible their ICT management risks and any existing ICT contractual arrangements. All of this is, of course, without prejudice to compliance with CSSF Circular 20/750 on ICT and security risk management, as amended, Circular 21/787 on major incident reporting under PSD2, Circular 22/806 on outsourcing arrangements, Circular 24/847 on ICT-related incident reporting or Circular letters of the Commissariat aux Assurances 20/13 and 21/15 on cloud computing or 22/16 on the outsourcing of critical or important operational functions – to name but a few ICT-related examples.

For more information on DORA and its future implementation, please contact our dedicated ICT, IP, media and data protection team.

1 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector.

2 Such as Circular CSSF 22/806 on outsourcing arrangements or Circular CSSF 20/750 on requirements regarding information and communication technology (ICT) and security risk management.

3 Article 3(1) of DORA.

4 Article 30 of DORA.

5 Article 28(3) of DORA.

6 Please consult: https://www.cssf.lu/en/Document/circular-cssf-24-847/.

7 Please consult: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023XC0918(01).

8 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 – to be transposed by Member States by 17 October 2024. On 21 February 2024, the Luxembourg Government Council approved the bill of law transposing NIS 2 into Luxembourg law. That bill shall hence soon be subject to the legislative process leading to its publication.

AI Act Adopted: introduction to the 458-page EU legislation

What Happened?

On 21 May 2024, the European Council gave its final approval to the regulation laying down harmonised rules on artificial intelligence (the "**AI Act**"), a comprehensive legal framework designed to address the development, placing on the market, putting into service and use of artificial intelligence ("**AI**") systems in the European Union (the " **EU**"). The AI Act marks the EU's first attempt to regulate AI technologies.

After less than three years of legislative negotiations, the AI Act has nearly doubled in volume from its initial proposal – notably adding "general purpose AI models" as a new category of regulated technologies – highlighting its importance on the EU's agenda.

Key Takeaways of the AI Act

The AI Act classifies AI systems into several categories based on the risks they pose to health, safety, and fundamental rights. The level of regulation increases with the level of risk, covering prohibited AI, high-risk AI, other AI systems and general-purpose AI with and without systemic risks.

- **Prohibition of certain AI practices:** the AI Act enforces strict prohibitions on specific AI practices that involve invasive or manipulative techniques leading to potential harm or discrimination. These particularly dangerous AI systems are prohibited in the EU without exception.
- **Heavy obligations for high-risk AI systems:** the AI Act sets stringent requirements for high-risk AI systems. These AI systems are defined according to Annex I and

Annex III of the AI Act, covering products in sectors such as machinery, toys, recreational crafts, personal watercraft, lifts, explosives, radio, pressure equipment, cableways, personal protective equipment, gas appliances, medical devices, civil aviation, vehicles, marine equipment, rail systems, as well as certain products related to biometry and critical infrastructure. This category entails obligations for the AI systems themselves, their providers, importers, distributors, and deployers. Providers have the most numerous obligations, but similar responsibilities extend across the entire value chain (e.g. all of these actors must halt the deployment of a high-risk AI system if they have reasons to believe that it is not compliant with the AI Act).

- **Transparency rules for "other AI systems":** the AI Act specifies transparency requirements for a category of AI systems referred to as "other AI systems", being AI interacting directly with natural persons (e.g. chatbot) or generating multimedia content for various purposes. Providers and deployers of these AI systems must ensure transparency by disclosing to users that such content has been artificially created or manipulated. This appears particularly useful in the age of deep fakes where AI is used to create images of existing persons or places.
- **Limited obligations for general-purpose AI models and general-purpose AI models with systemic risks:** the AI Act defines "general-purpose AI models" broadly as AI models capable of performing a wide range of tasks and integrating into various applications or systems. Providers of these AI systems have minimal obligations. However, many AI systems that fall within a higher-risk category with more extensive requirements are also likely to fall within the general-purpose AI model definition. Additionally, the AI Act introduces "general-purpose AI models with systemic risks" which are general-purpose AI models with high impact capabilities (i.e. using an extremely large amount of computing power for training). These models not only have the basic obligations of general-purpose AI but also additional requirements focused on assessing and mitigating systemic risks and performing model evaluations.
- **Establishment of new governance bodies at the European level:** the AI Act establishes several new European bodies, including (i) an AI Office within the European Commission to enforce the AI Act, (ii) the European Artificial Intelligence Board, comprising one representative from each Member State, to advise and assist the European Commission and Member States in implementing the AI Act, offering advice, recommendations, and opinions on relevant matters, (iii) an Advisory Forum, to provides technical expertise and advice to the Board and the European Commission, and (iv) a scientific panel of independent experts to support enforcement activities upon the request of Member States.
- **Establishment of new national competent authorities:** in addition to the above,

each Member State shall establish or designate as national competent authorities at least one notifying authority and at least one market surveillance authority.

What is next?

Now that the AI Act has been approved, it will be published in the Official Journal of the European Union later this month and will come into force 20 days after its publication. The AI Act will become applicable 24 months from its date of entry into force, but will be implemented in 3 stages:

- **Six months after entry into force:** rules regarding prohibited AI practices will apply.
- **Twelve months after entry into force:** rules for general-purpose AI (with and without systemic risks), the establishment of new EU governance bodies, and national competent authorities will apply.
- **Thirty-six months after entry into force:** rules for some of the high-risk AI systems will start to apply.

Additional European texts are intended to supplement the AI Act in the future, notably the AI Liability Directive and new Product Liability Directive.

At the national level, the CNPD (*Commission Nationale pour la Protection des Données*) announced on 14 June 2024 the opening of applications for their newly launched "Regulatory Sandbox". This collaborative environment allows companies registered in Luxembourg to test the legal compliance of their AI projects with GDPR requirements.

Adoption of eIDAS 2: paradigm shift for digital identity in Europe

What happened?

On 30 April 2024, the eIDAS 2 Regulation introducing a European Digital Identity Framework [1] (also known as "**EUDI**") was published in the Official Journal of the European Union. This regulation amends the eIDAS Regulation [2], in particular by establishing a mandatory European Digital Identity Wallet that can be linked to the national digital

identities of users and by expanding the list of trust services by introducing new qualified trust services.

With the eIDAS 2 Regulation, the European Commission wanted to harmonize and secure digital identification across the European Union with the aim of increasing security on the Internet and protecting users' data, and meet certain interoperability requirements to address the shortcomings of the eIDAS Regulation.

Key takeaways

The ID Wallet

The most significant change of the eIDAS 2 Regulation is the introduction of a fully mobile, secure and user-friendly European Digital Identity Wallet (the "**ID Wallet**"). This ID Wallet is defined as "*an electronic identification means which allows the user to securely store, manage and validate person identification data and electronic attestations of attributes for the purpose of providing them to relying parties and other users of European Digital Identity Wallets, and to sign by means of qualified electronic signatures or to seal by means of qualified electronic seals.*"

This is hence a means of electronic identification, for public or private services, characterised by citizens' full control over their own data and interoperability between EU Member States. The ID Wallet has the structure of a digital 'wallet' in which verifiable data and official documents – so-called 'attributes' – can be collected (including, for example, driving licenses, diplomas and bank accounts).

General requirements for the ID Wallet are laid down to ensure that qualified electronic attestations of attributes by public authorities have the equivalent legal effect of lawfully issued attestations in paper form. The conformity of the ID Wallet with those requirements would be certified by accredited conformity assessment bodies or certified private entities designated by EU Member States. Hence, public authorities or accredited private entities will be able to issue wallets.

New trust services

Another novelty introduced by the eIDAS 2 Regulation is the designation of new trust services such as the electronic attestation of attributes, the management of remote electronic signature and seal creation devices, the electronic archiving (i.e. a service that

enables the receipt, storage, retrieval and deletion of electronic data and documents in order to ensure their durability and readability as well as to preserve their integrity, confidentiality and proof of origin throughout the storage period), or the recording of electronic data in an electronic ledgers (i.e. a sequence of electronic data records that guarantees the integrity of these records and the accuracy of their chronological order).

Various requirements for qualified or non-qualified trust service providers

Qualified trust service providers will be, *inter alia*, subject, at their own expense and at least every 24 months, to an audit by a conformity assessment body in order to verify that they comply with the requirements of eIDAS 2 and Article 21 of the NIS2 Directive, i.e. cybersecurity risk-management measures. [3]

Non-qualified trust service providers will have to comply with notification obligations [4] and other additional requirements for managing legal, business, operational and other direct or indirect risks to the provision of the said non-qualified trust service.

Compliance with the GDPR [5]

The eIDAS 2 Regulation provides that any processing of personal data carried out by the Member States or on their behalf by bodies or parties responsible for the provision of European Digital Identity Wallets as electronic identification means shall be carried out in accordance with appropriate and effective data protection measures. Compliance of such processing with the GDPR shall be demonstrated.

What's next?

eIDAS 2 entered into force on the 20 th day following its publication in the Official Journal of the EU. Implementing acts from the Commission with the technical specifications for the ID Wallet will follow within 6 to 12 months thereafter. By way of illustration, by 21 November 2024 the Commission will have to establish a list of reference standards for the certification of the ID Wallet. Within 24 months from the date of entry into force of the implementing acts, EU Member States will have to make available at least one ID Wallet to all citizens and residents. The Commission will also eventually publish and maintain in a machine-readable form a list of certified ID Wallets.

1 Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

2 Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

3 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

4 Notably in case of any security breaches or disruptions in the provision of the service that have a significant impact on the trust service provided or on the personal data maintained therein.

5 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

Data protection

Implementation of non-performing loans Directive: GDPR implications

What happened?

On 18 July 2024, the Law of 15 July 2024 on the transfer of non-performing loans [1] (the "**NPL Law**") transposing Directive (EU) 2021/2167 on credit servicers and credit purchasers [2] (the "**NPL Directive**") was published in Luxembourg's Official Gazette and is now in force.

A key implementation point is that credit institutions operating under Article 28-3 of the Law of 5 April 1993 on the financial sector engaged in credit management activities in Luxembourg as at 30 December 2023 are allowed to continue these activities until 29 June 2024 or until they obtain a license under the new Article 28-14 of the same law, whichever is the earlier. [3]

That said, we will focus in this article on the interplay between, on the one hand, the obligation of the new NPL Law to provide information to prospective NPL buyers and, on the other hand, the obligations of data protection under the GDPR. [4]

Transparency obligation

The NPL Directive aims at fostering the development of secondary markets for non-performing loans.

Therefore, before transferring non-performing loans, credit institutions must provide potential buyers with certain information on the creditor's rights under a non-performing credit agreement or the non-performing credit agreement itself, and the related guarantees as applicable. Such information should enable prospective credit purchasers to assess the value of the creditor's rights under the non-performing credit agreement or the non-performing credit agreement itself, and the likelihood of recovery of the value of that agreement.

Data protection implications

According to Article 3 §2 of the NPL Law, credit institutions are obliged to provide the information only once during the process, but in any event before the conclusion of the transfer or assignment agreement. Potential buyers are obliged to ensure the confidentiality of the information made available and of business data.

However, in addition, Article 3 §2 of the NPL Law clearly states that, for the avoidance of doubt, the provision of the information concerned by credit institutions to potential buyers applies "in accordance with" the GDPR. In other words, credit institutions cannot rely on their obligation to provide the information alone to justify compliance with the GDPR.

To ensure that prospective buyers have all the information they need to make informed decisions, credit institutions must use the templates provided in the Commission Implementing Regulation 2023/2083 [5] laying down implementing technical standards ("**ITS**") with regard to these templates. The recitals of the Commission Implementing Regulation mention that the information should only be provided to prospective buyers who are seriously interested in purchasing the NPL agreement concerned. The ITS specify which fields of the template are mandatory and provide explicit guidance on the treatment of personal data and confidential information.

More specifically, credit institutions must identify information that is to be considered confidential or subject to banking secrecy and ensure that it remains adequately protected. In addition, the ITS mandate credit institutions and prospective buyers, before

the information is provided, to:

- enter into confidentiality agreements; and
- **share personal data only insofar as necessary** before entering into a contract for the transfer or sale of non-performing credit agreements.

Accordingly, personal data should only be shared **insofar as necessary** before the contract for the transfer or sale of non-performing credit agreements is entered into. In line with the principle of data minimization of the GPPR, which requires that personal data be adequate, relevant, and limited to what is necessary for the purposes for which they are processed, the latter requirement means that only personal data that meets the necessity test can be shared. However, the Commission Implementing Regulation is silent about when and according to which criteria the sharing would be necessary. The criteria for determining when the sharing of information is necessary would be left to the discretion of the parties involved. Nevertheless, it is important to note that some of the mandatory fields include personal data about borrowers who are individuals, such as for example their name, type, postal code, country code, whether or not their residency is in the same country of the credit institution, identifiers internal to the credit institution, some information about the proceedings to which they are subject and some information about the loans themselves and their guarantees.

The necessity test

Therefore, for the moment, the question of the exact necessity test to carry out remains open (except in relation to the mandatory fields mentioned above). That said, the concept of "necessity" is central to GDPR compliance as it is used in 5 out of the 6 available general legal bases for processing personal data. In this context, "necessity" means that the processing of personal data must be strictly necessary (as opposed to simply useful) in light of the legal basis concerned. The concept of "necessity" is also an integral part of the "three-step test" for assessing the principle of proportionality, which plays a key role in the interpretation of the NPL Directive and Commission Implementing Regulation. The necessity criterion requires that any measure taken to achieve a legitimate objective must be necessary, meaning that there are no more protective alternatives that could achieve the same result. By analogy, one could consider that the necessity test to be carried out in the context of the NPL Law is similar. Therefore, the question to consider is the following: how relevant and necessary is it for that prospective buyer to obtain a particular piece of information and consequently for the seller to provide the same to comply with its information obligation?

Subject to concrete assessment of the specific situation at hand, practical examples of possible necessity may include:

- Risk assessment: personal data may be necessary according to the particular credit agreements concerned to assess the risk profile of an NPL portfolio. In certain situations, knowing certain information about the borrower or their credits can be essential for reviewing their repayment and defaults history.
- Due diligence: as part of their due diligence, buyers may, under certain circumstances, need to receive information about certain borrowers to understand their financial status and repayment capacity. This may include, for example, income and employment status, recent bank statements, tax returns or other financial documents that provide insight into the borrower's financial situation.
- Legal and regulatory compliance, including anti-money laundering and counter terrorist financing laws (AML-CTF): a buyer may need to ensure that acquiring the NPL portfolio complies with legal and regulatory requirements in the country where it is located. This may include the necessity to receive records or documentation to perform AML checks.

In each case, the necessity assessment should be documented and the personal data possibly shared should be limited to what is "necessary" for the intended purpose in relation to those individuals in relation to which it is necessary. Irrelevant personal data should be excluded.

The above examples of situations where information sharing could be deemed necessary are for illustration purposes only and a thorough *in concreto* assessment should be carried out in each case to ensure compliance with the necessity test.

Other key considerations

- **GDPR compliance beyond the necessity test:** where personal data are processed, all other requirements of the GDPR must still be complied with.
- **Secure channels for information sharing:** credit institutions should ensure that all confidential information is shared through secure channels. Virtual data rooms or similar electronic means may be used as long as they meet the applicable industry standards for confidentiality and data security.
- **Machine-readable form:** the information should be provided in electronic and machine-readable form, unless credit institutions and prospective buyers agree otherwise.

- **Additional information sharing:** any information that the credit institution wishes to provide which is not identified in the ITS template should not, as a rule, contain any further personal data, in line with the principle of data minimization and the data protection by design and by default.

Key takeaway

The entry into application of the NPL Law marks a significant step towards financial stability by aiming to ensure that prospective buyers have the necessary information to conduct their due diligence. Nevertheless, this progress also requires careful adherence to the principles of the GDPR. This requires credit institutions to share with prospective buyers of NPLs only the personal data that is strictly necessary. It is however not entirely clear yet what personal data may be considered as strictly necessary in this context, except for the data that is mandatory as per the ITS. The credit institutions acting as controllers will have to make and document their assessment in this respect to remain compliant with the requirements of the GDPR while abiding to their obligation of information towards potential buyers.

For more details on the general content of this law, please find our article on the Bill of law No. 8185 here, complemented with this article about the passage of the bill into law.

1 Mém. A, No 292, 18 July 2024.

2 Directive (EU) 2021/2167 of the European Parliament and of the Council of 24 November 2021 on credit servicers and credit purchasers and amending Directives 2008/48/EC and 2014/17/EU.

3 The dates reflect those in Article 57 of the NPL Law, transposing Article 32 of the NPL Directive. This provision aimed to create a temporary grandfathering clause. However, due to the delay in the transposition of the NPL Directive into Luxembourg law, this grandfathering clause became obsolete at the national level. The Directive does not provide for the possibility of extending the grandfathering period beyond the deadlines specified in Article 32.

4 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

5 Commission Implementing Regulation (EU) 2023/2083 of 26 September 2023 laying down implementing technical standards for the application of Article 16(1) of Directive (EU) 2021/2167 of the European Parliament and of the Council with regard to the templates to be used by credit institutions for the provision to buyers of information on their credit exposures in the banking book

Intellectual property

Trade Marks & Copyright 2024 - Luxembourg

Counsel Emmanuèle de Dampierre and associate Florentine Frias contributed to the Chambers Trade Marks & Copyright 2024 Global Practice Guide, offering valuable insights into Luxembourg's trademark and copyright law and practice. Their comprehensive input covers various aspects, including trade mark and authors' rights ownership and protection, trade mark registrations and applications, trade mark opposition procedure, trade mark revocation/cancellation procedure, assignments and licensing, initiating trade mark and authors' rights lawsuits, litigating trade mark and authors' rights claims, defences and exceptions to infringement, remedies, resolving litigation, and additional useful considerations.

The guide was originally published on the Chambers and Partners Practice Guide website.