NautaDutilh

Benelux Technology Law

things you need to know in 2023

Intro

In 2023, we believe that you, as in-house counsel, will have to deal with five main developments in the area of technology and its legal aspects. By anticipating these changes, you can use them to your advantage and prepare for their impact. The five main developments we have identified are:

#1 Continued focus on IT resilience

#2 Shift in platform relations

#3 Increased focus on ESG

#4 Progress of AI legal framework

#5 Changes driven by foreign affairs

#1

Continued focus on IT resilience

In December 2022, the Official Journal of the EU finally published both the adopted Digital Operational Resiliency Act ("DORA") and the NIS2 Directive ("NIS2 Directive"). The legal landscape for IT resilience is now more complete (and busy!) than ever. At the same time, the final version of the updated Dutch Corporate Governance Code ("Code") was published.

↘

With the publication of DORA, the NIS2 Directive and the updated Corporate Governance code the legal landscape for IT resilience is now more complete (and busy!) than ever.

The Code states that companies are expected to pay explicit attention to *digitalisation* and *cybersecurity* when shaping strategy, risk management and in the context of expertise and development of the management and supervisory boards. See our website for more information on the Code.

DORA establishes a set of requirements, from risk management to operational resilience testing, through incident management and reporting in the financial sector at large (with an impressive list of no less than 21 different categories of in-scope entities, from credit institutions to ICT service providers, through crypto-asset service providers and insurance intermediaries!). DORA also regulates the contents of contractual arrangements concluded between financial entities and ICT service providers. The significant amount of work required to comply with DORA from an operational point of view is likely to involve a broad range of services of the in-scope entities, and makes the effective date of 17 January 2025 relatively short notice. Considering DORA in processes and contract negotiations with providers over the course of 2023 seems essential to ensure compliance in time. Still, in the financial sector, the deadline for adoption of the EBA guidelines on outsourcing (for credit institutions, investment firms and payment service providers) was, in principle, 31 December 2021 (or later where provided for in the national implementation), but this is a work in progress for most financial institutions. We expect this topic to remain high on the agenda of many institutions for part of 2023.

The NIS 2 Directive (remodeling of the original NIS Directive) is a further legal text imposing obligations in terms of IT resilience for a list of (highly) critical sectors (most utilities sectors, credit institutions, space sector, manufacturing of important products). Aimed at improving harmonisation of EU requirements, the NIS2 Directive sets specific minimum rules (and ensures consistency with DORA, where needed) in terms of ICT risk analysis and security policies, incident handling, business continuity and crisis management, as well as supply chain security and security in network and information systems acquisition, development and maintenance. Member States have until October 2024 to adopt, publish, and apply measures in line with NIS2. As we expect some Member States to set higher requirements than the minimum rules of NIS2, the implementation process in each

Member State where a business is active is essential to planning of compliance programmes and initiatives before the 2024 deadline.

In parallel, a Proposal for a Regulation on cybersecurity requirements for products with digital elements ("Cyber Resilience Act") is at advanced stages of discussion, aimed at improving cybersecurity in technological products (including hardware and software) designed, manufactured, imported or otherwise distributed within the EU, by establishing minimum cybersecurity requirements for such products. This new initiative demonstrates that cybersecurity must be an essential consideration in the design process of new technological products (and in the review process for importers and distributors), even for consumer-grade products.

Also in the area of cybersecurity, by the end of 2023 the European Commission is to have carried out its first assessment of the Cyber Security Act ("CSA") to determine if any ICT products, processes or services are to be covered by mandatory certification. The CSA lays down the main requirements for European cybersecurity certification schemes in the ICT field which are still voluntary at the moment. Businesses designing, manufacturing or implementing ICT products, services or processes should monitor the outcome to see whether it affects any of their offerings.

#2

Shift in platform relations

↘

With the DMA and the DSA a comprehensive package of legislation establishing new rules for online platforms has been implemented.

In mid-2023 the Digital Markets Act ("DMA"), which entered into force early November 2022, will start to apply. Come 3 July 2023, the largest platforms (both EU and non-EU based) must have notified the European Commission of their core platform services. No later than 6 September 2023, the European Commission will have designated which of these qualify as gatekeepers. After that date these platforms will have 6 months to comply with the obligations in the DMA (i.e. latest by 6 March 2024). For some, the DMA may have far-reaching consequences for their innovation efforts and business models, while for others it may offer opportunities to benefit from a more innovative and competitive business environment. For instance, we can expect (i) the end of platform monopolies (e.g. in hotel booking or car rental markets) because sellers will be free to offer their product elsewhere, and (ii) a better competitive position for non-gatekeeper businesses now that gatekeepers can no longer rank their own products and services above those of other providers. For instance Amazon has recently committed to altering the way data is collected on its online marketplace. In a recent press conference, EU Executive Vice-President Vestager stated that part of these changes concern business practices that are covered by the DMA. Also Google announced that it would let nongaming app developers

to use rival payment systems on its Android operating system for European users. For companies that offer services on the gatekeepers' platforms, or competing digital platforms, it may be worthwhile to analyse the DMA in more detail to see if the new regulatory framework provides a legal basis for a broader offering of services.

The Digital Services Act ("DSA"), which is part of the same set of new rules that aim to create a safer and more open digital space, also entered into force in November 2022. It applies to various online intermediary services, including platforms. The liability exemptions for intermediary service providers ("ISPs"), introduced by the e-Commerce Directive, remain in the DSA. However, in order to avoid liability under consumer protection laws, the providers of online B2C marketplaces will have to ensure that an average consumer does not believe that the information or product is provided by the online marketplace itself, rather than the professional trader using the marketplace. In-scope ISPs will have to comply with specific information and transparency obligations and may have to amend their terms and conditions accordingly. Due to the DSA's extraterritorial scope, ISPs established outside the EU that offer services in the EU must appoint a legal representative in the EU for compliance and supervision purposes. Hosting service providers (even when they are not an online platform or online marketplace) will have to put in place electronic reporting tools that allow users to report any illegal content and are subject to specific additional transparency obligations towards users and notification obligations towards law enforcement and judicial authorities. With the exception of micro and small enterprises, in addition, online platforms will have to provide users with access to internal complaint-handling systems and certified out-of-court dispute settlement bodies for disputes relating to decisions of the online platforms to suspend services or a user's account, for instance. They will also have to give priority to notices submitted by so-called "trusted flaggers", a status awarded by the supervisory authorities, and comply with enhanced transparency obligations. The European Commission has published a useful overview of obligations per different type of online service. Based on the number of active end-users, the Commission will determine whether a platform belongs in the 'very large' category, in which case broader obligations will apply. Platforms have until 17 February 2023 to report the number of end-users on their website. On 17 February 2024, the DSA will become fully applicable for all entities in scope. Apart from a safer and more transparent digital space, the harmonisation of these rules should make it easier for online platforms to start and grow in the EU.

The further development of the metaverse may also cause a shift in platform relations. We expect that in 2023 many more business will follow companies such as HSBC, JP Morgan, Nike and Gucci

to establish a presence in the metaverse. Unlike social media and search engines, which seem pretty well covered by giants such as Google and Meta, there is still everything to play for in the metaverse. 2023 is likely to bring further interesting developments in that area, as the EU will also present an initiative to address virtual worlds, such as the metaverse. The initiative was qualified as "key" by European Commission President Ursula von der Leyen, in the latest State of the Union letter of intent.

#3

Increased focus on Environment, Social & Governance (ESG)

↘

The amount and depth of sustainability reporting is likely to further increase in 2023.

The amount and depth of sustainability reporting is likely to further increase in 2023. At the European level, the most recent examples are the recently published Corporate Sustainability Reporting Directive ("CSRD") and the proposed Corporate Sustainability Due Diligence Directive ("CSDD"). These rules force companies to extend their understanding to their supply chains to analyse potential impacts for sustainability (human rights and environmental impacts). Examples of ESG issues in the technology sector are energy consumption (*e.g.* data centers), staff working conditions (IT service desks, low-wage countries), risks associated with big data / smart technology and facial recognition / surveillance technology, to name a few. The Netherlands has already started drafting a national legislative proposal that covers responsible and sustainable international business conduct (*Wet verantwoord en duurzaam internationaal ondernemen*). Although the larger parts of the relevant EU / local legislation target public interest / listed companies and other companies that meet certain thresholds (relating to net-turnover, number of employees or business sector), we expect that many tech companies will be directly or indirectly affected by the new rules. If not driven by their own intrinsic desire to meet ESG standards, then by their customers' due diligence requests or ethical consumerism.

In the area of governance, we also note that the earlier mentioned updated Dutch Corporate Governance Code has been updated in areas such as long-term value creation, diversity, and the role of shareholders. Management reports for 2023 will need to account for compliance with the updated code for the first time. See our website for more information on the Code.

#4

Progress of Artificial Intelligence (AI) legal framework

Since the first introduction of a Proposal for a Regulation on Artificial Intelligence ("AI Act") in 2021, the text was significantly amended and discussed. The goal is having it on the books by end of the year. The main impact of the AI Act would be on AI

↘

The AI Act will provide different obligations for multiple stakeholders, in particular with regard to high-risk AI systems.

systems classified as "high-risk" in the regulation identified in the latest proposal as:

- in themselves products, or forming part of or used as a safety component of a limited list of products defined in other harmonisation directives and regulations (including, for instance, motor vehicles, medical devices, toys) that are required to undergo a third-party conformity assessment with a view to placing them on the market or putting them into service; or
- expressly listed in the AI Act (such as some specific AI systems used in education, employment, or law enforcement), unless AI's output is purely accessory.

The AI Act provides different obligations for multiple stakeholders: providers, importers, distributors and users. In particular with regard to high-risk AI systems, each operator in the supply chain up to and including the user will have to comply with specific regulatory obligations. Users will, for instance, have monitoring and incident reporting obligations and the obligation to ensure human oversight.

The creation of a supervisory board, the European Artificial Intelligence Board ("EAIB"), inspired by the EU GDPR's EDPB and the EU GDPR's EDPS, is also an important component of the AI Act. The AI Act is without prejudice to the competences, tasks and independence of national data protection authorities which should have access to any documentation created under the AI Act. How the EAIB would collaborate with the European Centre for Algorithmic Transparency ("ECAT"), recently created by the DSA, is not yet clear. In the Netherlands, a new algorithm regulator will become part of the Dutch Data Protection Authority ("DDPA"). For this, the DDPA will set up a separate department. In the initial period, staring from 2023, the activities will mainly focus on identifying high-risk algorithms and gathering knowledge about them.

The AI Act was also completed with a separate (but complementary) initiative: the Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence ("AI Liability Directive") which is aimed at offering effective remedies to people having suffered damages caused by artificial intelligence. The AI Liability Directive introduces a rebuttable presumption of causality in case of non-compliance with a duty of care, and facilitates access to relevant evidence by enabling victims to request the court to order disclosures of information about high-risk AI systems.

We expect 2023 to be an important year in getting closer to final texts. As the deadlines to adapt to such significant changes would be quite short (36 months in the case of the AI Act and 24 months

for the national transposition of the AI Liability Directive), it would be important for relevant stakeholders to monitor the legislative trends, and to consider the probable impacts in 2023.

#5

Changes driven by foreign affairs

↘

In many EU countries, foreign direct investments ("FDI") screening mechanisms are being implemented.

In many EU countries, foreign direct investments ("FDI") screening mechanisms are being implemented (based on the EU FDI Regulation). According to the European Commission's Second Annual report (September 2022) on the screening of foreign direct investments into the Union, the ICT sector accounted for the highest number of notified transactions in 2021 (36% of the total investment activity). In the Netherlands, the Investment Screening Bill (*Wet veiligheidstoets investeringen, fusies en overnames*,"Vifo Act"*)* was adopted in May 2022 and is expected to come into force in early 2023. The Vifo Act is in addition to existing sectoral rules (such as for the telecommunications and energy sectors) and aims to manage risks to national security through an investment test – for both foreign and Dutch investors – involving Dutch based companies in three specific categories. These are (a) vital providers, (b) managers of a corporate campus and (c) companies active in the field of (highly) sensitive technology. Category (c) relates to goods with dual use (civil and military) and military goods. The proposed Dutch Sensitive Technology Decree further refines the scope of 'sensitive technology' and 'highly sensitive technology' and *e.g.* adds four technologies to the scope of sensitive technology: quantum technology, photonics technology, semiconductor technology and high-assurance products. Investments in a company belonging to the categories (a) – (c) will be subject to a prior notification obligation, a standstill obligation and possibly a permit requirement. For highly sensitive technology, the notification requirement applies in case of acquiring (new or increased) significant influence – which already exists at **10%** of the voting rights or when an existing shareholder increases its shareholding to respectively 20% and 25% - and (new) control. In case of sensitive technology other than highly sensitive, the duty to notify exists only in case of acquisition of control. In general, this can be the case for shareholdings of 51% and higher. Compared to other EU countries that have adopted FDI screening mechanisms, the 10% threshold can be considered quite low. When the Vifo Act takes effect, transactions that fall within its scope dating back to 8 September 2020 may also still be reviewed by the Investment Screening Agency (*Bureau Toetsing Investeringen*) upon request of the Minister. The explanatory memorandum clarifies that the retrospective review will be applied with restraint.

The Luxembourg FDI screening mechanism will be introduced by the bill n°7885 and will apply to foreign direct investments made by foreign investors that effectively participate in the

control of a Luxembourg company which carries out critical activities on Luxembourg territory. Among others, the draft bill identifies several technologies as critical. Control can follow from either (i) owning directly or indirectly **25%** or more of the capital of the Luxembourg company, (ii) having a majority of the voting rights of the shareholders of the Luxembourg company, (iii) having the right to appoint or remove the majority of the members of the administrative, management or supervisory body of the Luxembourg company, while at the same time being a shareholder, or (iv) being a shareholder of the Luxembourg company and pursuant to an agreement with other shareholders, controlling a majority of the voting rights.

The Belgian draft bill on FDI screening divides the in-scope foreign investments into two categories. The first category concerns investments through which, directly or indirectly, **25%** of the voting rights are acquired of a company which carries out sensitive activities such as vital infrastructure, resources and technology essential for interests related to security and public order, access to sensitive information and freedom of the media. The second category concerns investments through which directly or indirectly, **10%** or more of the voting rights are acquired of a company which carries out activities related to defense, energy, cybersecurity, electronic communications or digital infrastructure, and has an annual turnover exceeding 100 million euros.

Other developments driven by foreign affairs to be on the lookout for in 2023 are in the area of export restrictions. Reportedly, the Netherlands plans to restrict export to China for chips and/or chip manufacturing equipment. It will also be important to closely follow national and international sanction regulations, including with respect to Russia, Belarus and Iran, so that companies are able to respond to any changes in a timely manner.

About the team

NautaDutilh's Technology & Data Protection Team combines in-depth knowledge and understanding of its clients, their technologies and sectors with a pragmatic approach to resolving legal issues. The team is active at the intersection of technological innovation and the law and focuses on finding creative solutions to technology-driven challenges. Our team members are skilled at advising on fast-growing and emerging new technologies, including cloud computing, cybersecurity, data monetisation, open-source software, AI, OTT, Fintech and distributed ledger technology. The team further has extensive experience in advising clients on the widest range of data protection issues. These include conducting GDPR gap analyses, the drafting and review of privacy statements, advising on international transfers of data, data protection provisions in contracts and employee monitoring, as well as liaising with data protection authorities. The team is regularly praised for its dedication to clients, rapid response time and practical, high-quality advice.

Contact

For more information, please contact

Joris Willems Netherlands
+31 20 71 71 670
+31 6 52 05 03 90
Joris.Willems@nautadutilh.com

Vincent Wellens Luxembourg / Belgium
+352 26 12 29 34
+352 621 15 61 78
Vincent.Wellens@nautadutilh.com

Contributors

Marlous Schrijvers | Cyril Christiaans | Eva Reinders | Sigrid Heirbrant | Sarah Zadeh | Yoann Le Bihan