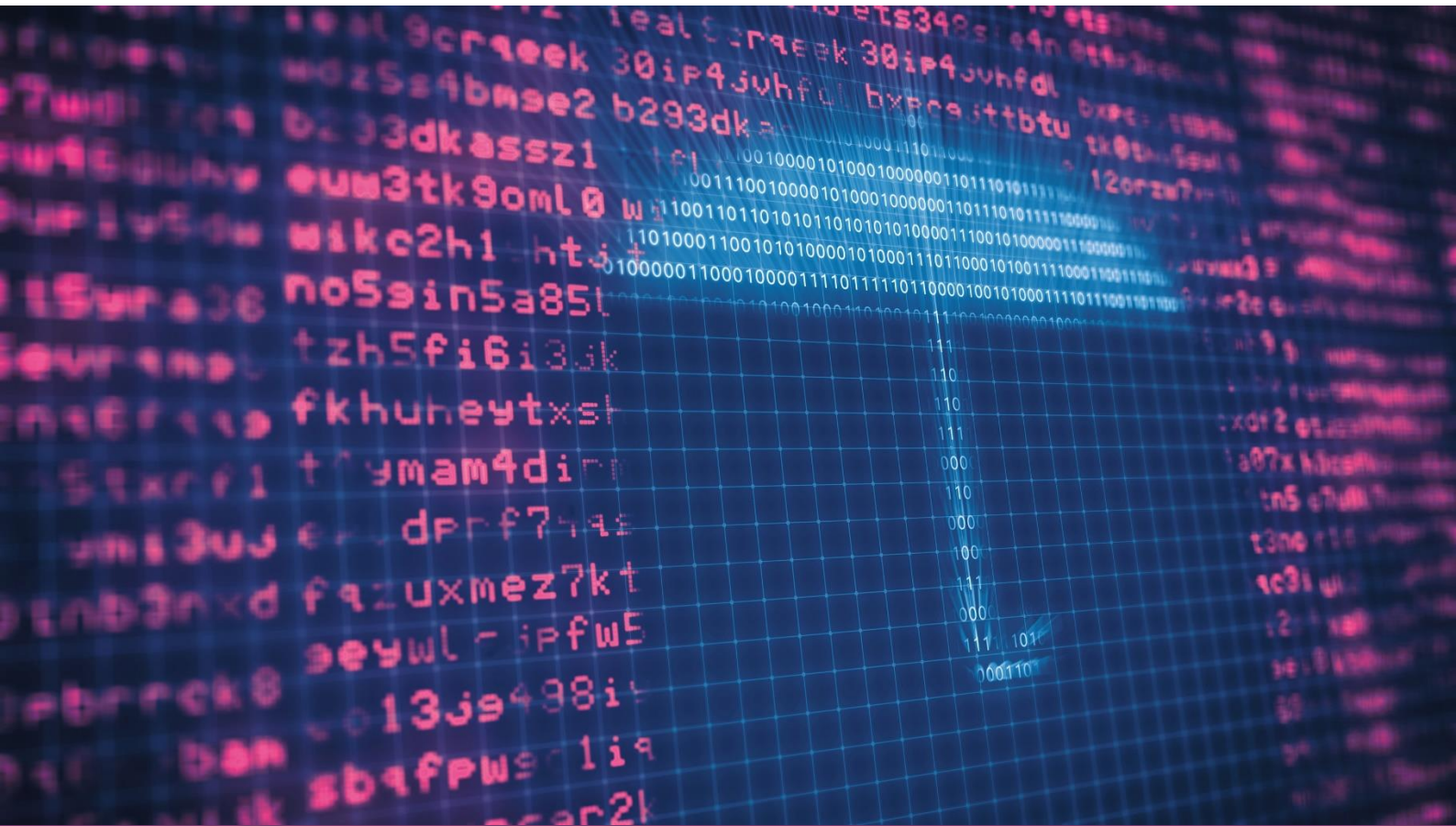
The EU Digital Single Market

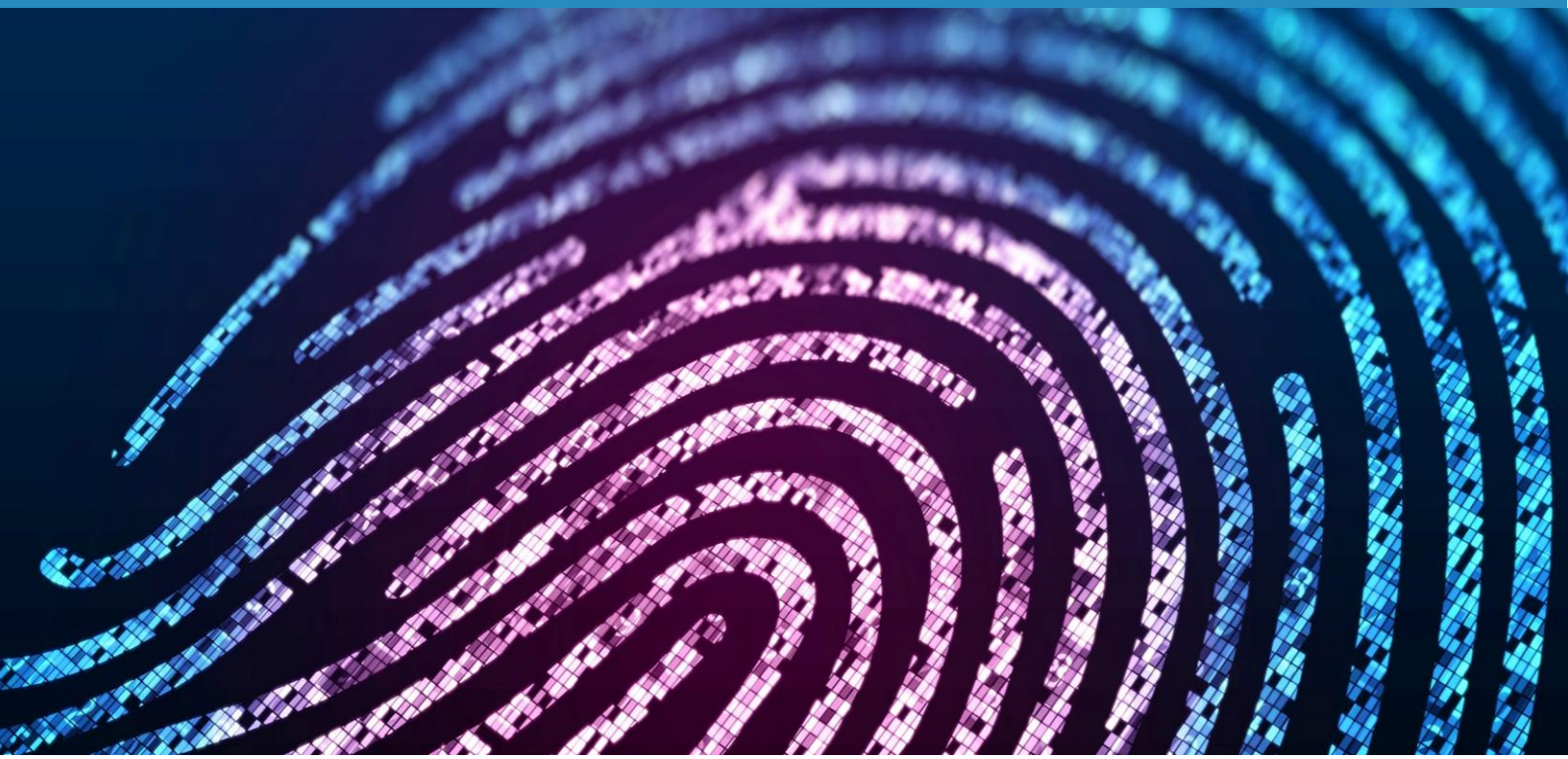
05 December 2022

State of Play

Contents



Introduction



The Digital Single Market strategy is one of the EU's top priorities. Adopted on 6 May 2015, the EU's ambition is to develop the EU into a single digital market and to make the EU's single market "fit for the digital age". On 9 March 2021, the EU Commission presented a vision and avenues for Europe's digital transformation by 2030.

Determined to make this Europe's "Digital Decade", the EU Commission has made several legislative proposals with a view to strengthening Europe's digital sovereignty. These proposals are both ambitious and transformative in nature. The goal is to put Europe at the forefront of technological development (with a strong focus on data, technology, and infrastructure) while protecting the fundamental rights of individuals. They will have a strong impact on the different actors of the digital economy as they increase the level of responsibility and create new obligations.

In this article, we present the state-of-play of the EU's key legislative proposals in the field of data protection, artificial intelligence, digital services and cybersecurity, and we provide a timeline explaining when these new laws come into force. In particular, we look into the future to see how the field of privacy is progressively evolving towards a new area that we like to call: "digital law".

1. Data protection and online privacy

1.1 General Data Protection Regulation

It's been more than four years since the GDPR came into force. Despite some criticisms, overall the GDPR has been a success. It has harmonized the data protection framework across the EU. It has raised awareness on the need to protect privacy and personal data among the various actors of the economy up to the highest levels of management. Individuals are better informed about their fundamental rights and are exercising them more freely. The GDPR has also put the European Union at the forefront of global data protection. The GDPR is recognised as a global standard for the protection of personal data and it has influenced legislators around the globe to adopt their own data protection laws. But most importantly, privacy has become a societal issue. Economists, philosophers, academics, practitioners, lawmakers, historians and data scientists all agree that we are living one of the most defining moments of our time. As we continue to evolve towards an ever more data-hungry society, never has it been so crucial to ask ourselves what world we want to live in and what future we want to leave to the next generations.

In this context, the GDPR represents a pillar on which the EU legislator is building the foundations of a new digital law framework. The variety of legislative proposals put forward by the Commission shows that it is no longer just about personal data. The Commission's proposals intend to regulate the processing of data in general, whether it be personal data or non-personal data. The rights, principles and concepts that are recognised in the GDPR will, however, continue to be the driving forces on which the EU's legislative landscape is built. Concepts such as 'consent' will be used and defined in other legal texts and applied in different situations.

There may be talks about reforming the GDPR. But this does not seem to be on the EU Commission's agenda for the time being. For now, the EU Commission's focus is on creating a comprehensive legislative arsenal that will regulate the digital space as a whole, with GDPR continuing to be one of the EU's founding laws in this field.

1.2 ePrivacy Regulation

Special rules regarding electronic communications have been in place since 2002 in the EU. As part of its Digital Single Market Strategy to reinforce trust and security, the EU Commission has put forward a proposal to replace the existing ePrivacy Directive with a new regulation ("**ePrivacy Regulation**").

1. Data protection and online privacy

The scope: The ePrivacy Regulation aims at providing uniform rules, as it will be directly applicable across the EU (save for a few margins of manoeuvre left to EU Member States). Inspired by the GDPR, the extended scope will have an extraterritorial reach, as it will apply as soon as persons – either end-users or recipients of direct marketing, physical or natural persons - are located in the EU, even if organisations are established abroad, in which case they will have to designate a representative in the EU.

The ePrivacy Regulation touches upon a broad range of topics, which will have various impacts on businesses, such as providers of electronic communications, the ad tech sector as a whole including website publishers and app developers, and more generally, any organisations that carry out online direct marketing in the EU.

Confidentiality of electronic communications: With respect to confidentiality of electronic communications, the ePrivacy Regulation strictly prohibits, as a matter of principle, to process and interfere with content and metadata (incl. location data) of electronic communications. However, the EU co-legislators disagree over the precise list of exceptions to this principle. While the 2002 ePrivacy Directive initially only applied to telecom operators, under the ePrivacy Regulation, machine-to-machine and IoT data transmitted via public networks would also be covered by the new rules.

Online tracking: Regarding online trackers and cookies, the EU co-legislators recognise that there is a need for more exceptions to the obligation to obtain user consent, such as online trackers used for analytics and security purposes. They also wish to address the existing user consent fatigue that results from multiple popups, for example by whitelisting providers or tracking purposes through browser settings. The wording used in the draft ePrivacy Regulation remains technology-neutral and it is yet to be seen whether it will capture the new forms of online tracking that are being developed (e.g. Google's FLoC) while third-party cookies are starting to be blocked by market practices.

Direct marketing: The ePrivacy Regulation does not change significantly the rules on online direct marketing. Nonetheless, the co-legislators disagree on the exact scope of the soft opt-in rule for existing customers. Possibly, this exception will end up being limited to "marketing emails" as opposed to instant messaging. The regime of live tele-marketing calls is also subject to disagreement over the application of a "hard" or "soft" opt-in or an opt-out. In addition, soft opt-in may only be valid for a limited period of time.

Enforcement: Regarding enforcement, the ePrivacy Regulation would empower authorities to enforce administrative fines, similar to the ones provided for in the GDPR. The EU Commission and Parliament have designated competent data protection authorities to enforce the ePrivacy Regulation. To further strengthen harmonisation with the GDPR, they have also provided for the application of the one-stop shop and cooperation and consistency mechanisms for cross-border matters.

Entry into force: The ePrivacy Regulation was initially due to be enter into force at the same time as the GDPR. However, since the Commission's proposal and the vote in the European Parliament in 2017, no less than eight different presidencies of the Council have fiercely discussed the text of the ePrivacy Regulation before finally agreeing on a common position in 2021. The ePrivacy Regulation has now been undergoing the trilogue process, as the Parliament and the Council have yet to find a mutual position. While some progress has recently been made, a number of disagreements remain, e.g. on electronic communications data and cookies. Once adopted, the ePrivacy Regulation would come into force after a period of transition (i.e. two years in the Council's version).

Lastly, the UK also recently showed its intention to reform its own ePrivacy rules, which had been incorporated into national law before Brexit. The Data Protection and Digital Information Bill introduced to the UK Parliament in July 2022 includes modifications to existing UK rules on cookie consent and enforcement powers.

2. Online platforms

2022 marks the adoption of the EU's two new rulebooks: the Digital Services Act ("DSA") and the Digital Market Acts ("DMA"). Both highly impact providers of intermediary services and by extension, their business users and users. Where the DSA intends to reinforce consumer protection on digital platforms, the DMA essentially aims at ensuring a level playing field for all digital companies, big and small.

2.1 Digital Services Act

The Digital Services Act ("**DSA**") intends to build on the rules set out in the e-commerce Directive, that has been the cornerstone for digital services regulation in the EU. It enhances and harmonises consumer protection online. According to the EU, what is illegal offline should be illegal online. However, it is important to understand that the e-commerce Directive will not be repealed but only be amended by the DSA.

The scope: The DSA covers digital service providers that act as intermediaries offering one of the following types of service: (i) a mere conduit service, (ii) a caching service, or (iii) a hosting service. In practice, it means that the scope of the DSA is very broad, covering actors such as internet service providers, domain name registrars, social media networks, messaging services, cloud services, app stores and online platforms and marketplaces.

In terms of territorial scope, the DSA will apply to all online intermediary service providers as long as their users (businesses or individuals) have their place of establishment or residence in the EU. Providers of intermediary services based outside of the EU will also have to comply with the DSA if they direct their services to EU-based users. In such a case, they must appoint a legal representative in the EU, as it is the case under the GDPR.

The DSA tackles two key topics: (i) an update of the e-commerce liability exemptions, and (ii) new transparency obligations for online intermediary services, especially in relation to content moderation and online advertising.

The liability exemptions: The Commission implements the well-known 'mere conduit', 'caching' and 'hosting' liability exemptions from the e-commerce Directive into the DSA to maximize harmonisation across the EU. All in all, no substantial changes were made to the 'mere conduit' and 'caching' exemption regimes.

2. Online platforms

However, the hosting exemption no longer applies to the case where a user buys illegal goods on an online platform if the user is lead to believe that the product is provided by the online platform itself, not by a trader using the platform.
Under the DSA, the providers of intermediary services are still not subject to a general monitoring obligation but proactive investigations conducted by the provider of intermediary services are encouraged.

Transparency obligations: The DSA introduces a series of asymmetric transparency obligations, which break down depending on the categories of intermediary services:

- All intermediary services will be required to establish a single point of contact for communication with competent authorities, to include in their terms and conditions any restrictions that they may impose on their service users, and to comply with transparency reporting obligations (except micro and small enterprises).
- Additionally, hosting service providers will need to put in place notice and action mechanisms to allow third parties to notify the presence of alleged illegal content. Where the provider removes or disables access to its user's content, it must provide such user with a statement of reasons containing specific information.
- Moreover, all online platforms (except micro or small enterprises) will have to set-up an internal complaint-handling system on decisions taken, to engage with certified out-of-court dispute settlement bodies, to cooperate in priority with entities to which status as a "trusted flagger" has been granted, and to take measures against abusive notices etc.
- Finally, very large online platforms ("*VLOPs*"), which dominate the market (reaching at least 45 million users in the EU representing 10% of the population), will be required to conduct risk assessments on the systemic risk regarding the use of their services, conduct mandatory external audits on an annual basis, appoint one or more compliance officer(s), provide access to certain data to competent authorities, etc.
- The DSA prohibits targeted advertising based on special categories of data, as well as targeted advertising to minor.

Enforcement: In terms of enforcement, each Member State will have to appoint a "*Digital Services Coordinator*", i.e. the primary national authority responsible for supervising the intermediary services established in their Member State. However, the EU Commission will maintain supervision, investigation and enforcement powers relating to VLOPs.

In terms of sanctions, the DSA allows for administrative fines up to 6% of the global annual turnover of the intermediary service. In addition, the Commission will also have the possibility to impose periodic daily penalties on VLOPs, which may not exceed 5% of the average daily turnover.

Entry into force: The DSA has been approved and published in October 2022, and will be applicable as of the 17 February 2024. Additionally, VLOPs will have four months from their designation to comply with the new rules.

2.2 Digital Markets Act

With the Digital Markets Act ("**DMA**"), the EU Commission addresses a number of issues identified around unfair business practices of digital players. Thus, the DMA introduces a series of new obligations and tools that should help start-ups and smaller companies to compete with 'Big Tech'.

Scope: The DMA applies to so-called "gatekeepers" that offer "core platform services", which includes amongst others: (i) online intermediation services, (ii) online search engines, (iii) online social networking services, (iv) video-sharing platform services, (v) number-independent interpersonal communications services, (vi) operating systems, (vii) web browsers, (viii) virtual assistants, (ix) cloud computing services and (x) actors in the adtech ecosystem.

A provider of core platform services will be designated by the Commission as a "gatekeeper" if (i) it has a significant impact on the internal market, (ii) it operates a core platform service which serves as an important gateway for business users to reach end users, and (iii) it enjoys an entrenched and durable position in its operations or it is foreseeable that it will enjoy such a position in the near future.

The DMA contains a number of legal presumptions, for example, when the core platform service provider provides its services to more than 45 million monthly active end users in the EU and to more than 10.000 yearly active business users in the EU, and when its group of companies achieve an annual EEA turnover equal to 6.5 billion in the last three financial years.

Furthermore, based on a set of additional criteria, the Commission may designate core platform service providers as gatekeepers even if they do not meet all the thresholds mentioned above.

2. Online platforms

In terms of territorial scope, the DMA applies whenever a gatekeeper offers the core platform services to business users or end users established in the EU irrespective of whether the gatekeeper itself is based in the EU.

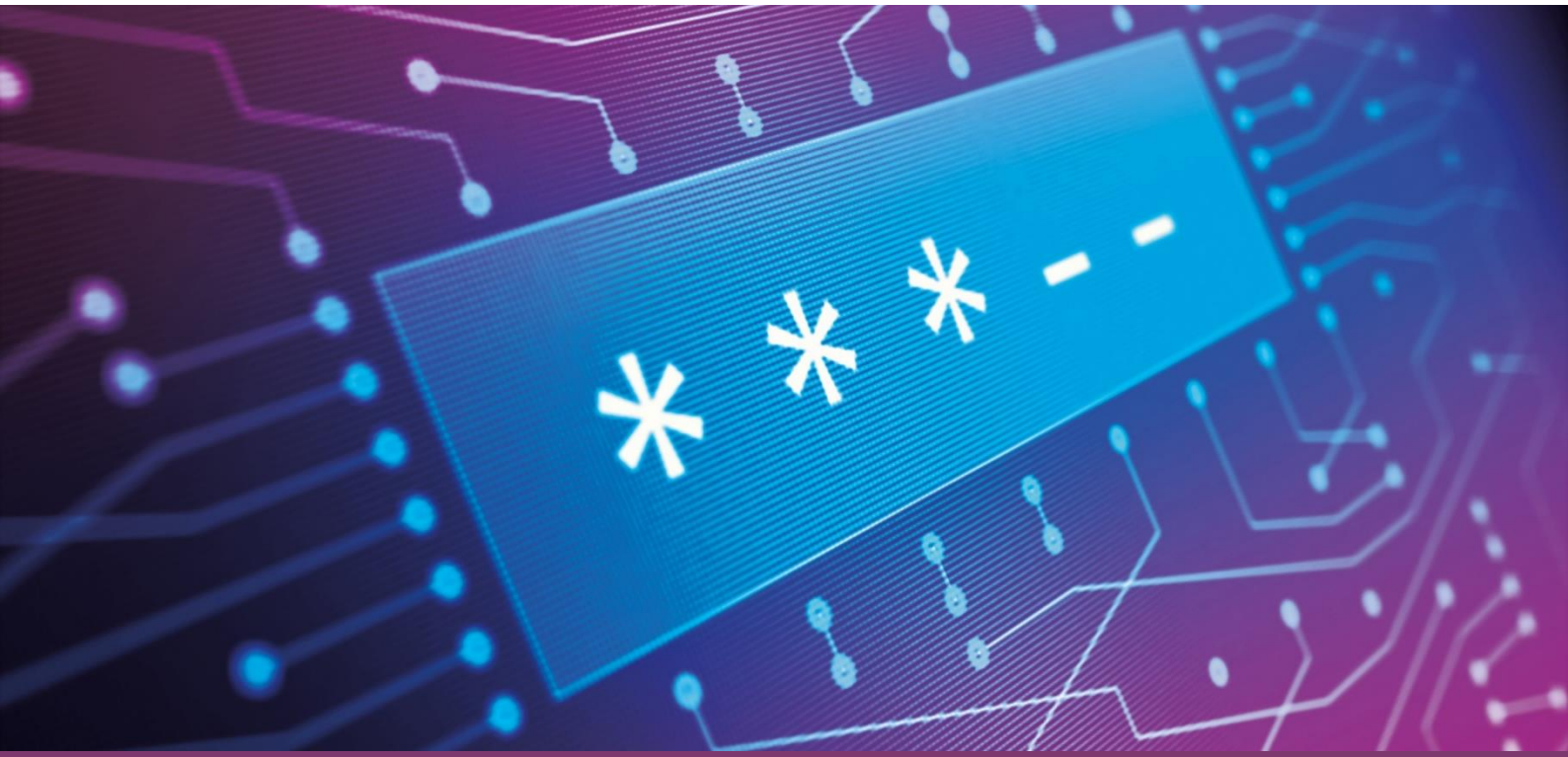
New obligations: The DMA imposes a number of positive obligations to gatekeepers. By way of example, they must (i) allow their business users to offer their products and services to customers outside the gatekeeper's platform, (ii) allow end users to un-install any pre-installed non-essential software applications on their core platform services, (iii) allow third parties to interoperate with the gatekeeper's own services in certain specific situations, or (iv) allow their business users to access and move the data that they generate in their use of the gatekeeper's platform.

As does the DSA, the DMA also contains a number of specific rules for online advertising which focus on price transparency.

Under the DMA, it will no longer be allowed for gatekeepers to combine personal data obtained via their core platform services with personal data from any other services the gatekeeper is offering, unless the end user has provided consent in accordance with the GDPR requirements. Gatekeepers should also refrain from requiring business users to use, offer or interoperate with the gatekeeper's identification service or from requiring business or end users to sign up to any other core platform services as a condition for accessing the platform.

Enforcement: In terms of enforcement, the EU Commission will have the power to investigate gatekeeper platforms and, in case of an infringement, to order interim measures and to impose both periodic penalty payments and/or fines up to 10% of total turnover in the preceding financial year.

Entry into force: Published in October 2022, the DMA will apply as of the 2 May 2023. Gatekeepers will then have six months following their designation by the EU Commission to comply with the obligations laid down in the Regulation.



3. Artificial intelligence

3.1 Artificial Intelligence Act

On April 24, 2021, the EU Commission unveiled a proposal for a regulation laying down harmonised rules on artificial intelligence – the artificial intelligence act ("AI Act"). The AI Act is part of a broader package of measures that address problems posed by the development and use of AI, such as the revision of sectoral product legislation (e.g. the Machinery Directive, the General Product Safety Directive) and the recent proposal for an Artificial Intelligence Liability Directive ("AILD" - see below). The overarching objective of the proposed AI Act is to create the conditions for an ecosystem of trust regarding the placing on the market, putting into service and use of AI in the EU.

Scope: The AI Act would apply to the development, placement on the market, and, in some circumstances the putting into service of "AI Systems". An AI system is defined very broadly. It as a system that is designed to operate with elements of autonomy and that, based on machine and/or human provided data and inputs, infers how to achieve its objectives using machine learning and/or logic- and knowledge-based approaches. It must also be able to produce system-generated outputs such as content (generative AI systems), predictions, recommendations or decisions, influencing the environments with which the AI system interacts.

Excluded from its material scope are (i) AI systems and their outputs developed and used exclusively for scientific research and development purposes; (ii) the use and placement on the market of AI systems for military, defence and national security purposes; and (iii) natural persons using AI systems in the course of a purely personal non-professional activity, it being understood that they would still have to comply with the transparency obligations under the AI Act.

Territorially, the AI Act would apply to (i) providers of AI systems (in and outside the EU) who place AI systems on the EU market, or put them into service in the EU, (ii) users of AI systems established within the EU and (iii) providers and users of AI systems that are established outside the EU, where the AI system's output is used in the EU. The proposal also entails obligations for product manufacturers, importers and distributors of AI systems.

Risk based approach: The AI Act adopts a risk-based approach whereby it differentiates between uses of AI that create (i) an unacceptable risk, (ii) a high risk, and (iii) a low or minimal risk.

3. Artificial intelligence

(i) Unacceptable risk

Harmful AI practices that contravene European Union values would be prohibited. This would apply to AI practices that are used to materially distort a person's behaviour in a manner that can cause physical or psychological harm beyond a person's consciousness. Similarly, it would apply when an AI system exploits the vulnerability of special groups of people based on their age, physical or mental disability, or enables social scoring by public authorities. The use of remote biometric identification systems in publicly accessible spaces for law enforcement purposes also appears on the blacklist, subject to some exceptions.

(ii) High-risk AI systems

For the so-called "high-risk AI systems" – being those that pose a significant risk to the health and safety or fundamental rights of persons, the proposal lays down a set of horizontal mandatory requirements for trustworthy AI, as well as some obligations for the relevant operators. The classification of an AI system as "high-risk" is based either on the intended purpose of the AI system or the fact that those AI systems are safety components of products or systems in line with existing product legislation. Most of the debate relates to the type of systems that should be regarded as high-risk AI systems.

High-risk AI systems would have to undergo a conformity self-assessment before they can be placed on the Union market and receive the 'CE' marking. In addition, high-risk AI systems would have to comply with legal requirements pertaining to the quality of data sets used, data governance, technical documentation, record-keeping, transparency, human oversight, robustness, accuracy and cybersecurity. These requirements would apply in light of the intended purpose of an AI system and the risks it poses to the rights of individuals.

Providers of high-risk AI systems would need to install a post-market monitoring system and to inform national supervisory authorities about serious incidents or breaches of national or European law protecting fundamental rights resulting from the use of their high-risk AI systems. They should do so immediately after establishing a (reasonably likely) causal link between an incident and the AI system, and at the latest within 15 days after becoming aware of the incident. They should also report any recalls or withdrawals of AI systems from the market.

(iii) Low/ minimal risk AI systems

Finally, for low or minimal risk AI systems, the proposal only lists a few transparency obligations. Notably, users should be informed that they are interacting with an AI system, and not a human being, unless this is "obvious from the circumstances and the context of use". Nonetheless, providers of AI systems are encouraged to subscribe to codes of conduct intended to foster the voluntary application of the mandatory requirements applicable to high-risk AI systems.

General purpose AI systems: For the so-called "general purpose AI systems", which are AI systems that are intended by the provider to perform generally applicable functions in a plurality of contexts, the application of the abovementioned rules was considered problematic. As such, at the time of publication, the Czech presidency proposed that these types of AI systems be regulated in a separate track. Under the currently proposed text, the EU Commission is prompted to evaluate how best to adapt the obligations under the AI Act to this type of AI system and to adopt implementing acts accordingly. Providers of general purpose AI systems would only have to comply with the provisions relating to the obligations for high-risk AI providers, the appointment of a legal representative in the Union, the declaration of conformity with EU law, and the post-market monitoring once such implementing acts enter into force.

Regulatory sandboxes: To foster innovation, the AI Act also envisages setting up 'regulatory sandboxes', allowing businesses to explore and experiment with innovative technologies in a controlled environment under the watchful eye of supervisory authorities.

Enforcement: In terms of enforcement, the AI Act would require Member States to appoint a national authority responsible for the supervision of AI based technologies. Unlike the GDPR, the AI Act would not introduce a one-stop shop mechanism. However, the proposal would create a "European Artificial Intelligence Board" ("EAIB") composed of EU Member State representatives that would ensure a consistent application of the AI Act across the EU.

Non-compliance with the AI Act could lead to administrative penalties ranging from the higher amount of 6% of global annual turnover or € 30 million, 4% of global annual turnover or € 20 million, or 2% of global annual turnover or € 10 million, depending on the type of infringement and whether or not the infringer is an SME.

3. Artificial intelligence

Entry into force: At the time of publication, the text of the AI Act is being discussed by the co-legislators, the European Parliament and the Council. Once the final text has been agreed and published, it will take another two years before the AI Act comes into force.

3.2 Artificial Intelligence Liability Directive (AILD)

Next to the horizontal framework that is the AI Act, the EU Commission has also taken steps in the field of civil liability for AI systems. More specifically, on 28 September 2022, the EU Commission issued a Proposal for an Artificial Intelligence Liability Directive ("**AILD**").

Scope: The AILD firstly aims to ensure that persons harmed by AI systems enjoy the same level of protection as persons harmed by other technologies. Indeed, it was observed that because of the complexity, autonomy and opacity (the so-called "black-box" effect) of AI systems, it is prohibitively difficult for a person suffering harm from AI systems to obtain compensation under a traditional fault-based liability system. The difficulties of proving the causal link between fault and damages in an AI system, as well as associated expensive procedural costs may be an obstacle for victims of damages caused by AI to claiming compensation altogether.

For businesses, the lack of clarity on how existing liability regimes apply to damages caused by AI creates legal uncertainty. Indeed, in the absence of an overarching legal framework, national judges will apply their respective tort liability rules. In doing so, it cannot be excluded that, to come to a just result for victims, judges may adapt the way they apply existing liability rules to accommodate for the specific characteristics of AI on an ad hoc basis.

Finally, the EU Commission observed that several Member States were in the process of drawing up bespoke national civil liability regimes for damages caused by AI enabled products or services. This would have eventually resulted in a patchwork of diverging national approaches to AI related civil liability, which, in turn, would have hampered the development and roll-out of AI systems throughout the European Union. With the AILD, the EU Commission seeks to improve the functioning of the internal market by laying down uniform rules for certain aspects of non-contractual civil liability for damage caused with the involvement of AI systems.

The AILD will apply to non-contractual civil-law claims for damages caused by an AI system, where such claims are brought under a fault-based liability regime.

New obligations: The AILD introduces measures to alleviate the burden of proof on the victim of AI related damages. It does so in two ways. Firstly, it imposes an information disclosure obligation on providers of AI systems, product manufacturers, distributors, users of AI systems etc. Secondly, the AILD introduces a rebuttable presumption of causal nexus between fault and the (lack of) output of an AI system.

(a) Information disclosure obligation

The AILD establishes the possibility for those seeking compensation for damages to obtain information on high-risk AI systems. This links with the obligation under the AI Act to keep records and technical documentation for high-risk AI systems. In practice, the AILD requires Member States to empower national courts to order the disclosure of relevant evidence about a specific high-risk AI system that is suspected of having caused damage. This will help those seeking compensation to identify potentially liable parties, and to collect potential evidence to support substantiated claims against such parties.

If the defendant fails to provide the requested documentation, the AILD installs a rebuttable presumption that the defendant has violated its duty of care in relation to the facts underpinning the claim for damages.

(b) Rebuttable presumption of causal nexus in case of fault

The AILD introduces a rebuttable presumption of causal nexus between the existence of a breach of the duty of care committed by the defendant and the output – or lack of output – of its AI system.

However, this presumption does not exempt the claimant from proving that the (lack of) output of the AI system gave rise to the damages it suffered.
In relation to high-risk systems, the AILD includes an exception to this of causal nexus if the defendant can demonstrate that sufficient evidence and expertise is reasonably accessible for the claimant to prove the causal nexus.

For AI systems that do not present a high-risk, the presumption only applies insofar as the court considers that it is excessively difficult for the claimant to prove the abovementioned causal link.

3. Artificial intelligence

The newly introduced liability regime – which departs from a minimum harmonisation approach – would not touch upon the definition of fundamental national law concepts such as "fault" or "damage". It will also not affect Union or national rules determining, for instance, which party has the burden of proof or what degree of certainty is required as regards the standard of proof.

Entry into force: The AILD is still in the early stages of the legislative process. The AILD proposal is currently being reviewed by the European Parliament Committee on Legal Affairs for a first reading. Once the European Parliament and the Council will have reached a common position on the final text, Member States will have 24 months to transpose the Directive into national law.

4. Cybersecurity

In 2016, the NIS Directive was the first EU-wide legislation on cybersecurity to enter into force. More recently, we have seen other pieces of legislation emerge to address cybersecurity risks in a targeted manner. The Cybersecurity Act establishes an EU framework for cybersecurity certification, enhancing the level of cybersecurity of products and services in Europe. The Cyber Resilience Act intends to cover cybersecurity risks presented by connectable products to strengthen the resilience of the whole chain or system. Finally, DORA will introduce specific operational resilience obligations for the financial sector.

4.1 Network & Information Security Directive II

On 10 November 2022, the European Parliament voted the Directive on measures for a high common level of cybersecurity across the Union ("**NIS 2**"), which will repeal and replace the current NIS Directive. NIS 2 came about in the face of growing threats posed by digitalisation, increased dependence on information technology – especially since the Covid-19 crisis – and cyber-attacks.

NIS 2 lays down obligations and requirements for both the public and private sector. It requires Member States to adopt national cybersecurity strategies, sets out rules and obligations on cybersecurity information sharing, and provides legal certainty and coherence by clarifying the relationship between NIS 2 and sector-specific cyber security legislation.

Scope: As a response to the generally increased exposure to cyber threats within Europe, NIS 2 has a broader scope than its predecessor. It covers medium and large entities from more sectors, based on their criticality for the economy and society. EU Member States will have to lay down cybersecurity risk management and reporting obligations for entities that are qualify as *'essential entities'* and '*important entities'.*

Whether an organization qualifies as an 'essential' or 'important' entity depends *inter alia* on the sector in which they are active and on their size. In that regard, 'essential sectors' notably cover the energy, transport, financial, health, drinking water, digital infrastructure sectors and public administrations. 'Important sectors' include the postal and courier services, waste management, manufacturing, chemicals and food sectors.

4. Cybersecurity

In some circumstances, Member States can identify entities as 'essential entities' regardless of the activity sector or size of the organization in question – e.g. when disruption of the service provided by the entity could have a significant impact on public safety, public security or public health.

Micro -and small enterprises are excluded from the scope of NIS 2, unless they fall under certain specific categories, such as providers of electronic communications networks or of publicly available electronic communications services, trust service providers, Top-level domain name (TLD), name registries and public administration. The EU Commission will provide further guidelines to help micro- and small enterprises assess whether or not they fall under the scope of NIS 2.

Lastly, it is important to highlight that NIS 2 no longer maintains the distinction between *'operators of essential services'* and *'digital service providers'* (e.g., online marketplaces, search engines and cloud service providers). This differentiation was proven to be obsolete in light of the importance of the sectors or services for societal and economic activities within the internal market.

Key obligations: NIS 2 aims to increase the level of security maintained by essential and important entities by imposing **additional cyber-security risk management measures** on organisations, including incident response and crisis management, cybersecurity testing, encryption, and vulnerability handling and disclosure.

The cybersecurity risk measures that are adopted should be proportionate to the risks posed to the relevant information system (based *inter alia* on the relevant entity's exposure to such risk and the potential detrimental effects of an incident), the state-of-the-art, the costs of implementation, and where relevant, the existence of European and international standards. The EU Commission will adopt implementing acts which further harmonize and specify technical and methodological requirements for various entities that often operate cross-border (e.g. DNS service providers, cloud computing service providers, data centre service providers, content delivery network providers, providers of online marketplaces, of online search engines and of social networking services platforms, and trust service providers).

Essential entities are subject to an elaborate *ex ante* and *ex post* supervisory regime, whereby they are required to document measures taken to comply with cyber-security risk management measures systematically. This *ex ante* supervision may consist of on-site inspections, targeted security audits or security scans. Important entities are only subject to an *ex post* supervisory regime: supervisory authorities will only supervise these entities if there are indications that they infringement NIS 2.

The **reporting obligations** under NIS 2 will be streamlined, with more precise provisions on the reporting process, the contents of reporting and the timeline. Affected companies have 24 hours after first becoming aware of an incident to submit an initial report – a so-called '*early warning*'. Still within 72 hours of becoming aware of the incident, they can update the submitted information through the early warning with an *incident notification*. A *final report* should be submitted no later than one month after the incident notification. Member states must see to it that these notification obligations do not impede the notifying entity from adequately handling the incident. They are also encouraged to set up a single point of notification of security incidents – which may come in handy for organizations that are subject to various notification obligations under different legal instruments. NIS 2 also promotes reporting of cyber threats that have not materialized and so-called 'near misses'.

Enforcement: NIS 2 establishes a minimum list of administrative sanctions that apply when an entity breaches its cybersecurity risk management or reporting obligations. These sanctions include imposing binding instructions, a temporary suspension of an authentication or certification to conduct certain activities, a temporary prohibition to exercise certain managerial functions at CEO or legal representative level, an order to implement the recommendations of a security audit, etc. In addition, essential entities can be imposed an administrative fine of up to the higher amount of € 10 million or 2 % of the total worldwide turnover of the undertaking (for important entities the maximums fine is the higher of € 7 million or 1,4 % the global annual turnover). Furthermore, the Directive introduces the possibility for company management to be held accountable for compliance with cybersecurity risk-management measures.

Entry into force: NIS 2 will enter into force 20 days after it has been published in the Official Journal. Member States will then have 21 months to transpose the Directive into national law.

4. Cybersecurity

4.2 Cyber Resilience Act

As cyber-attacks continue to rise, the EU is seeking to tackle vulnerabilities and become more resilient through a European Cyber Defence Policy.

On 15 September 2022, the EU Commission released a Proposal on a Regulation on horizontal cybersecurity requirements for products with digital elements (the **"Cyber Resilience Act**"). The Cyber Resilience Act will affect a whole range of economic actors who are developing, manufacturing, marketing, importing and distributing connectable products. All these actors will have to adjust their existing processes and extensively document their compliance.

Scope: The Cyber Resilience Act sets out comprehensive and mandatory requirements for the security of connected environments. More specifically, the proposal applies to 'products with digital elements', whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network (e.g. through an API or a software interface or through hardware interfaces). Such connectable products are broadly defined as "*software or hardware product and its remote data processing solutions, including software or hardware components (…)*" (the **"Products").**

According to the EU Commission, the security of connectable Products would ensure the security of the whole chain or system. The proposal does not apply to products that are already regulated, such as medical devices, nor does it apply to services, including SaaS. However, it overlaps with – and complements – other pieces of legislation such as the AI Act, the NIS 2 and the GDPR.

The territorial scope of the proposal is not explicitly mentioned and thus unclear at this stage.

New obligations: The proposal entails significant obligations for manufacturers, importers and distributors of Products. More specifically, Products may not be placed in the EU market, unless (i) they have been designed, developed and produced in compliance with the essential cybersecurity requirements identified in Annex I to the proposal, and (ii) the manufacturer puts in place the required processes to handle vulnerabilities effectively, as set out in said Annex.

To that end, manufacturers must perform a cybersecurity risk assessment. They must also complete their technical documentation with additional information and instructions addressed to users. After assessing the conformity with the essential requirements, manufacturers must draw up an EU declaration of conformity. The functioning of these obligations is therefore quite similar to those laid down in the AI Act.

However, the essential cybersecurity requirements are rather general and drafted in a technology-neutral way. For example, the Products must "ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems". They must also be free of known vulnerabilities and have secure settings by default.

It will also be possible to rely on cybersecurity certification schemes or standards.
Importantly, importers and distributors are also subject to some of the above extensive obligations when they market a Product under their own name or trademark, or carry out a substantial modification to the Product.

To ensure the cybersecurity of the Products throughout their lifecycle, manufacturers must notify the European Union Agency for Cybersecurity (ENISA) within 24 hours in case they detect an actively exploited vulnerability of the Product or any incident having impact on its security. Manufacturers must also inform users about the incident and if necessary of mitigating measures.

Critical or highly critical Products that present a high cybersecurity risk are subject to a stricter regime. The proposal categorises the "core functionalities" of Products that are to be considered as critical (e.g. remote access/sharing software, network traffic monitoring systems, industrial IoT devices) or highly critical (e.g. smartcards, smart meters, operating systems for servers, desktops and mobile devices). The EU Commission is competent to update this list and provide the definition of these categories.

Enforcement: National market surveillance authorities will be competent to enforce the Cyber Resilience Act, including through wide investigative powers and by imposing administrative fines which – depending on the infringement – may amount to € 15 million or 2,5% of the global yearly turnover of the preceding financial year, whichever is higher.

4. Cybersecurity

Entry into force: Once adopted, the Cyber Resilience Act would come into force after a two-year period of transition, except for the reporting obligation on manufacturers, which would be applicable after one year. Importantly, the Act will only apply to Products that have already been placed on the market before its date of application if, from that date, those Products are subject to substantial modifications in their design or intended purpose. Reporting obligations in case of incidents or vulnerabilities will apply to all Products.

The territorial scope of the proposal is not explicitly mentioned and thus unclear at this stage.

New obligations: The proposal entails significant obligations for manufacturers, importers and distributors of Products. More specifically, Products may not be placed in the EU market, unless (i) they have been designed, developed and produced in compliance with the essential cybersecurity requirements identified in Annex I to the proposal, and (ii) the manufacturer puts in place the required processes to handle vulnerabilities effectively, as set out in said Annex.
To that end, manufacturers must perform a cybersecurity risk assessment. They must also complete their technical documentation with additional information and instructions addressed to users. After assessing the conformity with the essential requirements, manufacturers must draw up an EU declaration of conformity. The functioning of these obligations is therefore quite similar to those laid down in the AI Act.

However, the essential cybersecurity requirements are rather general and drafted in a technology-neutral way. For example, the Products must "ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems". They must also be free of known vulnerabilities and have secure settings by default.

It will also be possible to rely on cybersecurity certification schemes or standards.
Importantly, importers and distributors are also subject to some of the above extensive obligations when they market a Product under their own name or trademark, or carry out a substantial modification to the Product.

To ensure the cybersecurity of the Products throughout their lifecycle, manufacturers must notify the European Union Agency for Cybersecurity (ENISA) within 24 hours in case they detect an actively exploited vulnerability of the Product or any incident having impact on its security. Manufacturers must also inform users about the incident and if necessary of mitigating measures.

Critical or highly critical Products that present a high cybersecurity risk are subject to a stricter regime. The proposal categorises the "core functionalities" of Products that are to be considered as critical (e.g. remote access/sharing software, network traffic monitoring systems, industrial IoT devices) or highly critical (e.g. smartcards, smart meters, operating systems for servers, desktops and mobile devices). The EU Commission is competent to update this list and provide the definition of these categories.

Enforcement: National market surveillance authorities will be competent to enforce the Cyber Resilience Act, including through wide investigative powers and by imposing administrative fines which – depending on the infringement – may amount to € 15 million or 2,5% of the global yearly turnover of the preceding financial year, whichever is higher.

Entry into force: Once adopted, the Cyber Resilience Act would come into force after a two-year period of transition, except for the reporting obligation on manufacturers, which would be applicable after one year. Importantly, the Act will only apply to Products that have already been placed on the market before its date of application if, from that date, those Products are subject to substantial modifications in their design or intended purpose. Reporting obligations in case of incidents or vulnerabilities will apply to all Products.

4.3 Digital Operational Resilience Act (DORA)

The financial sector has become heavily dependent on ICT systems and therefore it is inevitably exposed to cyber disruptions and threats. To address this issue, the EU Commission has decided to streamline and fill the gaps of the current fragmented framework by proposing a consolidated cross-sectoral approach: the Digital Operational Resilience Act ("**DORA**").

As DORA contains cybersecurity-related provisions, this raises questions on its interplay with NIS 2 which targets critical infrastructures to Member States. To address potential overlaps, DORA introduces a *lex specialis* exemption as a result of which it takes precedence over NIS 2.

4. Cybersecurity

DORA will apply to almost the entire financial sector, including banks, fintechs, stock exchanges, and insurance structures. However, entities operating pension schemes that do not have more than 15 members in total will be exempt from the new rules.

Scope: DORA introduces five core sets of obligations applicable to financial entities: (i) the implementation of a risk management framework and governance to detect, prevent and manage ICT risks, (ii) the classification of ICT incidents and the reporting of the major ones, (iii) the performance of resilience testing, (iv) the sharing of information and intelligence within the sector, and (v) the sound management of ICT third-party risk and the review of providers' contracts. Those obligations will apply proportionally to financial entities taking into account their size and overall risk profile.

More crucially, ICT third-party services providers, including cloud services providers, will also be subject to DORA. ICT providers which are deemed "critical" will be subject to oversight by one of the European Supervisory Authorities ("ESAs"). The latter will have far-reaching powers including the right to request information, conduct investigations, formulate recommendations and impose sanctions for non-compliance. Furthermore, critical ICT providers with no EU presence will be required to set up an EU subsidiary.

In addition to the above, the ESAs will also develop mandatory regulatory technical standards.

Entry into force: On 10 November 2022, the EU Parliament voted DORA. The new regulations will take effect 24 months after DORA's publication in the Official Journal of the EU.

5. Use and sharing of data

After enacting the Open Data Directive and the Free-Flow of Non-Personal Data Regulation, the EU Commission's Digital Single Market strategy will be complemented in a near future by three new acts: the Data Governance Act, the Data Act and the European Health Data Space Regulation.

With these three new data related acts in the pipeline, the EU is aiming to make itself a key player within the digital economy. The three acts have the ambition to facilitate the sharing of data between market actors and enhance the trust among them and the fairness within their practices. However, the scope of each of those soon-to-be regulations is different and will be developed hereunder.

5.1 Data Governance Act

The Data Governance Act ("**DGA**") intends to regulate the sharing of data, be it personal or non-personal, held by public sector bodies which are covered by rights preventing disclosure. These categories of data were not covered by the Open Data Directive and the Data Governance Act intends to foster growth in the data-driven economy notably by ensuring that no business suffers from any discrimination when accessing data they would like to re-use (i.e. condition, pricing, etc.).

Scope: The DGA applies to the re-use of certain categories of data held by public sector bodies, such as the data protected under commercial or statistical confidentiality rules or protected by intellectual property rights of a third party or personal data rights. The DGA is also providing a legal framework for data sharing services and the entities registered as collecting and processing data for altruistic purposes, i.e. processing which is based on the authorisation of data subjects or on permissions of data holders (in relation to non-personal data) without seeking a reward, for purposed of general interest.

5. Use and sharing of data

Key obligations: Regarding the re-use of data, the DGA prevents public sector bodies from entering into exclusive agreements, thus creating a level-playing field between all actors. Moreover, the conditions to re-use data, which must be made publicly available, shall be non-discriminatory, proportionate and objectively justified.

The DGA also creates the possibility for organisations to position themselves as 'safe data sharing service providers', i.e. intermediation services between either data holders or data subjects and potential data users. Similarly, not-for-profit organisations will be able to register as 'data altruistic organisations', when they aim to foster access to data in order to serve the general interest (e.g. to improve public services).

Finally, the DGA imposes strict conditions on the sharing of data outside the EU, adopting GDPR-like rules which will apply to international transfers of non-personal data.

Entry into force: The DGA entered into force on 23 June 2022. The new rules will start to apply on 24 September 2023.

5.2 Data Act

The Data Act intends to regulate the sharing of data holistically by creating a fair environment for the sharing of any kind of data between different types of actors (governmental bodies, public authorities, private companies, multinational companies, cloud service providers, etc.). The EU Commission published its proposal for a Data Act on 23 February 2022. This regulation aims at fostering data-driven innovation, the use of Big Data and Machine Learning. It also intends to ensure the competitiveness of cloud service providers and the creation of contractual standards. Moreover, it aims to ensure that maximum safeguards against misappropriation of data, including access to data by foreign governments that could jeopardise trade secrets and other valuable and protected data. Finally, the Data Act seeks to ensure that the existing Database Directive does not constitute an obstacle to data sharing in the context of IoT and other connected devices.

Scope: The Data Act proposes to impose obligations on certain companies such as cloud service providers and other companies that share data on a regular basis. These must ensure that the users of a product or service have access to the data generated through their use of the product or service.

The Data Act proposal applies to data holders making data available to data recipients in the Union and providers of data processing services offering such services to customers in the Union. The other actors subjects to the Data Act will be the following:

- manufacturers of products and suppliers of related services placed on the market in the Union and the users of such products or services;
- data recipients in the Union to whom data are made available;
- public sector bodies and Union institutions, agencies or bodies that request data holders to make data available where there is an exceptional need to that data for the performance of a task carried out in the public interest and the data holders that provide those data in response to such request.

Key provisions: The Data Act proposal has seven chapters that contain the key provisions applicable to the data economy and data sharing practices.

In relation to the sharing of data in a B2B and B2C context, the Data Act would require data generated by services or products are made data available to the user in an easy and safe manner. If that is not possible, the data holders shall provide information if the user issues an access request. The user has the right to request the sharing of data generated with a third party, except if the latter is considered a gatekeeper under the DMA.

To protection SMEs, the Data Act would contain a black list and grey list of abusive clauses in contracts, which would be considered void.
Public sector bodies would have a right to have access to data on demand, if an exceptional need exists, such as the necessity to respond to a public emergency or the lack of available data preventing the achievement of a task in the public interest.

Conscious of the international dimension of the industry, the Data Act proposal provides data transfer rules to ensure secure transfer of data outside of the EU and to prevent access by foreign governments.

Finally, the providers of data processing services shall ensure that their users can easily shift to another service provider and shall ensure interoperability as well. Operators of a data space would also be obliged to ensure interoperability with the services of other data space operators.

5. Use and sharing of data

Entry into force: The Data Act is still in the early stages of the legislative process. The proposal is currently being reviewed by the European Parliament and by the EU Council. Once the European Parliament and the EU Council will have reached a common position on the final text, the Data Act would apply from 12 months after its date of entry into force.

5.3 European Health Data Space

The European Health Data Space ("**EHDS**") is a proposal for a Regulation regarding the use of electronic health data. The EHDS is not limited to personal data but covers any information that is related to the health and treatment of patients. The objective of the proposal is to create a European Health Union and to favour the creation and exploitation of a safe and secure exchange, use (i.e. primary use) and reuse (i.e. secondary use) of health data.

Furthermore, the proposal aims at enhancing the rights of patients to increase their control over their medical data. Additionally, the EHDS proposes to adopt rules regarding the rollout of electronic health record (EHR) systems in the EU.

Finally, the EHDS proposes to create a mandatory cross border framework for primary and secondary uses of electronic health data in the whole EU, respectively MyHealth@EU and HealthData@EU.

Scope: The EHDS aims at protecting EU citizens and third-country nationals legally residing in an EU Member State.

The actors covered by the EHDS proposal are:

- Manufacturers and suppliers of EHR systems and wellness applications placed on the market and put into service in the EU and the users of such products;
- Controllers and processors established in the EU processing electronic health data of EU citizens and third-country nationals legally residing in the territories of Member States;
- Controllers and processors established in a third country that has been connected to or are interoperable with MyHealth@EU;
- Data users to whom electronic health data are made available by data holders in the EU.

Key provisions: A first set of obligations focuses on strengthening the access rights of data subjects to their electronic health data and to grant them to right to receive an electronic copy of their health data in a standardised electronic health data ("**EHR**") exchange format adopted by the EU Commission.

The EHDS also proposes requirements for holders of EHD to make available some categories of EHD for secondary use, such as relevant pathogen genomic data, health-related administrative data, human genetic, genomic and proteomic data, electronic health data from clinical trials or from medical devices etc.

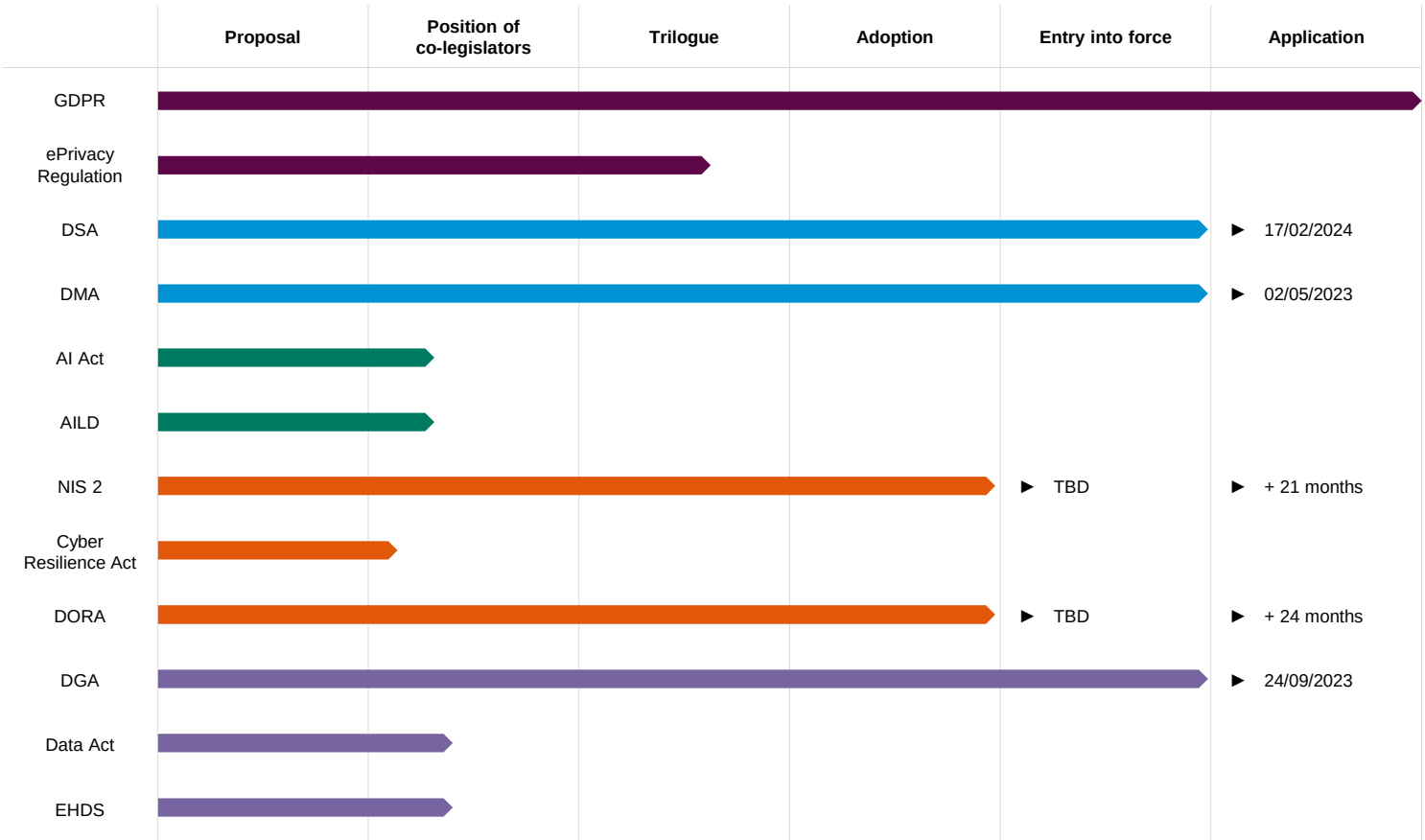
The EHDS proposal also contains a white list and a black list of processing activities relating to EHD. The white list would contains activities for reasons of public interest in the area of public and occupational health (such as protection against serious cross-border threats to health), education, R&D and for the provision of personalised healthcare. Among the prohibited uses are notably advertising activities towards health professionals, taking decisions detrimental to a natural person based on their EHD and developing products or services that may harm individuals and societies at large.

The Member States will have to designate the bodies in charge of granting access to electronic health data for secondary use. The designated bodies will also serve as a point of contact for natural persons.

Furthermore, the EHDS proposal contains obligations that would apply to manufacturers of EHR systems and wellness apps. Most of the obligations relate to conformity, transparency, registration and information of authorities when putting products on the market.

Entry into force: The proposal for the EHDS was published on 3 May 2022. Therefore, it is still in the early stages of the legislative process. The proposal is currently being reviewed by the European Parliament and by the EU Council. Once the European Parliament and the EU Council will have reached a common position on the final text, the EHDS would apply from 12 months after its date of entry into force.

6. Timeline



Status as of 23 November 2022

Key contacts

Fieldfisher's Technology and Data Group is one of the largest and most experienced in Europe. This breadth and depth of expertise means clients regularly instruct us on complex, international mandates with complete confidence.

Our team in Brussels is composed of French and Belgian qualified lawyers who advise multinational organisations and SMEs both in Belgium and abroad, and support them on multinational projects. Working from the heart of Europe, we provide clients with unique insights into the European Union's plan for a digital Europe and we provide full-scale services on all aspects of the digital economy.

Whether our clients need expertise on how to comply with the GDPR, the latest position of regulators on the use of cookies and other online tracking technology, or support to negotiate an IT deal, we have a proven track record in global, organisation-wide data governance strategies.

We also have market-leading expertise in privacy & data protection, technology & outsourcing and e-commerce projects, both from a compliance and contractual perspective.

Fieldfisher Belgium Tech & Data team

Tim Van Canneyt
Partner
+32 2 742 70 36
tim.vancanneyt@fieldfisher.com

Olivier Proust
Partner
+32 2 742 70 15
olivier.proust@fieldfisher.com

Sixtine Crouzet
Senior Associate
+32 2 742 70 55
sixtine.crouzet@fieldfisher.com

Louis Vanderdonckt
Associate
+32 2 742 70 86
louis.vanderdonckt@fieldfisher.com

Eliot Sanam-Ilung
Associate
+32 2 742 71 13
eliot.sanamIlung@fieldfisher.com

Naomi Capelle
Associate
+32 2 742 70 86
naomi.capelle@fieldfisher.com