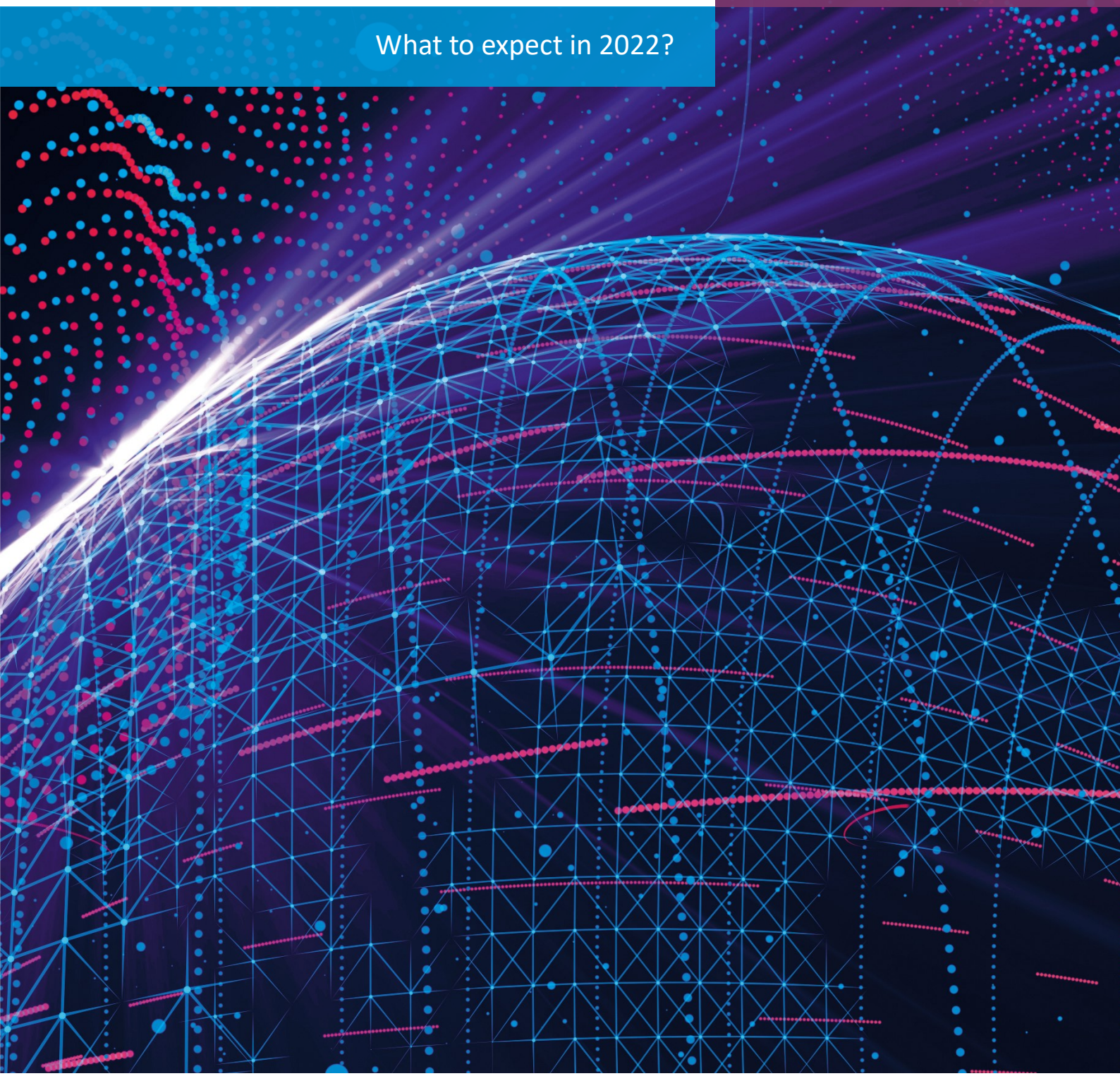
fieldfisher

State of play of the EU's digital legal landscape

28 January 2022

What to expect in 2022?



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 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 some of the EU's key legislative proposals in the field of data protection, artificial intelligence, digital services and cybersecurity. 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. General Data Protection Regulation

It's been nearly four years since the GDPR came into force (25 May 2018). Despite some criticisms, overall the GDPR is 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 Commission's agenda for the time being. For now, the 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.

2. Digital Services Act

The proposal for a 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, and enhance and harmonise 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 DSA intends to cover digital service providers that act as intermediaries offering one of the following types of service:

1. a mere conduit service;
2. a caching service; or
3. 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.

Territorial scope

In terms of territorial scope, the DSA would 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 would still 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.

Key points

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 European Commission proposes to move the well-known 'mere conduit', 'caching' and 'hosting' liability exemptions from the e-commerce Directive into the DSA to maximize harmonisation across the EU. The proposed DSA does not contain substantial changes to the 'mere conduit' and 'caching' exemption regimes.

However, the hosting exemption would no longer apply 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 would still not be subject to a general monitoring obligation but proactive investigations conducted by the provider of intermediary services would be encouraged.

Transparency obligations

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

All intermediary services would 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** would 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) would 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), would 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.

Despite the many calls for a ban on targeted advertising, the DSA will likely not go that far but it is expected to impose stricter rules, especially with regard to the targeting of minors.

In terms of enforcement, each Member State would 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 European Commission would maintain supervision, investigation and enforcement powers relating to VLOPs .

Sanctions

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

Timing

Following the recent vote in the European Parliament, the trilogue discussions between the Commission, the Council and Parliament will soon commence. The French presidency of the EU (running until end of June 2022) is determined to adopt a final text by end of June 2022. In terms of transition period after the adoption of the final text, the Commission is proposing a fairly short transition period of 3 months, whereas the Council wants to extend it to 18 months.

3. Digital Markets Act

The Digital Markets Act ("DMA") and the DSA can be viewed as siblings. Where the DSA, as explained earlier, 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. The Commission considers that the current competition rules alone do not address a number of issues identified around unfair business practices. The DMA therefore proposes to introduce a series of new obligations and tools that should help start-ups and smaller companies to compete with 'Big Tech'.

The DMA will apply to so-called "*gatekeepers*" that offer "*core platform services*", which includes:

1. online intermediation services,
2. online search engines,
3. online social networking services,
4. video-sharing platform services,
5. operating systems,
6. cloud computing services and
7. 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, or 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.

Territorial scope

In terms of territorial scope, the DMA would apply 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.

Key points

The proposed DMA contains a number of positive obligations that gatekeepers will have to comply with. 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 would no longer be allowed for gatekeepers to combine personal data obtained via its 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.

Sanctions

The Commission would 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.

Both the Council and the Parliament have adopted their position thus allowing the trilogue discussions to begin. As is the case with the DSA, the French presidency of the EU is determined to adopt a final text by end of June 2022. A six months transition period after the adoption of the final text is expected.

4. Artificial Intelligence Act

On April 24, 2021, the European Commission unveiled a proposal for a regulation laying down harmonised rules on artificial intelligence – the artificial intelligence act ("AI Act"). The AI Act is the result of elaborate collaboration and consultation with multiple stakeholders, and 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 initiatives that address liability issues related to new technologies. The overarching objective of this proposal 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.

The proposed AI Act would apply to the development, placement on the market, and putting into service of "*AI Systems*". AI systems are defined very broadly as software developed (i) in accordance with the first Annex to the proposal – this Annex covers notably AI based on machine-learning approaches, logic and knowledge-based approaches and statistical approaches – and (ii) that can, for a given set of human-defined objectives, generate outputs influencing the environments they interact with.

Territorial scope

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.

The AI Act is based on 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.

Unacceptable risk

Harmful AI practices that contravene European Union values would be prohibited. For example, 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, to exploit the vulnerability of special groups of people based on their age, physical or mental disability, or to enable social scoring by public authorities, are blacklisted. The use of remote biometric identification systems in publicly

accessible spaces for law enforcement purposes also appears on the blacklist, although there are exceptions where it can be permitted.

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.

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.

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, and not a human being, unless this is "obvious from the circumstances and the context of use". Nonetheless, they are encouraged to subscribe to codes of conduct intended to foster the voluntary application of the mandatory requirements applicable to high-risk AI systems.

In terms of enforcement, the AI Act would require Member States to appoint a national authority responsible for the supervision of AI based technologies. Contrary to 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.

Sanctions

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.

Timing

The text of the AI Act is still in the early stages of the legislative process. As a next step, the Rapporteur for the AI Act at the EU Parliament will issue a draft report containing proposed amendments to the text. Once the final text has been agreed and published, it will take another two years before the AI Act comes into force.

5. 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 European Commission has put forward a proposal to replace the existing ePrivacy Directive with a new regulation ("ePrivacy Regulation").

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.

Key points

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.

With respect to confidentiality of electronic communications, the ePrivacy Reguation 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.

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.

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.

Sanctions

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.

Timing

The ePrivacy Regulation was initially due to be enter into force at the same time as the GDPR. However, since the 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 last year. The ePrivacy Regulation will now undergo the trilogue process, as the Parliament and the Council have yet to find a mutual position. Once adopted, the ePrivacy Regulation would come into force after a period of transition (i.e. two years in the Council's version).

6. Network & Information Security Directive

On December 16th 2020, the European Commission submitted a proposal for a new directive on the security of network and information systems ("NIS 2 Directive"), which would repeal and replace the current NIS Directive. Growing threats posed by digitalisation, increased dependence on information technology – especially since the Covid-19 crisis – and cyber-attacks have prompted the EU Commission to update the existing NIS directive.

Scope

The NIS 2 Directive will have a broader scope than its predecessor. The current proposal covers medium and large entities from more sectors, based on their criticality for the economy and society. EU Member States would have to lay down cybersecurity risk management and reporting obligations for entities that are referred to as '*essential entities*' (energy; transport; banking; financial market infrastructures; health, drinking water; waste water; digital infrastructure; public administration and space) and '*important entities*' (postal and courier services; waste management; manufacture, production and distribution of chemicals; food production, processing and distribution; manufacturing and digital providers).

Micro -and small enterprises would be excluded from the scope of the directive, 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.

Lastly, it is important to highlight that the new proposal no longer maintains the distinction between '*operators of essential services*' and '*digital service providers*' (e.g., online marketplaces, search engines and cloud service providers), thus limiting a fragmented interpretation across the EU.

The proposal aims to increase the level of security by imposing additional security requirements on organisations, including incident response and crisis management, cybersecurity testing, encryption, and vulnerability handling and disclosure.

The reporting obligations under NIS 2 would become more streamlined, with more precise provisions on the reporting process, the contents of reporting and the timeline. Affected companies would have 24 hours after first becoming aware of an incident to submit an initial report, followed by a final report no later than one month later.

Sanctions

The proposal establishes a minimum list of administrative sanctions whenever entities breach the rules regarding cybersecurity risk management or their reporting obligations. These sanctions could include binding instructions, an order to implement the recommendations of a security audit, an order to bring security measures in line with the NIS 2 requirements, and administrative fines up to the higher amount of €10 million or 2% of the entities' total worldwide turnover. Furthermore, the proposal introduces the possibility for company management to be held accountable for compliance with cybersecurity risk-management measures.

Timing

Trilogue inter-institutional discussions are expected to start in the beginning of 2022. Under the current proposal, Member States would be required to implement the Directive under national law within 18 months once the Directive comes into force.

7. Data Governance Act/Data Act

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 two new acts: the Data Governance Act and the Data Act.

With these two new data related acts in the pipeline, the EU is aiming to make itself a key player within the digital economy. Both 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.

Data Governance Act

The Data Governance Act intends to regulate the sharing of data, be it personal or non-personal, held by public sector bodies which are covered by rights such as trade secret obligations, intellectual property or personal data protection. 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.). The proposal also prevents public sector bodies from entering into exclusive agreements with regard to the re-use of data, thus creating a level-playing field between all actors. The Data Governance Act would also open the door to creating new business models. First, it provides that intermediaries would be able to register to national authorities to ensure the provision of safe data sharing services. Second, organisations willing to foster access to data in order to serve the general interest (e.g. to improve public services) could register nationally as data altruistic organisations. Finally, the proposed regulation would impose strict conditions on the sharing of data outside the EU, in particular when data is being accessed by foreign governments. For now, both the European Parliament and the Council have endorsed the provisional agreement reached on 30 November 2021. The next step is for the European Parliament to review and adopt its amendments on the text.

Data Act

Separately, 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 has not yet officially made a proposal, but the Inception Impact Assessment and Public Consultation has shed some light on issues met by the stakeholders and the remedies that this regulation could potentially offer. This regulation would aim at fostering data-driven innovation, the use of Big Data and Machine Learning, competitiveness of cloud service providers, creating contractual standards to remedy the imbalance of power and ensuring maximum safeguards against misappropriation of data including access to data by foreign governments which can jeopardise trade secrets and other valuable and protected data. Additionally, the regulation would ensure that the existing Database Directive is not an obstacle to data sharing in the context of IoT and other connected devices.

Unlike the Data Governance Act which does not intend to impose any obligations on public sector organisations for the sharing of data – but rather intends to frame the sharing of data that is made available for re-use, the Data Act would impose a new set of rules on certain companies such as cloud service providers and other companies that share data regularly/frequently.

8. 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. In her speech on the State of the Union in 2021, Ursula von der Leyen announced that the Commission would come up with a Cyber Resilience Act in 2022.

Key points

This Act will set common cybersecurity standards and will complement the revision of the NIS directive as well as existing sectoral regulation. As a horizontal legislation, it will cover connected devices - machines, sensors, components – and so-called associated services, which are marketed in the EU. To that end, it will impose a set of obligations on developers and manufacturers of such devices, at a time when European homes are becoming increasingly connected. As a result, it is likely that the whole supply chain of the Internet of Things will be impacted. The Commission already mentioned the possibility of introducing a duty of care, which would address software vulnerabilities, including through software and security updates[1]. In addition, personal and sensitive data would need to be deleted at the end of the product lifecycle.

Timing

The European Commission is currently working on a proposal for Q3 2022. It is unclear at this stage whether the Commission plans to draft these new rules in the form of a directive or a regulation. In any case, there is unanimity with the other EU institutions that new rules are necessary. The Council initially invited the Commission to strengthen the Digital Single Market to enhance trust while boosting EU cyber competitiveness[2]. Last June, the EU Parliament also called for tighter rules on this matter[3].

1. Joint communication to the European Parliament and the Council, "The EU's Cybersecurity Strategy for the Digital Decade", 16 December 2021.
2. Council Conclusions call for horizontal measures on the cybersecurity of connected devices; 13629/20, 2 December 2020.
3. Press release "Parliament calls for beefed-up EU security against cyber threats", EU Parliament, 10 June 2021.

Contacts

fieldfisher

Oliver Proust
Partner, Technology , Outsourcing & Privacy
+32 2 742 70 15
olivier.proust@fieldfisher.com

Tim Van Canneyt
Partner, Technology , Outsourcing & Privacy
+32 2 742 70 36
tim.vancanneyt@fieldfisher.com

Sixtine Crouzet
Associate, Technology , Outsourcing & Privacy
+32 2 742 70 55
sixtine.crouzet@fieldfisher.com

Louis Vanderdonckt
Associate, Technology , Outsourcing & Privacy
+32 2 742 70 86
louis.vanderdonckt@fieldfisher.com

Eliot Sanam Ilung
Associate, Technology , Outsourcing & Privacy
+32 2 742 71 13
eliot.sanamilung@fieldfisher.com

Fieldfisher is proud to be home to one of the world's finest and largest privacy and technology law practices.

Our international team comprises over 60 multinational, and multilingual data protection experts throughout office in the EU, US and China who dedicate 100% of their practice to data protection meaning they have a level of legal, regulatory and commercial privacy expertise seldom found elsewhere. Through our experience of working with all types of organisations across all types of sectors and markets, we can advise not just on what the law requires, but what is common in the market and how similar organisations respond to the issues at hand.

Our team aligns itself across three broad privacy pillars:

1. Operational Compliance: We are experts in data governance, accountability and advisory work. We advise our clients on **policies, procedures and practices** to ensure their operational processes are compliant with data protection requirements - whether that be in connection with GDPR assessments, **international data export compliance** (including Binding Corporate Rules), data protection officer services or data record keeping requirements. We can also advise on the wide range of practical and **strategic implications** presented by operational compliance issues – for example: is it really necessary to undergo an expensive data center relocation project, or are there other, more cost-effective ways to address legal data export challenges? Where, within the organisation, should the privacy team sit and to whom should they report? How do you integrate privacy by design into development practices?

2. Commercial and Product: Working with some of the largest and most sophisticated technology companies in the world, our Privacy, Security and Information team handles an enormous volume of **commercial and product -related data protection work** - from commercial contracting with customers and vendors, through to new product reviews (including DPIAs and LIAs), sales and advertising advice across all marketing channels (e-mail, text, phone, post etc.), and **profiling and online advertising in the adtech world**. We have outstanding experience in helping businesses achieve their commercial- and product-oriented goals in a way that provides effective protection for individuals' data.

3. Cyber and crisis management: Recent legislation has introduced new requirements for reporting cybersecurity incidents to both regulators and to affected individuals. However, the decision to notify, or not to notify, is often finely balanced - how to determine if an incident is "risky enough" to merit notification? Moreover, what will the consequences be if you do? In addition, many organizations face increasing challenges through the so-called "weaponisation" of data subject rights, where individuals can submit enormously time-consuming and expensive requests easily, and without cost. Our team has significant experience in counselling organizations in both **preparing for these risks and also mitigating them** as and when they arise. Should you find yourself on the wrong end of a regulatory investigation, we have extensive experience in managing those too.