The Hague, 29 April 2022

Overview upcoming EU law on digital technology - April 2022

In 2022 to 2024 the EU will introduce multiple new laws to regulate (the market for) digital technology. This legislation is part of the EU's digital strategy 2019-2024 'A Europe fit for the digital age'. CIO Platform Nederland (CIOPN) voices the interest associations of business users of digital technologies on these dossiers. CIOPN collaborates with the CIO associations of France (Cigref), Belgium (Beltug)and Germany (Voice). This memo points out seven of the laws that are most relevant to business users of digital technology:

- Artificial Intelligence Act (AIA)
- Data Act
- Data Governance act (DGA)
- Digital Markets Act (DMA)
- Digital Service Act (DSA)
- Cyber resilience Act (CRA)
- NIS2 Directive

Artificial Intelligence Act (AIA)

The Artificial Intelligence Act (AIA) lays down harmonised rules for the development, placement on the market and use of AI systems. It establishes obligations for providers of AI-systems as well as for (business) users and other participants across the AI value chain.

The purpose of the AIA is to foster the development, use and uptake of AI while providing a high level of protection of public interests. The AIA should make the EU a global leader in the development of secure, trustworthy and ethical AI.

The AIA follows a risk-based approach based on the intended purpose of the AI system. It differentiates between uses of AI that create (i) an unacceptable risk, (ii) a high risk, and (iii) low or minimal risk. AI-systems posing an unacceptable risk are prohibited. High-risk AI systems are permitted on the EU market but have to comply with requirements related to data and data governance, documentation and recording keeping, transparency and provision of information to users, human oversight, robustness, accuracy and security. To low-risk AI systems, only minimum transparency obligations apply. If an AI system does not fall in one of the three categories, no obligations apply.

The AIA introduces most rules for high-risk AI systems. For high risk AI systems a conformity assessment is required. This can be part of the conformity assessment of the products of which the AI-system is a component (e.g. machinery and medical devices), or through internal control checks by the provider of the AI system.

The legislative process is progressing while the debate on issues like the definition of AI and responsibility for General Purpose AI continues. The Council of the EU is finalising its position and the European Parliament is drafting their opinion before negotiations may start by end the of 2022. Once positions are finalised, the Council and the Parliament will enter into negotiations. The AIA could enter into force by 2023 and apply as of 24 months thereafter.

Information about the AIA is available here and here. The legislative process is outlined here.

Data Act

On 23 February 2022, the European Commission published their proposal for the Data Act. The aim is to ensure fairness in the allocation of value derived from data among actors in the data economy and to

foster access to and use of data. The three main topics of the Data Act are: data sharing, switching between cloud services, and establishment of interoperability standards for data spaces.

In more detail, the data sharing relates to business to business and business to consumer data sharing. This concerns data generated by – in short – the use of Internet of Things (IoT) devices and related services; smart products such as medical devices, smart agricultural equipment or smart fridges. The Data Act establishes 1) an obligation to make data generated by the use of products and related services accessible, 2) a right of users to access and use data generated by products or related service, 3) a right to share data with third parties, and 4) obligations for third parties who receive data at the request of the user. Note that the Data Act limits data holders in their use of the data they obtain.

On the switching between cloud services, the Data Act stipulates that providers of such services must remove commercial, technical, contractual and organisational obstacles which inhibit costumers to switch to cloud services of another provider.

The legislative process is in the initial phase. The Council is expected to draft their opinion by mid-2022, while the European Parliament may start their process in 2022/2023. If so, the Data Act could apply by 2024.

Information about the Data Act is available here and here. The legislative process is outlined here.

Data Governance Act (DGA)

The Data Governance Act (DGA) aims to increase trust in data sharing. For that purpose, the DGA creates rules on three main topics.

Firstly, the DGA creates a mechanism for re-using categories of data by public sector bodies. The DGA provides a set of basic conditions under which the re-use of such data may be allowed (e.g. the requirement of non-exclusivity). The DGA does not create any obligation on public sector bodies to allow re-use of such data.

Secondly, the DGA establishes EU rules on the neutrality of data marketplaces for B2B and B2C sharing of personal and non-personal data. Providers of data sharing services are prohibited to use the data exchanged for any other purpose. This rule requires a structural separation between the data sharing service and other services they provide.

Thirdly, the DGA facilitates data altruism, which is data voluntarily made available by individuals or companies for purposes of general interest. Organisations that collect data for a general interest, e.g. in the field of medical research, may be listed in a register of recognised data altruism organisations. This should encourage individuals to donate their data to these organisations and will make it easier for organisations to use data for societal good.

On 30 November 2021, the European Parliament and Council reached a provisional agreement on the DGA. The DGA will apply as of mid-2023.

Information about the DGA is available here and here. The legislative process is outlined here.

Digital Markets Act (DMA)

The Digital Markets Act (DMA) establishes rules for large online platforms - so-called ‘gatekeepers’ - , such as search engines and e-commerce platforms. The gatekeeper-status is assigned if specific criteria are met regarding the magnitude or economic position of platforms.

The DMA defines and prohibits unfair practices by gatekeepers, like treating services and products offered by the gatekeeper itself more favourably in ranking than similar services or products offered by third parties on the gatekeeper's platform. The DMA also labels the practice of preventing users from

un-installing any pre-installed software as unfair. Furthermore, the new law will allow users to freely choose their browser, virtual assistants or search engines.

The European Parliament and the Council negotiators reached a compromise on 24 March 2022 which the Council and the European Parliament now need to formally approve. The DMA may apply by 2023.

Information about the DMA is available here. The legislative process is outlined here.

Digital Service Act (DSA)

The Digital Services Act (DSA) aims to create a safer and trusted online environment by defining rules for online intermediary services. The DSA applies to multiple types of online intermediary services (i.e intermediary services offering network infrastructure, hosting services, online platform services, and very large online platforms services). The act stipulates basic obligations applicable to all providers of intermediary services, for example regarding transparency. For hosting services, online platform services, and very large online platforms services the DSA establishes more specific and cumulative requirements.

The European Parliament, the Council and the European Commission have reached a political agreement on the final text of the DSA. The DSA may apply by 2024.

More information about the DSA is available here. The legislative process is outlined here.

Cyber Resilience Act (CRA)

The European Commission aims to publish a legislative proposal for the Cyber Resilience Act (CRA) later this year. It is expected to address market needs and protect consumers from insecure products by introducing common cybersecurity rules for manufacturers and vendors of tangible and intangible digital products and ancillary services. The CRA has to complement the Cybersecurity Act and the Network and Information Security (NIS) Directive of 2016 (and the future NIS2 Directive).

The CRA should address the problem that in a connected environment, a cybersecurity incident in one product can affect an entire organisation or even a whole supply chain with severe consequences. When placing digital products or services on the market, vendors often do not put in place adequate cybersecurity safeguards. Also, vendors' response to vulnerabilities throughout their products' lifecycle is too often inadequate. The current EU legislation only covers certain aspects linked to the cybersecurity of tangible digital products and, where applicable, embedded software concerning these products. It does not cover all types of digital products like a variety of widely used hardware and non-embedded software products.

The EC proposal for the CRA is expected to be published in Q3 of 2022. A consultation of the European commission for the CRA closes 25 May 2022.

Information about the CRA is available here. The legislative process is outlined here.

NIS2 Directive

A review of the current Network and Information Security (NIS) Directive of 2016 resulted in the proposal for the NIS2 Directive. NIS2 aims to address the deficiencies of the NIS Directive and to make it future-proof.

The scope of the current NIS Directive is extended by adding new sectors based on their criticality for the economy and society, and by introducing a clear size cap – meaning that all medium and large companies in selected sectors will be included in the scope. The proposal for NIS2 also eliminates the distinction between operators of essential services and digital service providers.

The proposal strengthens security requirements for the companies, by imposing a risk management approach providing a minimum list of basic security elements that have to be applied. NIS2 establishes basic security requirements for companies and introduces more precise obligations on incident reporting. In addition, the European Commission proposes to address the security of supply chains and supplier relationships by requiring individual companies to address cybersecurity risks in supply chains and supplier relationships. NIS2 also includes supervisory measures and accountability of company management for compliance with cybersecurity risk-management measures.

NIS2 is in the process of negotiations between the European Parliament, the Council and the European Commission.

Information about NIS2 is available here and here. The legislative process is outlined here.