Bird & Bird

One firm.
Your firm.

Digital Rights & Assets

European Digital Strategy Developments

December 2022

The number of digital rights & assets in existence across the world is *vast and growing*

Data, content, currencies and online reputations are some of the most valuable parts of the asset base of many businesses worldwide.

These digital assets are often essential to the effective understanding, management, operation and growth of organisations, and are at the forefront of organisations' thinking as they look ahead to a world of interconnected devices and ultrafast connectivity.

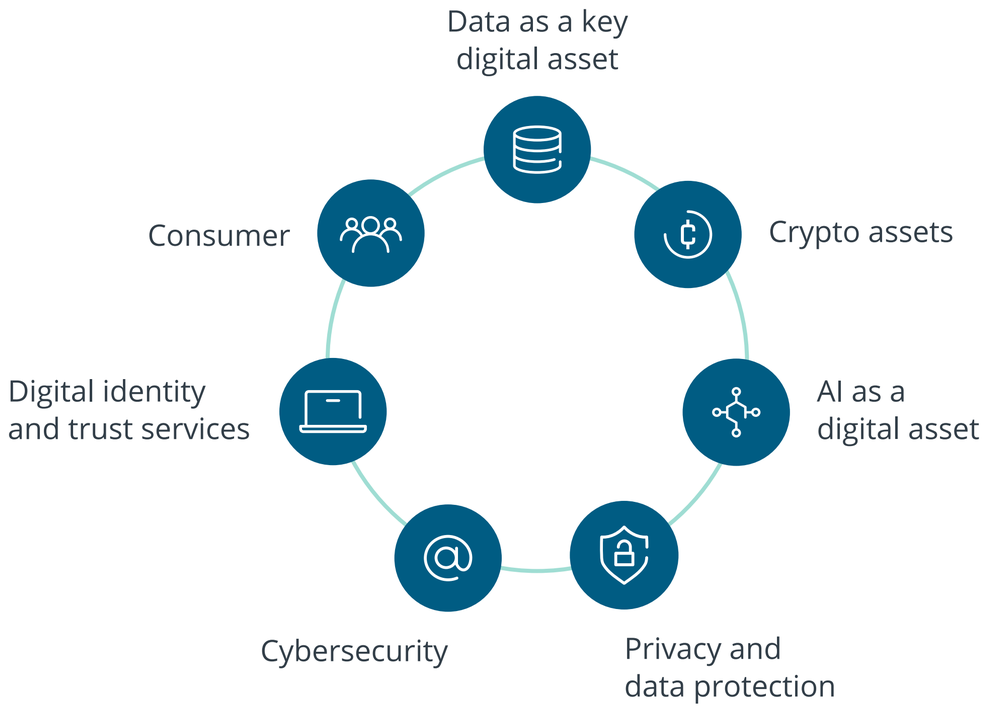
The European Commission has a range of initiatives in motion in the digital space, covering a broad range of topics including intellectual property (IP Action Plan), accessibility (European Accessibility Act) and consumer law (New Consumer Agenda). Of particular note, its *"European Digital Strategy"* for the period until 2025 sets out four overarching aims:

1. Technology that works for people
2. A fair and competitive digital economy
3. An open, democratic and sustainable digital society
4. Setting Europe as a global digital player

At a time of intensifying regulatory activity in digital asset governance, effective digital asset management is commonly a core component of compliance and positive reputation management. But with so many moving parts in this field, what do you need to be aware of?

In this document we'll take you through the latest developments in each of these areas, how they could be relevant to you and the next steps that are being taken.

Click on the icons below to navigate to the section you'd like to learn about.



Data as a key digital asset

Anthony Rosen
Legal Director
+44 (0)20 7415 6000
anthony.rosen@twobirds.com
Learn more →

Francine Cunningham
Regulatory & Public Affairs Director
+32 47 21 10 130
francine.cunningham@twobirds.com
Learn more →

Digital Services Act (DSA)

Digital Markets Act (DMA)

Data Governance Act (DGA)

Data Act

Digital Services Act (DSA)

1/2

Latest developments:

Fourth Quarter 2022 – The Digital Services Act entered into force in November 2022. The obligations on the largest platforms will apply from July 2023 and wider application from February 2024

Summary:

The DSA will introduce new rules for information society services, intermediaries, online platforms and search engines including the following measures:

Online platforms

- **Swift removal of illegal content online, including products, services:** a clearer "notice and action" procedure;
- **Greater responsibility for online marketplaces:** strengthened checks to prove that the information provided by traders is reliable ("Know Your Business Customer" principle); and
- **Victims of cyber violence will be better protected** especially against non-consensual sharing of illegal content (revenge porn) with immediate takedowns;
- **Algorithmic accountability:** the European Commission and Member States to have access to the algorithms of very large online platforms

Safer online space for users

- **New transparency obligations** for recommender systems and possibility for users to choose at least one option not based on profiling;
- **Online advertising:** targeted advertising banned when it comes to sensitive data (e.g. based on sexual orientation, religion, ethnicity);
- **Protection of minors:** platforms accessible to minors will have to take specific measures, including a full ban on targeted advertising; and
- **Manipulating users' choices through 'dark patterns'** will be prohibited

Harmful content and disinformation

- **Very large online platforms to assess and mitigate systemic risks** and will be subject to independent audits each year
- **Special measures in times of crisis:** the Commission may require very large platforms to limit any urgent threats on their platforms e.g. to public security of health, for up to three months

Digital Services Act (DSA)

2/2

How could it be relevant for you?

The proposal is relevant for providers of intermediary services in consumer and business markets, as well as digital advertising players and traders selling via online marketplaces

Next steps:

While the DSA is expected to be directly applicable across the EU from February 2024, some provisions concerning Very Large Online Platforms and Very Large Search Engines will apply from the date of entry into force of this Regulation

Digital Markets Act (DMA)

1/2

Latest developments:

Fourth Quarter 2022 – The Digital Markets Act has entered into force and will start to apply from May 2023

Summary:

The DMA will impose a range of obligations on providers of 'Core Platform Services' (CPS) which are designated as 'Gatekeepers'

The ex-ante obligations on 'Gatekeepers' are aimed at ensuring fair and open digital markets

The DMA will capture the following CPS:

- online intermediation services,
- online search engines,
- online social networking,
- video-sharing platform services,
- number-independent interpersonal communication services (e.g WhatsApp, IMessage),
- operating systems,
- web browsers,
- virtual assistants,
- cloud computing services,
- online advertising services

CPS provides that satisfy the relevant criteria will be designated as “Gatekeepers”:

A market capitalisation of at least **€75 billion** or an annual turnover of **€7.5 billion** and have at least **45 million** monthly end users in the EU and **10,000** annual business users

The DMA includes a list of do’s and don’ts including the following:

“Gatekeepers” should:

- for the most important software (e.g., web browsers), not require this software by default upon installation of the operating system;
- ensure the interoperability of their instant messaging services’ basic functionalities;
- allow app developers fair access to the supplementary functionalities of smartphones;

Digital Markets Act (DMA)

2/2

- give sellers access to their marketing or advertising performance data on the platform; and
- inform the European Commission of their acquisitions and mergers

“Gatekeepers” should not:

- rank their own products or services higher than those of others (self-preferencing)
- reuse private data obtained from one service for the purposes of another service;
- establish unfair conditions for business users;
- pre-install certain software applications; and
- require app developers to use certain services (e.g., payment systems or identity providers) in order to be listed in app stores

Companies that do not comply with the new rules can face fines of up to **10%** of their total worldwide turnover in the preceding financial year and **20%** in case of repeated infringements

How could it be relevant for you?

The initiative is relevant for providers of 'core platform services' and for businesses who interact with these services

Next steps:

The DMA will apply from May 2023

Data Governance Act (DGA)

Latest developments:

Second quarter 2022 – After final adoption by the European Parliament and Council, the Data Governance Act was published in the EU Official Journal on 3 June 2022 and enters into force 20 days thereafter

Summary:

The proposed Data Governance Act, which was the first legislation tabled as part of the EU's data strategy, aims to foster: the exchange of data in the European Union and with third countries through neutral data intermediaries; free up repositories of public data; and enable citizens to donate their data for the public good e.g., for medical research, through acts of "data altruism"

Main elements of the proposal include:

- A mechanism to facilitate the reuse of public sector data;
- Secure processing environments in which the shared data can be used;
- Introduction of a standard consent form for data altruism schemes; and
- Powers for competent authorities to monitor and supervise compliance of data service providers and data altruism organisations

How could it be relevant for you?

The DGA will be relevant to any entity that has large data sets (whether personal or non-personal), any entity that wants to reuse public sector data and sectors that could benefit from acts of "data altruism" e.g. medical research projects

Next steps:

The Regulation will apply 15 months after its 23 June publication in the EU Official Journal, which is expected to be 24 September 2023

Data Act

1/2

Latest developments:

Third quarter 2022 – the European Parliament and Council are in the process of assessing and amending the Proposal for an EU Data Act which was presented by the European Commission on 23 February 2022

First quarter 2022 – the European Commission presented its Proposal for a Data Act

Summary:

The Data Act aims to create a Single Market for industrial data by setting common basic rules on who can use and access data from connected (Internet of Things) devices across all economic sectors. It takes the form of a horizontal Regulation which will be directly applicable on the 27 EU Member States. By creating this new legal framework, the Commission aims to encourage fair business-to-consumer, business-to-business and business-to-government exchange of data

Main elements of the proposal include:

- **B2B and B2C data sharing:** designers and manufacturers shall provide products in which data is accessible by default;
- **Data availability and contractual terms:** data holders should make data available under fair, reasonable, non-discriminatory and transparent (FRAND) terms;
- **Public usage of data:** obligation to make data available for free in case of exceptional need, such as public emergencies;
- **Switching between data processing services:** service providers obliged to remove obstacles of any kind to enable switching between services (e.g. cloud services);
- **International access to data:** safeguards to avoid any unlawful third-party access to data located in the Union;
- **Interoperability:** the Commission is empowered to enable the interoperability through implementing acts;
- **Review of the Database Directive:** databases containing machine-generated data are excluded from the protection of *sui generis* right in the Directive 1996/9/EC; and
- **Enforcement and penalties** Member states shall lay down rules on effective, proportionate and dissuasive penalties

Data Act

2/2

How could it be relevant for you?

The Data Act proposal sets common rules on access and use of data from Internet of Things devices and access across all economic sectors. Several sector specific initiatives will be built on to it e.g., concerning the Data Health Space and connected mobility

Next steps:

Once both the European Parliament and the Council have reached their respective positions, three way "trilogue" negotiations will begin to reach consensus on final text. If discussions follow a typical timeline, the new legislation may come into force at the end of 2023 or in the course of 2024

Crypto assets

Digital finance package strategy

1/2

Gavin Punia
Partner
+44 (0)20 7982 6444
Gavin.punia@twobirds.com
Learn more →

Giuseppe D'Agostino
Of Counsel
+39 02 30 35 60 47
giuseppe.dagostino@twobirds.com
Learn more →

Latest developments:

September 2020 – proposed legislation published by the European Commission

Summary:

The Digital Finance Package Strategy aims to address the need to drive and harness digital transformation within the EU financial sector by promoting new opportunities and tackling the risks and benefits to consumers and businesses, while ensuring an integrated and level playing field for existing and new market players. As part of the Digital Finance package, the European Commission published a proposal for a Regulation on Markets in Crypto-assets (MiCA), aiming at creating an EU framework for crypto-assets falling outside the scope of existing EU financial regulation, as well as e-money tokens. This regulation considers within its scope:

a) **e-Money tokens** that are intended primarily as a means of payment aimed at stabilising their value by referring only to a single fiat currency

b) **Asset-Referenced tokens,** intended to maintain by referencing several currencies that are legal tender, one or several commodities, one or several crypto-assets, or a basket of such assets. They could also be used as a means of payment

c) **Utility tokens,** intended to provide digital access to a good or service available on distributed ledger technology (DLT), are included in the scope of MiCA only if fungible and transferable

Non-Fungible Tokens - whose value is attributable to each crypto-asset's unique characteristics – are excluded from the scope of MiCA

In any case, the European Commission is mandated to prepare a comprehensive assessment of the rules applicable to the NFT market and, if deemed necessary, will present a specific, proportionate and horizontal legislative proposal to create a new regime for NFTs and address emerging risks

Crypto assets

Digital finance package strategy

2/2

The proposal for Regulation on Markets in Crypto-assets sets out: (1) rules for issuers and offerors of crypto-assets; and (2) rules for entities that provide services related to crypto-assets (exchanges, trading platforms, custodial wallet providers etc.)

How could it be relevant for you?

The EC regulatory proposal has as its first objective the creation of legal certainty for crypto-asset markets within the EU. This regulatory framework will further push the tokenization of the digital economy, opening up a huge variety of ways to rewrite economic relationships. Tokenization makes it possible to carry out "peer-to-peer" (P2P) operations by creating, issuing and transferring "digital tokens" (crypto-assets) in a decentralised network (Distributed Ledger Technology systems), protected from the risk of theft, tampering or hacking

In any number of ways cryptocurrency and digital payments have fast become a popular space in modern society and a household digital asset. Behind the legislation, regulation and investment are the tangible topics of intangible assets that organisations and individuals deal with day-to-day

Next steps:

The Council Presidency and the European Parliament reached a preliminary agreement on the MICAR proposal on 30 June 2022

The Council’s Coreper endorsed on October 5, 2022, the final compromise text with a view to an agreement.

The adoption is now subject to the European Parliament's position in the first-reading.

According to the EU legislative procedure, should the European Parliament adopt its first-reading position in the form indicated in the compromise package, the Council would approve the position and adopt the Act.

AI as a digital asset

Feyo Sickinghe
Of Counsel
+31 (0)70 353 8800
feyo.sickinghe@twobirds.com
Learn more →

Katharine Stephens
Partner
+44 (0)207 415 6104
katharine.stephens@twobirds.com
Learn more →

Shima Abbady
Associate and PhD-Researcher
+31(0)70 353 8800
shima.abbady@twobirds.com
Learn more →

Ethics Guidelines for Trustworthy AI

Civil Liability Regime for AI

AI Regulatory Package

Ethics Guidelines for Trustworthy AI

Latest developments:

High-Level Expert Group on AI appointed by the European Commission: (1) issued Ethics Guidelines for Trustworthy AI and (2) established an Assessment List for Trustworthy AI for actors to self-assess whether they comply with the requirements identified in the Ethics Guidelines

Summary:

The Ethics Guidelines identify 7 key requirements that AI systems should satisfy in order to be trustworthy:

1. human agency and oversight
2. technical robustness and safety
3. privacy and data governance
4. transparency
5. diversity, non-discrimination and fairness
6. societal and environmental well-being
7. accountability

How could it be relevant for you?

Whilst there are currently no regulatory requirements specific to AI, there are major plans to develop such requirements which will ultimately affect all businesses utilising AI systems

Next steps:

The Guidelines provided input for the European Commission's White Paper on AI and will also inform discussions on the proposal for an AI Regulatory Package which was launched on 21 April 2021

Civil Liability Regime for AI

1/2

Latest developments:

28 September 2022 – The European Commission published a proposal for a revision of the Directive on liability for defective products (“Revised Product Liability Directive”) in order to accommodate for emerging digital technologies

28 September 2022 – The European Commission published a proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence (“AI Liability Directive”)

Summary:

The proposal for the Revised Product Liability Directive will apply to product liability claims for damages in the form of physical harm, property damage and loss/corruption of data (on the condition that this property/data is not used exclusively for professional purposes). The proposal specifically provides that AI-systems and AI-enabled goods are ‘products’ within the meaning of the Directive and provides a basis to claim not only from hardware manufacturers but also software providers and providers of digital services who affect the functioning of the product. This includes parties who integrate AI-systems into other products and parties who are responsible for changes to AI-systems which are already on the market (including those triggered by software updates and machine learning)

Compensation is available when defective AI-systems cause damage, without the injured party having to prove fault, just like for any other product. The Directive provides for a basis on which to claim disclosure of evidence from the defendant when the claimant has presented facts and evidence sufficient to support the plausibility of the claim. The Directive lightens the claimant’s burden of proof by introducing presumptions of defectiveness/causality e.g., in complex cases, when defendants fail to comply with an order to disclose evidence and when products fail to comply with safety requirements, such as those in the (Draft) Artificial Intelligence Act. The proposal also removes the current minimal claim value threshold of EUR 500

Civil Liability Regime for AI

2/2

The proposal for the AI Liability Directive will apply to all other forms of non-contractual (civil) liability, where the injured party does have to prove fault. Compensation is available in any form available pursuant to national laws (including non-material damages resulting from e.g., discrimination and privacy breaches). The proposal introduces a right to disclosure of evidence when the claimant has presented facts and evidence sufficient to support the plausibility of a claim for damages caused by a high-risk AI-system (within the meaning of the Artificial Intelligence Act). This proposal also introduces a presumption of causality (between the fault of the defendant and the output/failure to produce an output by the AI-system) in case of non-compliance with a legal duty of care intended to protect against the damage in question. However, this only applies if it can be considered reasonably likely that the fault has influenced the output of the AI-system/the failure of the AI-system to produce and output and the claimant has demonstrated that the output/failure to produce an output gave rise to the damage. In case of a high-risk AI-system, the presumption applies when the defendant has failed to comply with an order for disclosure of evidence or where the system is non-compliant with several requirements laid down in the Artificial Intelligence Act. In case of a non-high-risk AI-system, the presumption only applies where a national court considers it excessively difficult for the claimant to prove causality

How could it be relevant for you?

Both proposals create a stricter liability regime than currently exists in most Member States and would be relevant to all manufacturers, importers, distributors and operators of AI-systems in the EU

Next steps:

The European Council and the European Parliament will provide their input, after which voting will take place according to the ordinary legislative procedure

AI Regulatory Package

1/3

Latest developments:

First and Second Quarter 2022 – The Council and the European Parliament are currently discussing and amending the proposal for an AI Act which was published by the European Commission as part of the Artificial Intelligence Regulatory Package on 21 April 2021

The former Slovenian Presidency of the EU tabled a first Council compromise proposal on 29 November 2021 which has been followed by the French Presidency's second compromise proposal on 31 January 2022. After nine months of delay, caused by a competence battle between several committees, the European Parliament launched its work on the Proposal for an EU AI Act in January 2022

Summary

AI package comprises:

- A Proposal for a Regulation on a European approach for Artificial Intelligence;
- An updated Coordinated Plan with Member States; and
- A Proposal for a Regulation on machinery products

A risk-based approach was proposed by the Commission, built around the concept "the higher the risk, the stricter the rule". Therefore, the proposal differentiates AI uses into four categories:

- **Unacceptable risks:** AI systems falling within this category are prohibited, as they are deemed to be against EU fundamental rights and values. Banned AI systems include exploitative or manipulative practices, such as "practices that have a significant potential to manipulate persons through subliminal techniques", and AI-based social scoring carried out by public authorities;
- **High risks:** Such high-risk AI systems will be allowed only if they comply with certain mandatory requirements comprising: data governance, documentation and record-keeping, transparency and provision of information to users, human oversight, robustness, accuracy and security, as well as ex-ante conformity assessments. The identification of high-risk AI will be closely linked to their intended purpose and includes systems used in for critical infrastructure, educational training, hiring services,

AI Regulatory Package

2/3

migration and border control tools, justice administration and law enforcement. Real-time biometric systems (facial recognition) are included in this group and would be banned unless strictly necessary;

- **Low risks:** AI systems to which only specific transparent obligations will apply, as of making citizens aware that on the other side there is a machine (and not a human) interacting with them e.g., chatbots; and
- **Minimal risks:** this last group comprises AI systems that are considered not to constitute a risk or pose a threat to citizens' fundamental rights and to which no specific obligation will be applied

Emerging themes

The Internal Market Committee (IMCO) and the Civil Liberties Committee (LIBE) Committees leading on the file. MEPs Brando Benifei (S&D, Italy) and Ioan-Dragoş Tudorache (Renew, Romania) presented their joint **draft report** on 20 April which comprises 309 proposed amendments. In total, the Committees proposed more than 3,000 amendments. Co-rapporteurs have added "predictive policing" practices to the list of AI forbidden uses, as they believe that "liberal societies cannot use technology in breach of the key principle of presumption of innocence"

Other proposed additions to the list of high-risk AI uses include systems:

- Used by children in ways that have a significant impact on their personal development, including through personalised education;
- Making or assisting in decisions on the eligibility of persons for health and life insurance;
- Used by political parties, political candidates, public authorities, or on their behalf for influencing people's votes in local, national, or European Parliament elections; and
- Processing or counting voting ballots for such elections

Regarding the relationship between the AIA and the other data-related proposals, it is worth highlighting amendment 96 which clarifies that "error-free" datasets "should be an overall objective to reach to the best extent possible, rather than a precise requirement"

Other relevant amendments in the draft Report include an increase of tasks of the AI Board, better governance, legal remedies and a new enforcement mechanism by the Commission inspired in the model of the Digital Services Act

In parallel, the French Presidency of the EU is also making progress on the AI Act and has already presented compromise proposals on several articles

AI Regulatory Package

3/3

Interplay with EU framework

The European Data Protection Supervisor, the European Data Protection Board and the European Central Bank have published relevant opinions about this proposal in the fields of their competence. Questions have been raised regarding the interplay of the proposed AI Regulation and consistency with the EU legal framework including the EU Charter of Fundamental Rights, the General Data Protection Regulation (GDPR) and the Product Liability Directive, the General Product Safety Directive and among other instruments

How could it be relevant for you?

The AI Package represents the first ever set of rules on AI, which will be binding for AI systems, developers, users and importers of such technologies

The package is aimed at striking a balance between building citizens' trust in AI systems to mitigate associated risks and boosting investment and innovation in the further development of AI systems

Next steps:

The EU ministers have approved the compromise text of the Czech presidency on 6 December. The European Parliament is expected not to come to a final position until March 2023. The inter-institutional negotiations between the Parliament, the Council and the Commission are likely not to start before the end of the first quarter of 2023.

Privacy & Data Protection

ePrivacy Regulation

Berend van der Eijk
Partner
+31 (0)6 4406 4843
Berend.van.der.eijk@twobirds.com
Learn more →

James Mullock
Partner
+44 (0)20 3017 6901
james.mullock@twobirds.com
Learn more →

ePrivacy Regulation

1/2

Latest developments:

February 2021 – the EU Council of Ministers reached a General Approach on the proposal for the ePrivacy Regulations

Summary:

While the GDPR is the main legislative framework for data protection rules, some other EU laws contain rules on the use of personal data too. For example, the Second Payment Services Directive (PSD2) which contains rules around access and use of payment data, but the ePrivacy regulation is perhaps the most well-known – and long anticipated

The purpose of the ePrivacy regulation (historically), is to provide specific privacy and data protection rules in relation to electronic communications. Key points of the proposed ePrivacy regulation are:

Expanded scope: The scope of the ePrivacy rules will be extended to apply to so-called 'over the top' electronic communication service providers such as VoIP, various (B2B and B2C) messaging and communication services and videoconference providers. This is to ensure that these popular services provide the same level of protection of the confidentiality of communications as traditional telecoms services

Communications content and metadata: The rules around the use of communication metadata (i.e., time, location and addressees) and content data are updated to ensure strong privacy protection, but also enable companies to explore new business models under the right safeguards

Updated rules on cookies: The European Commission sought to streamline the cookie rules with new provisions and seeks to rely (again) on browser settings to accept cookies and other identifiers and allow more exemptions for non-privacy-intrusive cookies which have the potential to improve the internet experience (e.g., remembering users' shopping cart history) or analytical cookies. Given the amount of disagreement around the new rules and continuous opposition against the use of cookies for commercial purposes such as advertisements, it is not certain whether the new rules will be adopted

Protection against spam: The proposal upholds the general ban on unsolicited electronic communications by email, SMS, and automated calling machines and extends it to other means to send such messages, such as via over-the-top communication channels

More effective enforcement: The enforcement of the confidentiality rules in the regulation will be the responsibility of data protection authorities, already in charge of enforcement of the General Data Protection Regulation

ePrivacy Regulation

2/2

How could it be relevant for you?

Marketing via online advertisements and the sending of electronic messages is of vital importance for many companies, both those operating in a B2B environment as well as B2C environment, and companies should be aware of the reforms and there is still the opportunity to engage in the legislative process

In addition to the marketing rules, the proposals around confidentiality are relevant to parties offering communication services, both traditional players such as telecom operators as well as companies that provide 'over-the-top' communication services (including as part of a wider offering)

Next Steps

Tough negotiations are expected in the trilogue-phase of the proposal, where the Council and the European Parliament will need to reach consensus on the text, together with the European Commission. While it is not clear when the Regulation will be adopted there will be opportunities for industry to contribute to the decision-making process

Cyber-security

ENISA Threat Landscape Report

Revised NIS Directive

RCE Directive - Directive on the resilience of critical entities

The EU Cyber-security Act

DORA

CRA - European Cyber Resilience Act

Simon Shooter
Partner
+44 (0)20 7415 6000
simon.shooter@twobirds.com
Learn more →

Natallia Karniyevich
Senior Associate
+49 (0)211 2005 6192
natallia.karniyevich@twobirds.com
Learn more →

ENISA Threat Landscape Report

1/2

Latest developments:

November 2022 – the EU Agency for Cybersecurity (ENISA) published the 10th annual ENISA Threat Landscape Report 2022, providing an independent review on top cyber threats, major trends observed with respect to threats, threat actors and attack techniques as well as describing relevant mitigation measures

Summary:

For any organisation operating in the digital space, security against threats is a key focus, and cybersecurity has been confirmed as one of the European Commission's top priorities – described as a "cornerstone of the digital and connected Europe"

The ENISA Threat Landscape Report 2022, covering a period of reporting starting from July 2021 up to July 2022, identifies and focuses on eight prime threat groups. These threat groups are highlighted because of their prominence during the reporting period, their popularity and the impact that was due to the materialisation of these threats:

- Ransomware;
- Malware;
- Social Engineering threats;
- Threats against data;
- Threats against availability: Denial of Service;
- Threats against availability: Internet threats;
- Disinformation – misinformation; and
- Supply-chain attacks.

Ransomware has been, once more, one of the prime threats during the reporting period, with several high profile and highly publicised incidents. According to ENISA's Threat Landscape for Ransomware Attacks report, ransomware is defined as a type of attack where threat actors take control of a target's assets and demand a ransom in exchange for the return of the asset's availability. This action-agnostic definition is needed to cover the changing ransomware threat landscape, the prevalence of multiple extortion techniques and the various goals, other than solely financial gains, of the perpetrators

ENISA Threat Landscape Report

2/2

In the context of cyber threats, it is furthermore worth mentioning that ENISA worked with the European Commission in developing the new EU Cybersecurity Strategy which was published at the end of 2020 and aims to bolster Europe's collective resilience against cyber threats and help to ensure that all citizens and businesses can fully benefit from trustworthy and reliable services and digital tools

How could it be relevant for you?

ENISA's Threat Landscape for Ransomware Attacks report can be used by companies to help guide their preparations and responses to the major cyber threats facing their industries

NIS2 Directive

1/3

Latest developments:

Fourth Quarter 2022 – the NIS2 Directive was adopted in November 2022 and Member States now have 21 months to adopt implementing legislation. Companies will need to begin start to think about compliance now

Summary:

The new 'NIS2 Directive' will repeal the current Directive on security of network and information systems (NIS Directive), amending the rules on the security of network and information systems. The NIS2 Directive is part of a package of instruments and initiatives to further improve the resilience of public and private entities against cybersecurity threats. It sets rules to ensure protection and smooth uninterrupted functioning of services which are critical for the society. To this aim, it modernises the existing legal framework built on the NIS Directive, in particular expanding its scope as well as strengthening and streamlining security and reporting requirements. The act furthermore introduces more stringent supervisory measures for national authorities, stricter enforcement requirements and aims at harmonising sanctions regimes across Member States

How could it be relevant for you?

The NIS2 Directive expands the scope of the current NIS Directive in two manners by the following:

- **Adding new sectors**, including inter alia data centre service providers, providers of social networking services platforms and certain groups of manufacturers, selected based on how crucial they are for the economy and society, and
- **Introducing a clear company size threshold** which, if met or exceeded, assumes that companies of certain sectors are critical and thereby in scope, meaning that all medium and large companies in selected sectors (see Annex

I (Sectors of High Criticality) and Annex II (Other Critical Sectors)) will be included in the scope. At the same time, certain further entities with a high security risk profile and regardless of their size (e.g. trust service providers and top-level domain name registries as well as DNS service providers), including those designated by Member States, will be subject to the new regime

The Act furthermore eliminates the distinction between operators of essential services and digital service providers. Entities will be divided into essential and important entities reflecting the level of criticality of the sector or of the type of services they provide, as well as their size

Annex I – Sectors of High Criticality

- Energy
- Transport
- Banking
- Financial market infrastructures
- Health
- Drinking water
- Waste water
- Digital infrastructure
  - Internet Exchange Point providers
  - DNS service providers, excluding operators of root name servers
  - TLD name registries
  - Cloud computing service providers
  - Data centre service providers
  - Content delivery network providers
  - Trust service providers
  - Providers of public electronic communications networks or providers of publicly available electronic communications services
- ICT-service management (B2B)
  - Managed service providers (MSP)
  - Managed security service providers (MSSP)
- Public administration entities (excluding the judiciary, parliaments and central banks) and
- Space

Annex II – Other Critical Sectors

- Postal and courier services
- Waste management
- Manufacture, production and distribution of chemicals
- Food production, processing and distribution
- Manufacturing
  - Manufacture of medical devices and in vitro diagnostic medical devices
  - Manufacture of computer, electronic and optical products
  - Manufacture of electrical equipment
  - Manufacture of machinery and equipment n.e.c.
  - Manufacture of motor vehicles, trailers and semi-trailers
  - Manufacture of other transport equipment
- Digital providers
  - Providers of online marketplaces
  - Providers of online search engines
  - Providers of social networking services platform
- Research

Next steps:

Once published in the Official Journal, the NIS2 Directive will enter into force 20 days after publication. Member States will then have 21 months to transpose the Directive into national law. In Germany, for example, following the IT Security Act 2.0, the legislator will have to deal with an IT Security Act 3.0

RCE Directive - Directive on the resilience of critical entities

1/2

Latest developments:

16 September 2022 – the compromise text of RCE Directive was published

22 November 2022 – the European Parliament approved the Act

Summary:

While the NIS2 Directive aims to respond to the security concerns for the cyber dimension, the RCE Directive sets rules to reduce the vulnerabilities and strengthen the physical resilience of critical entities. These are entities active in such sectors as energy, transport, health, drinking water, waste water, and space and providing vital services on which the livelihoods of EU citizens and the proper functioning of the internal market depend

How could it be relevant for you?

The RCE Directive will replace the Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, which was limited to energy and transport sectors

The Act will finally cover eleven sectors: energy, transport, banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure (i.e., IXP providers; DNS service providers, excluding operators of root name servers; TLD name registries; providers of cloud computing service; providers of data centre service; providers of content delivery network; trust service providers; and providers of public electronic communications networks as well as providers of publicly available electronic communications services), public administration, space, and food

RCE Directive - Directive on the resilience of critical entities

2/2

Critical entities within the scope of the new rules will need to:

- Carry out risk assessments to identify all relevant risks that may disrupt the provision of essential services concerned;
- Take appropriate technical, security, and organisational measures to ensure their resilience; and
- Notify without undue delay the competent authority of incidents that significantly disrupt or have the potential to significantly disrupt the provision of essential services

Next steps:

Once published in the Official Journal, the Directive will enter into force 20 days after publication. Member States will then need to transpose the provisions of the Directive into national law within 21 months

The EU Cybersecurity Act

Latest developments:

The European Union's Cybersecurity Act became effective on 27 June 2019

It establishes an EU-wide cybersecurity certification framework for digital products, services and processes with uniform rules, technical requirements, standards and procedures to avoid fragmentation to cybersecurity certification processes across the EU. Some provisions of the EU Cybersecurity Act entered into force on 28 June 2021

Summary:

In June 2019, the EU adopted Regulation (EU) 2019/881 (“EU Cybersecurity Act”) which both strengthened the ENISA mandate and established a certification framework for information and communications technology

The framework provides a system to regulate the issue of European cybersecurity certificates and statements of conformity to security standards for information and communication technology products, services, and processes

How could it be relevant for you?

The Cybersecurity Act provides an opportunity for businesses supplying digital products to market them certified as meeting EU cybersecurity standards. While certification will be voluntary, at least initially, the European Commission will keep under consideration whether to make it mandatory

Next steps:

Businesses should evaluate the potential benefits from certification of their products

DORA - regulation of the financial services sector to secure operational resilience

Latest developments:

Fourth quarter: Digital Operational Resilience Act (DORA) was adopted by the Council on 28 November 2022

Summary:

The main goal of this initiative is to harmonise and strengthen the digital operational resilience requirements in the financial services sector against information and communication technology (ICT)-related incidents

The DORA is part of the Digital Finance Package that the Commission unveiled in September 2020 and which included two legislative initiatives within the cybersecurity domain: the DORA Regulation and a Directive with provisions amending eight other Directives

How could it be relevant for you?

The Act focuses on financial entities regulated at EU level, such as banks, payment providers, electronic money providers, investment firms, crypto-asset service providers (e.g., data center service providers) and to ICT third-party service providers. Co-legislators have agreed that the inclusion of statutory auditors and audit firms in the scope of the Regulation will be subject to a review within three years

Its central approach will be to require financial entites to maintain an ICT risk management framework, to report major ICT-related incidents to the competent authorities, to undertake resilience testing as well as sound monitoring of ICT third-party risk

Next steps:

Rules will apply 24 months after they enter into force

CRA - European Cyber Resilience Act

1/3

Latest developments:

15 September 2022 – the European Commission published a Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Cyber Resilience Act)

19 September – 30 January 2023 (midnight in Brussels time) the act is open for feedback

---

Summary:

With the aim of creating the first EU-wide legislation of its kind and to protect consumers and businesses from products with inadequate security features, the European Commission presented on 15 September 2022 a proposal for a new European Cyber Resilience Act. The Act introduces horizontal mandatory cybersecurity requirements for products with digital elements which are not specific to sectors, throughout their whole lifecycle. The proposal is complementary to the requirements under the proposal for a NIS2 Directive which aims at ensuring a high level of cybersecurity of services provided by essential and important entities

CRA - European Cyber Resilience Act

2/3

How could it be relevant for you?

The Cyber Resilience Act will apply to manufacturers, importers and distributors, so-called economic operators. Within the scope of this new draft regulation are all products that are connected either directly or indirectly to another device or network, like smart Internet of Things devices, computers, mobile devices, operating systems and apps, as well as safety-critical components that are installed in networks or industrial facilities. There are some exceptions for products, for which cybersecurity requirements are already set out in existing EU rules for medical devices, aviation or cars

The proposed measures lay down:

(a) Rules for the placing on the market of products with digital elements to ensure their cybersecurity;

(b) Essential requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to these products;

(c) Essential requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the whole life cycle as well as obligations for economic operators in relation to these processes. Manufacturers will also have to report actively exploited vulnerabilities and incidents; and

(d) Rules on market surveillance and enforcement

The core element of the Cyber Resilience Act are the essential requirements that all products with digital elements must fulfil. These include security-by-design features, such as ensuring protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems. Cybersecurity should be considered part of the design process and throughout the development and manufacturing process in the whole product life cycle. No product may be delivered with known vulnerabilities, according to the Commission's plans

In case of non-compliance with the essential cybersecurity requirements, the draft foresees administrative fines of up to EUR 15 million or, if the offender is an undertaking, up to 2.5 percent of its total worldwide annual turnover for the preceding financial year, whichever is higher

CRA - European Cyber Resilience Act

3/3

Next steps:

The Cyber Resilience Act is now open for feedback until 30 January 2023. Drafting feedback requires an impact assessment on your business. The feedback will be published here. All feedback received will be also summarised by the European Commission and presented to the European Parliament and Council, which are now examining the Act, with the aim of feeding into the legislative debate

Once adopted, economic operators and Member States will have two years to adapt to the new requirements. An exception to this rule is the reporting obligation on manufacturers for actively exploited vulnerabilities and incidents. This obligation will apply already one year from the date of entry into force considering the fewer organisational adjustments than the other new obligations

Digital Identity and Trust Services

European Digital Identity (EUid)

1/3

Piotr Dynowski
Partner
+48 22583 7914
piotr.dynowski@twobirds.com
Learn more →

Gian Marco Rinaldi
Counsel
+39 (0)23 035 6071
gianmarco.rinaldi@twobirds.com
Learn more →

Latest developments:

3 June 2021 – the European Commission published the Proposal for a Regulation amending the 2014 EU Regulation on electronic identification schemes and trust services for electronic transactions (known as the eIDAS Regulation)

17 June 2021 – the European Commission presented the legislative proposal to Parliament's lead Industry, Research and Energy Committee (ITRE) committee. MEPs welcomed the proposal while raising some concerns on the digital divide and inclusion for those citizens less digitally literate and the need to guarantee security and data protection in the solutions

30 November 2021 – the ITRE discussed the proposals and on 3 February 2022 there was a public hearing on “European Digital Identity Wallet and Trust Services” in the ITRE Committee

3 February 2022 - ITRE held a public hearing on the European Digital Identity Wallet and Trust Services where numerous concerns about the new framework were raised by various stakeholders

31 May 2022 – ITRE published its draft report in which it amended the definition of European Digital Identity Wallet and included an explicit requirement for the design of the wallet to ensure cybersecurity and privacy by design. The draft report also includes a new chapter on the European Digital Identity Board which will be tasked with helping the European Commission to prepare legislative proposals and policy initiatives and support the application of the regulation

3 June 2022 - Transport, Telecommunications and Energy Council approved the progress report of the working party on telecommunications and information society of 17 May 2022. Member States remain divided as regards the identification function of the digital identity wallet or level of security to be put in place as well as on the issue of the unique identifier. However, most Member States seem to agree to accepting the digital identity wallet as one of the electronic identification means. The Council has not yet reached a general approach on the file.

14 June 2022 – ITRE committee discussed the draft report in ITRE committee. The discussion focussed mainly on digital wallet. It was stressed that the digital identity wallet should be technologically neutral and that some aspects related to data protection need to be further developed. Also newly introduced

Digital Identity and Trust Services

European Digital Identity (EUid)

2/3

chapter on governance and entities that should be authorised to issue and recognise the digital identity wallet was discussed

July 2022 – ITRE committee introduced further amendments to its draft report, including that the digital identity wallet could be provided by qualified trust service providers established in the EU

Next step will include a vote in ITRE on its report

Summary:

The objective of this initiative is, amongst other things, to establish a more harmonised approach to digital identification and to:

(1) provide a future proof regulatory framework to support an EU-wide, simple, trusted and secure system to manage identities in the digital space, covering identification, authentication and the provision of attributes, credentials and attestations (European Digital Identity – EUid); and

(2) create a universal pan-European single digital ID; and (3) extend benefits of eIDAS to the private sector

In particular, the Proposal introduces the "European Digital Identity Wallet" which should be a product and service that, amongst other things, allows users to store identity data, credentials and attributes linked to their identity, to:

a) provide them to relevant parties on request and to use them for authentication, online and offline, for a service; and

b) create qualified electronic signatures

The Proposal aims to establish the inclusion of "electronic attributes", such as medical certificates or professional qualifications which should have the same legal effect as lawfully issued attestations in paper form. Under the Proposal it should be made easier to ensure pan-European legal recognition of such electronic attributes in electronic form, too

In addition, the Proposal addresses qualified electronic archiving services (whose technical standards shall be specified by means of implementing acts) as well as services, including remote qualified signature creation devices and electronic ledgers; all these services shall be provided only by qualified trust service providers

Digital Identity and Trust Services

European Digital Identity (EUid)

3/3

How could it be relevant for you?

The initiative is particularly relevant for trust service providers, but also to all European residents and businesses using electronic identification in connection with civil acts and commercial transactions or interacting with administrative bodies

Next steps:

The Proposal is currently under discussion in the European Parliament where the Industry, Research and Energy Committee is taking the lead and a range of other Committees are providing opinions. At the same time, Member States are discussing the proposal in the Council with a view to reaching partial agreement. Once the European Parliament and Council have both adopted their positions, there will be three-way negotiations along with the European Commission to achieve a final consensus

The Proposal is accompanied by a Recommendation. The European Commission has invited Member States to establish a common toolbox by September 2022 and to start the necessary preparatory work immediately. This toolbox should include the technical architecture, standards and guidelines for best practices and will allow a smooth entry into force of the amended eIDAS Regulation once it is approved by the European Parliament and Council

Next steps as described above are expected to take place in 2022 and 2023

Consumer

Roelien van Neck
Partner
+31703538828
roelien.van.neck@twobirds.com
Learn more →

Rob Turner
Partner
+44 (0)20 7415 6000
robert.turner@twobirds.com
Learn more →

Latest developments:

- Digital Content and Services Directive (EU 2019/770)
- Sale of Goods Directive (EU 2019/771)
- Omnibus Directive (EU 2019/2161)
- Representative Actions Directive (EU 2020/1828)

How could it be relevant for you?

If you sell or supply digital content or goods, including goods with a digital element to consumers you must ensure that your consumer facing channels and documentation (apps, websites, as well as the relevant standard terms, policies, etc) meet the requirements of the directives

Summary:

The Omnibus Directive and the Representative Actions Directive are part of the "New Deal for Consumers", an initiative from the European Commission. With the New Deal initiative, the European Commission aims to modernise the current EU consumer protection legislation in view of market developments, including the further digitalisation, and to strengthen the enforcement of EU consumer law, mainly regarding EU-wide infringements

The Digital Content and Services Directive and the Sale of Goods Directive regulate the supply of digital content and services and introduce new rules regarding the sale of non-digital goods and services that may have a digital element. Both directives are part of the Digital Single Market strategy from the European Commission

Next steps:

Where required, you need to take action as outlined above

The regulatory timelines are as follows:

- The Digital Content Directive and the Sale of Goods Directive have been transposed into national law by 1 January 2022
- The Omnibus Directive should be transposed into national law by May 28, 2022. Implementation legislation should be published by the Member States by 28 November 2021
- To be completed: the Representative Actions Directive should be transposed into national law by 25 June 2023. Implementation legislation should be published by the Member States by 25 December 2022

Country Contacts

European Union
Francine Cunningham
+32 47 21 10 130
francine.cunningham@twobirds.com

Jose Rivas
+32 (0) 2282 6093
jose.rivas@twobirds.com

Feyo Sickinghe
+31 (0)70 353 8800
feyo.sickinghe@twobirds.com

Australia
Sophie Dawson
+61 2 9226 9888
sophie.dawson@twobirds.com

Belgium
Benoit Van Asbroeck
+32 (0)2 282 6000
benoit.van.asbroeck@twobirds.com

China/Hong Kong
Hank Leung
+852 2248 6000
hank.leung@twobirds.com

Czech Republic
Vojtech Chloupek
+420 226 030 518
vojtech.chloupek@twobirds.com

Denmark
Morten Nissen
+45 27 59 32 04
morten.nissen@twobirds.com

Finland
Tobias Bräutigam
+358 (0)9 622 6670
tobias.brautigam@twobirds.com

France
Thomas Oster
+33 (0)142 68 67 41
thomas.oster@twobirds.com

Germany
Fabian Niemann
+33 (0)14 268 6741
fabian.niemann@twobirds.com

Hungary
Peter Rippel-Szabo
+36 1 301 8900
peter.rippel-szabo@twobirds.com

Ireland
Deirdre Kilroy
+353 1 (0)574 9850
deirdre.kilroy@twobirds.com

Anna Morgan
+353 1 (0)574 9850
anna.morgan@twobirds.com

Italy
Giuseppe D'Agostino
+39 (0)23 035 6047
giuseppe.dagostino@twobirds.com

Gian Marco Rinaldi
+39 (0)23 035 6071
gianmarco.rinaldi@twobirds.com

The Netherlands
Shima Abbady
+31 (0)70 353 880
shima.abbady@twobirds.com

Poland
Tomasz Zalewski
+48 22 583 79 00
tomasz.zalewski@twobirds.com

Singapore
Jeremy Tan
+65 64 28 94 87
jeremy.tan@twobirds.com

Slovakia
Ivan Kisely
+42 123 233 2825
ivan.kisely@twobirds.com

Spain
Jose Miguel Lissen
+34 917 906 009
jose.miguel.lissen@twobirds.com

Sweden
Mattias Lindberg
+46 (0)8 506 320 00
mattias.lindberg@twobirds.com

UAE
Yannick Hefti
+971 4 309 3222
yannick.hefti@twobirds.com

UK
Richard McMorris
Head of Digital
Rights & Assets
+44 (0)20 7415 6000
richard.mcmorris@twobirds.com

US
Nick Aries
+1 415 231 6568
nick.aries@twobirds.com