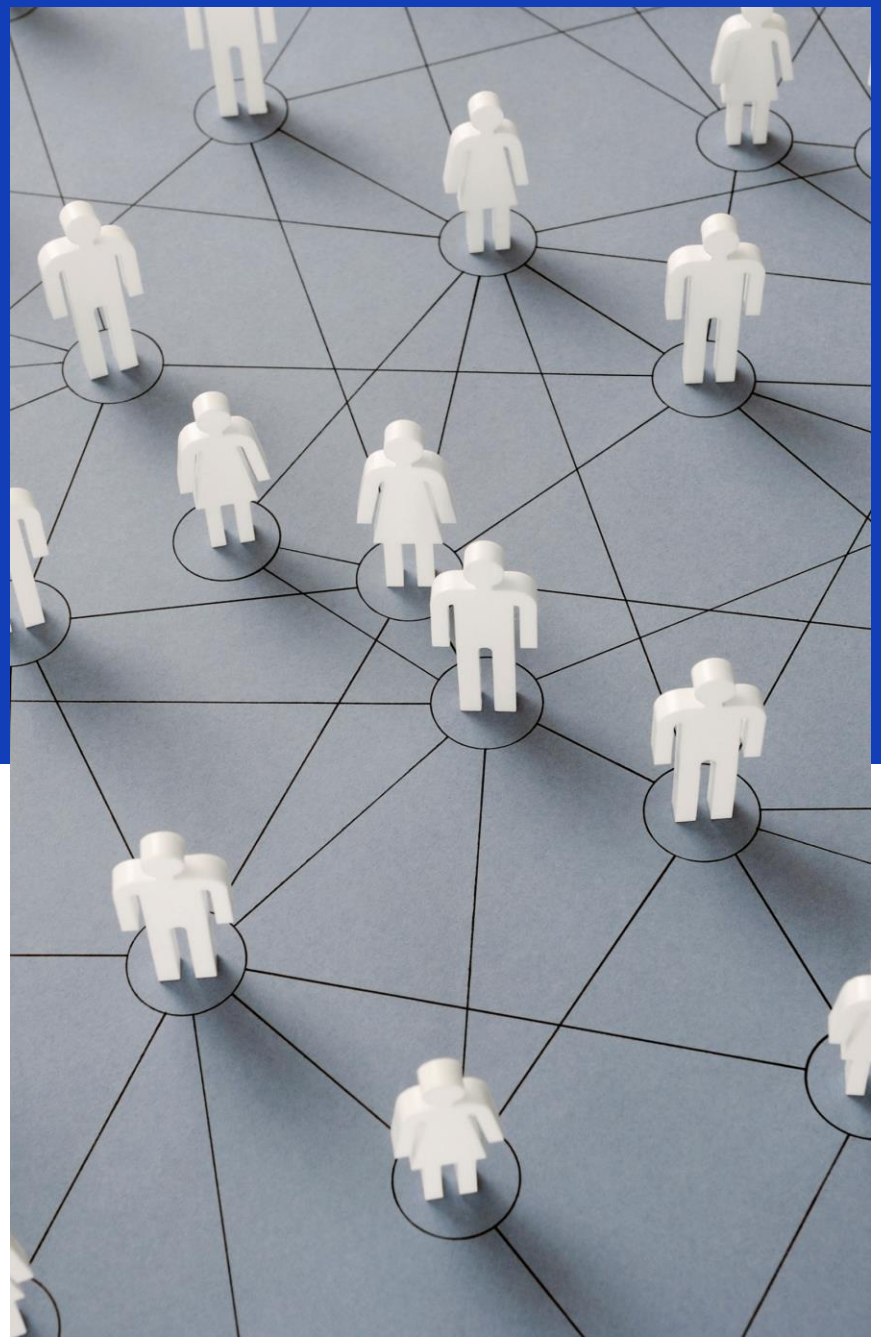
EU digital legislations

Implications for SMEs

Batura, O. (Olga) | VNO-NCW, Utrecht

TNO innovation for life



Agenda

1. EU digital strategy - overview
2. Digital Markets Act
3. Digital Services Act
4. Data Act
5. Open Data Directive
6. Digital Content and Digital Services Directive
7. Cyber Resilience Act
8. Other legislation and what to expect

EU Digital Strategy

- 2030 Digital Compass: the European way for the Digital Decade – the EU Digital Strategy
  - To foster digital transformation until 2030
  - To address challenges of digital technology, digital services and markets
  - To ensure Europe's digital autonomy
  - To make it work for businesses and people
- Areas covered by EU actions (policy and legislation):
  - Digital markets and services
  - Data
  - Cybersecurity
  - Artificial intelligence (AI)
  - E-Government, e-Identity
  - Digital infrastructure

Digital Markets Act

- **Main focus**: to ensure fair competition on digital markets & curb the power of gatekeepers
- Benefits/ rights for **SMEs that are business users of gatekeepers**:
  - Level playing field between offers on gatekeeper's platform and outside of it
  - Freedom from bundled offers of core and ancillary platform services
  - Detailed information about advertising, free of charge
  - Access to app stores, search engines and social networking services on Fair, Reasonable and Non-discriminatory (FRAND) terms
  - Access to search query data on FRAND terms
  - Interoperability with the core platform services
  - Free-of-charge and high-quality access to data on the core platform services

Digital Services Act

- **Main focus**: online content regulation and user protection
- Obligations of SMEs depend on the role:
  - If SMEs is **intermediary service providers** = providers of mere conduit (e.g. s internet exchange points, wireless access points, virtual private networks, DNS services), caching (e.g. content delivery networks, reverse proxies or content adaptation proxies) or hosting
  - If SMEs is **hosting service providers** = providers of storage of information provided by, and at the request of, a recipient of the service (e.g. cloud computing, web hosting, paid referencing services or services enabling sharing information and content online, including file storage and sharing)
  - If SMEs is **online platform** = hosting service that, at the request of a recipient of the service, stores and disseminates information to the public (e.g. social networks, online auctions)

Digital Services Act

- **Main focus**: online content regulation and user protection
- Obligations of SMEs:
  - If SMEs = **intermediary service providers**:
    - ✓ Single point of contact & legal representative in the EU
    - ✓ Changes to Terms & Conditions of use
  - If SMEs = **hosting service providers**:
    - ✓ Easy-to-access, user-friendly Notice-and-Action mechanisms
    - ✓ Notify relevant parties, including, if necessary, law enforcement authorities
  - If SMEs = **online platforms**:
    - ✓ Trusted flaggers for illegal content
    - ✓ Internal complaint handling
    - ✓ Out-of-court dispute resolution
    - ✓ Transparency & control for ads and recommendations
    - ✓ Traceability of traders

Data Act

- **Main focus**: access and use of non-personal data generated by IoT devices
- Relevance for **SMEs that are IoT device manufacturers and users**:
  - Data access by design applicable to IoT products placed on the EU market after 12 September 2026:
    - ✓ Users can share data with third parties
    - ✓ Detailed pre-contractual information
    - ✓ Readily available data and relevant meta-data by default, securely, easily, in a commonly used and machine-readable format, and free of charge. If the data cannot be accessed directly from the device or service, it must be made accessible through other (simple and electronic, where feasible) means without undue delay
    - ✓ Terms for data access must be FRAND
    - ✓ Appropriate technical and organisational protection (e.g. for trade secrets) can be used
    - ✓ Unfair contractual terms are not binding
  - Easy access to dispute settlement
  - Non-binding model contractual terms to be developed by the European Commission

Open Data Directive

- **<u>Main focus</u>**: access to and re-use of public sector data
  - Public sector data =
    - ✓ Documents held by public sector bodies (government of all levels),
    - ✓ Documents held by public undertaking (i.e. public service operators, transportation companies fulfilling public service obligations, companies in the areas of water, energy, and postal services supply)
    - ✓ Research data generated with public money

Open Data Directive

- **Main focus**: access to and re-use of public sector data
- Rights/ benefits for **SMEs that are data users**:
  - Quick and easy access to public sector data for anyone (this may include a licence if necessary)
  - Data formats are open, machine-readable, accessible, findable and re-usable, including their metadata
  - Data provided free of charge (with few exceptions)
  - Re-use conditions must be objective, proportionate, non-discriminatory and justified on grounds of public interest
  - Datasets that are considered high-value (geospatial, earth observation and environment, meteorological, statistics, companies and company ownership, mobility) must be:
    - ✓ available free of charge
    - ✓ machine readable
    - ✓ provided via APIs
    - ✓ provided as a bulk download, where relevant

Digital Content and Digital Services Directive

- **Main focus**: consumer protection in the context of contracts for the supply of digital content/ services
- Relevance for **SMEs that are suppliers of digital content or digital services**:
  - Digital content = data which are produced and supplied in digital form (examples: computer programmes, applications, video files, audio files, music files, digital games, e-books, other e-publications,)
  - Digital service =
    a) a service that allows the consumer to create, process, store or access data in digital form; or
    b) a service that allows the sharing of or any other interaction with data in digital form uploaded or created by the consumer or other users of that service

    (examples: software-as-a-service, such as video and audio sharing and other file hosting, word processing, games offered in the cloud computing environment and social media)

Digital Content and Digital Services Directive

- **Main focus**: consumer protection in the context of contracts for the supply of digital content/ services
- Relevance for **SMEs that are suppliers of digital content/ services**:
  - Rules on the conformity of the supplied content/ service with the description and purpose, accompanied with instructions and, possibly, updates
  - Rules related to the incorrect integration of digital content/ service into consumer's digital environment
  - Rules related to trader's liability for the failure to supply content/ service and for the lack of conformity of content/ service, including when it happens after updates
  - Burden of proof that the content/ service was supplied and was in conformity lies on the trader
  - Rules on remedies and reimbursement by trader for the failure to supply or lack of conformity

Cyber Resilience Act

- **Main focus**: ensuring cybersecurity of products with digital elements (software and hardware) placed in the EU market
- Obligations for **SMEs that are manufacturers of products with digital elements** placed on the EU market:
  - Products with digital elements = *software or hardware and their remote data processing solutions*, including software or hardware components being placed on the market separately

Cyber Resilience Act

- **Main focus**: ensuring cybersecurity of products with digital elements (software and hardware) placed in the EU market
- Obligations for **SMEs that are manufacturers of products with digital elements** placed on the EU market:
  - To ensure that products comply with essential requirements (free of known vulnerabilities, protect data confidentiality, integrity and availability, limit data processing and attack surfaces, provide security logs, have secure settings and access controls, etc.)
  - To conduct, document and update cybersecurity risk assessment and use the outcomes to reduce cybersecurity risks, prevent and mitigate security incidents, protect users
  - To exercise due diligence when integrating third-party software, including FSS and OSS
  - To provide clear technical documentation and user instructions
  - To ensure the support period for the product of at least 5 years
  - To conduct conformity assessment and attach CE marking (for high-risk products – third-party conformity assessment)
  - To report any vulnerability of products and severe security incidents to the Computer Security Incident Response Team (SCIRT) and ENISA

Other legislations

- In addition to the above, the General Product Safety Regulation is important (replacement of the General Product Safety Directive).

- Due to the recent European Parliament's elections, difficult to predict what parts of the digital strategy will remain high on the legislative agenda and what new topics might come up.
- Based on the previous legislative priorities, the following should be on the radar in the near future:
  - AI Liability Directive
  - Directive on liability for defective products (revision of the Product Liability Directive)
- Not clear whether the new European Commission and Parliament will be just as active in legislation or more focused on the implementation and application => compliance and enforcement might become priorities

Take-home messages

- Incredible legislative activity of the EU in the last few years
- “Know your rights and obligations” as important as ever:
  - SMEs need to look at their compliance where they have (new) obligations
  - SMEs need to benefit of rights provided by (new) legislation
- More support necessary for SMEs due to complexity and number of legislations. SMEs well advised to:
  - Pay attention to further implementing acts and guidance documents coming from the Commission and EU-level bodies (AI Office and similar)
  - Participate in regulatory sandboxes and pay attention to their outcomes (for the AI Act and Cyber Resilience Act)
  - Take advantage of the existing industry fora (such as AI Coalition, Centre of Excellence for Data Sharing & Cloud, Data Spaces Support Centre and others)

Yasmine Boudiaf & LOTI / Better Images of AI / Data Processing / CC-BY 4.0

Thank you for your attention!

olga.batura@tno.nl

TNO innovation for life