

DEEP DIVE

DIGITAL LEGAL >
ACADEMY 2022

by TaylorWessing

Is a digital regulatory tsunami on the way? The EU's digitization plans and their impact on companies

A Digital Legal Academy DEEP DIVE

31 August 2022

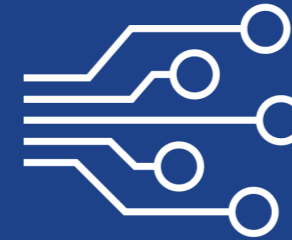
Private and Confidential

Content

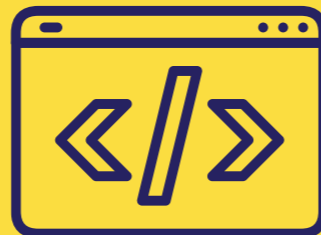
eCommerce



Data



Tech-Competition



IT-Security



eCommerce



Omnibus Directive

What plan?

- Directive (EU) 2019/2161 (so-called Omnibus Directive).
- Implementation through expansion of the BGB/EGBGB and the *Preisangabenverordnung* (PAngV)

What is it about?

- EU-wide strengthening of consumer rights, especially by modernizing existing regulations and introducing extended transparency and information obligations vis-à-vis customers in online commerce.

Who is affected?

- e-commerce providers and operators of online marketplaces.

When?

- From 28 May 2022

What actions must be taken?

- Suppliers should ensure that consumers are provided with all necessary pre-contractual information, e.g. by updating the applicable terms and conditions.
- Price marketing in accordance with the new PAngV.

Threat of fine/sanctions?

- Violations may result in warnings and cease-and-desist orders.
- In case of widespread infringements with Union-wide dimension, fines of at least 4% of the annual turnover or of at least 2 million euros if no information on the turnover is known (see Art. 246e EGBGB).



Digital Content Directive

What plan?

- Directive (EU) 2019/770 (so-called Digital Content Directive).
- Implementation through expansion of the BGB, in particular through the introduction of §§ 327 ff. BGB.

What is it about?

- Extended consumer rights when purchasing digital products, e.g., comprehensive warranty rights, information obligations, and an update obligation for providers.

Who is affected?

- Providers of digital products, such as software, e-books, apps, cloud computing, and streaming services.

When?

- Since January 1, 2022

What actions must be taken?

- Review of the existing terms and conditions and appropriate adjustment if necessary.

Threat of fine/sanctions?

- In the event of violations, consumers are threatened with warranty claims as well as warnings and cease-and-desist orders.



Fair Consumer Contracts

What plan?

- Fair Consumer Contracts Act
(*“Gesetz für faire Verbraucherverträge”*)
- Implementation through the expansion of the German Civil Law Code (*“BGB”*) and the Unfair Competition Law (*“UWG”*)

What is it about?

- Extension of consumer rights.

Who is affected?

- All companies whose business is focused on consumers.

When?

- 1 March, 2022 (provisions for fairer consumer contracts).
- 1 July, 2022 (cancellation-button obligation for websites).

What actions must be taken?

- Review of the existing terms and conditions with regard to the new regulations.
- Where relevant, introduction of the cancellation-button on the website.

Threat of fine/sanctions?

- Violations may result in cease-and-desist claims.
- Adjustment of the provisions on fines in the UWG with regard to the maximum fines - up to 100,000 euros.



Digital Services Act

What plan?

- Digital Services Act (DSA)

What is it about?

- Creation of a safe digital space which is free of illegal content.

Who is affected?

- All providers of intermediary services.
- In particular, the DSA includes tiered regulation with increasing obligations for intermediary services, host providers, online platforms, and very large online platforms.

When?

- Expected in January 2024.

What actions must be taken?

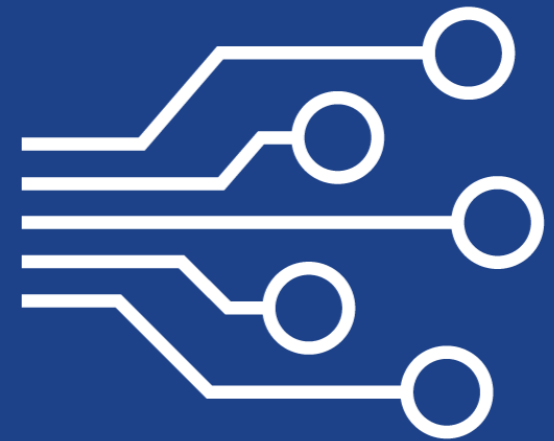
- Detailed tracking of the effective date of the DSA.
- Early planning to implement all DSA requirements, particularly in regards to content moderation.

Threat of fine/sanctions?

- The competent authorities have comprehensive rights of information, search, order and sanction.
- Fines for very large online platforms are of up to 6% of annual revenues or annual turnover are possible.



Data



Data Act & Data Governance Act

What plan?

Data Act & Data Governance Act

What is it about?

Promoting the availability and usability of data (personal and non-personal) in the EU through

- Rights of access to and use of data (Data Act)
- Data sharing infrastructures (Data Governance Act)

Who is affected?

- Manufacturers and owners of connected devices (IoT) and parties interested in the generated data (third-party recipients)
- SMEs
- Cloud services
- Public bodies
- Data intermediation services

When?

- Data Act: Expected 2024 (Commission draft from February 2022)
- Data Governance Act: September 24, 2023

What actions must be taken?

- Legal adjustments (contracts vis-à-vis users of IoT devices and third-party recipients, transparency obligations, "fair" SME contracts, cloud switching)
- Technical adaptations ("data accessibility by design and default", smart contracts, interoperability)
- Organizational adjustments (compliance management, data access requests, third-country access)

Threat of fine/sanctions?

- Data Act: reference to GDPR fines!
- Data Governance Act: „dissuasive financial penalties“



ePrivacy Regulation Draft

Which project?

- Adaptation of privacy protection to technological change in the telecommunications sector and convergence with GDPR (DSGVO)

What is it about?

- Confidentiality of communications (telecommunications secrecy)
- Processing of communications data (e.g. traffic data)
- Storing and reading information on terminal equipment (e.g. cookies)
- Protection against unsolicited communication requests

Who is affected?

- Providers of telecommunication and telemedia to
 - Protection of natural and legal persons
 - End users: all users who do not provide public electronic communications networks or publicly available electronic communications services

When?

- Currently in the trilogue procedure in the EU Parliament
- Entry into force approx. 2023 / applicability approx. 2025

What actions must be taken?

- Adaptation to existing regulations such as DSGVO, TTDSG
- Observation of further procedure

Threat of fine/sanctions?

- Monitoring by data protection supervisory authorities
- Fines up to max. 10.000.000 euros/ 2% of global annual turnover for unsolicited communications and up to max. 20.000.00 euros/ 4% of global annual turnover for a breach of telecommunications secrecy



What plan?

- Proposal for a regulation of the EU Commission laying down harmonised rules on Artificial Intelligence (AI Act)

What is it about?

- First dedicated AI regulation for placing on the market, putting into service and use of AI systems
- Prohibited AI practices (e.g. subliminal manipulation or exploitation of vulnerabilities of specific vulnerable persons)
- Requirements for high-risk AI systems (AI systems with a risk to health, safety or fundamental rights)
- “Product Compliance”, market surveillance and monitoring

Who is affected?

- Central addressee: providers of AI systems
- All persons and entities utilising AI for business purposes are concerned (importers, distributors and users)

When?

- Original plan of the EU Commission: adoption 18 months after publication of the draft (November 2022)
- Currently thousands of amendments in the EU Parliament (situation is comparable with GDPR) – trilogue said to start approx. end 2022
- Time until applicability probably about two to four years

What actions must be taken?

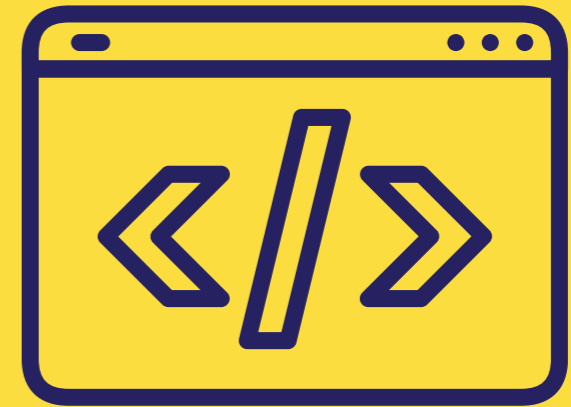
- Review of the distribution or use of AI systems
- Review of the potential relevance of the AI Act
- Develop preparatory measures and implementation plan
- Visit www.taylorwessing.com/ai-act-tracker

Threat of fine/sanctions?

- Fines of up to 30 million euros or up to 6% of the worldwide annual turnover
- Regulatory restriction or even prohibition of the provision of AI systems



Tech-Competition



Digital Markets Act (DMA)

Which legislative plan?

Digital Markets Act (DMA)

What is it about?

To create contestable and fair markets for the benefit of both end users and business users of core platform services. Imposes numerous obligations upon so-called gatekeepers – prohibits inter alia cross-platform combination of personal data, anti-steering, self-preferencing and most-favoured-nation clauses; creates obligations inter alia to guarantee interoperability of messaging services and allow easy un-installing of software applications and change of default settings.

Who will be affected?

Gatekeepers: Alphabet, Amazon, Apple, Meta and Microsoft; other large undertakings active in the digital sector will probably also qualify as gatekeepers.

When?

The DMA will likely enter into force in October 2022 and will be applicable six months later. The designation of gatekeepers will start in spring 2023 and the obligations will be binding six months after the designation.

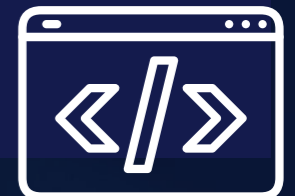
What actions must be taken?

Examine whether the DMA will be applicable on your undertaking and if so, which steps and measures must be taken to ensure compliance with the DMA.

Threat of fines/sanctions?

The EU Commission can impose fines of up to 20% of the total annual worldwide turnover and periodic penalty payments of up to 5% of the average daily worldwide turnover of the undertaking.

In addition, the EU Commission can impose behavioural and structural remedies.



What plan?

Vertical Block Exemption Regulation (Regulation (EU) 2022/720) and Vertical Guidelines

What is it about?

Distribution competition law, inter alia competition law in e-commerce. Topics include: Competition law requirements for online intermediation platforms; online distribution (e.g. marketplace bans, requirements for online advertising channels, dual pricing systems online / offline); dual (online) distribution; best-price clauses (booking.com); customer and territorial restrictions; price fixing in distribution; exclusive distribution; selective distribution; non-competition clauses; commercial agents, etc.

Who is affected?

All companies, no matter what size; concerns any contract for the purchase and sale of goods and services, online and offline.

When?

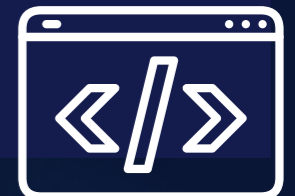
1 June 2022

What actions must be taken?

Check all distribution and purchasing contracts for compliance with competition law, transition period until 31 May 2023;
Use new room for manoeuvre

Threat of fines/sanctions?

- For companies: Fines of up to 10% of total worldwide group turnover; invalidity of clauses and contracts; claims for damages by customers, suppliers and competitors; entry in the competition register; exclusion from public tenders; disgorgement of benefits.
- For natural persons: Fines of up to 1 million euros (in Germany); claims for damages by customers, suppliers and competitors; recourse and claims for damages by the employer; extraordinary termination without notice



IT-Security



Which project?

- NIS Directive-2.0: Reform of the Network and Information Security Directive (2016)

What is it about?

- More comprehensive measures, requirements for reporting content
- Expansion of the target group
- Extension of the cooperation of the Member States
- Establishment of a European Massive Cybersecurity Incident Network consisting of national competent authorities (EU-CyCLONe)

Who is affected?

- Operators of essential or important services (depending on the degree of criticality of the sector)
- Critical sectors: Wastewater, public administration, space + well-known sectors (e.g., energy, transport, health care)
- Generally all included, exceptions for micro/small enterprises

When?

- 13 May 2022: Political agreement between Council and Parliament
- After entry into force: Implementation period of 21 months

What actions must be taken?

- Checking whether companies are covered by the extended scope of application and whether the (extended) specified protective measures are (already) implemented (incl. compliance with reporting obligation))

Threat of fines/sanctions?

- Maximum limit of fines increased
 - Up to 10 million euros or 2% of the companies' total annual worldwide sales, whichever is higher



Which project?

- Digital Operational Resilience Act, short DORA
- Draft regulation on the operational stability of digital systems in the financial sector → uniform set of rules

What is it about?

- Governance and risk management requirements for information/communication technology (ICT)
- Reporting ICT-related incidents
- Checking the digital operational stability
- Managing the risk from third-party ICT providers
- Information exchange agreements

Who is affected?

- Banks, insurance companies, payment service providers, other stakeholders in the financial sector (various requirements, depending on size and company profiles)
- (critical) third-party ICT providers

When?

- Political agreement on 11 May 2022, end of the trialogue
- Effective date: 24 months after entry into force

What actions must be taken?

- Inventory of own DORA compliance
- Use of "critical" third-party ICT providers as intended by DORA?
- Review of the ICT service providers used (1 x per year)

Threat of fines/sanctions?

- Yes, DORA provides for various administrative sanctions and remedies (e.g., requirement to terminate contract)
- No separate catalog of fines, but mandatory fines against critical ICT third-party providers amounting to 1% of global daily turnover



The Speaker



Mareike Gehrmann



Mona Wrobel



DEEP DIVE
DIGITALLEGAL
ACADEMY 2022
by TaylorWessing



Nathalie Koch



Elisa Eschborn



Fritz Pieper



Manuel Nagel



Daniel Tolks



Paul Voigt



Thomas Kahl



Stefan Horn



DEEP DIVE

DIGITAL
LEGAL
ACADEMY
2022

by TaylorWessing

taylorwessing.com

© Taylor Wessing 2022

This publication is not intended to constitute legal advice. Taylor Wessing entities operate under one brand but are legally distinct, either being or affiliated to a member of Taylor Wessing Verein. Taylor Wessing Verein does not itself provide services. Further information can be found on our regulatory page at taylorwessing.com/en/legal/regulatory-information.