



Background Information

This document offers a brief overview of each of the seven pieces of digital legislation analysed in the framework of the DLIFE project.

1. THE DIGITAL SERVICES ACT (DSA)

It aims to improve the safety and accountability of digital services across the European Union, whether these are EU-based or not, with a specific focus on content moderation and transparency. It applies to a broad range of online intermediaries, including internet access providers, cloud hosting services, social networks, online marketplaces, and app stores. It imposes regulations on very large online platforms and very large online search engines (very large meaning more than 45 million active users). *Digital Services Act*.

2. THE DIGITAL MARKETS ACT (DMA)

It applies to very large tech companies or 'gatekeepers' that provide services to both businesses and end users in the European Union. To date, seven of these have been identified: Alphabet, Amazon, Apple, Booking, ByteDance, Meta, Microsoft (see image below). It aims to ensure fair competition and foster transparency and innovation within the digital economy by regulating the gatekeepers with respect to their impacts in the EU. The DMA also emphasises data portability and interoperability. *Digital Market Act*.

3. THE DATA GOVERNANCE ACT (DGA)

It encourages safe, transparent, and cross-sector data sharing, with a particular focus on public-sector data and data altruism (i.e. voluntary sharing of data for the public good). While the DGA is not aimed specifically at educational institutions, it offers opportunities for the sector to benefit from enhanced data sharing, particularly through the reuse of public data and the implementation of data altruism initiatives. *Data Governance Act*.

4. THE DATA ACT (DA)

It introduces changes to how data is accessed, shared, and managed across various sectors, including education. It introduces obligations to improve data portability and protect intellectual property and outlines (emergency or crisis) conditions under which public sector bodies may access private sector data. Its primary objectives are to promote fair use of data, prevent imbalances in the market, and foster innovation. The DA also emphasises the importance of data literacy. *Data Act*.

5. THE CYBER SECURITY ACT (CSA)

It aims to strengthen cybersecurity across the EU, and is focused on the creation of a robust cybersecurity framework supported by the European Union Agency for Cybersecurity (ENISA). In the educational sector, the Act brings about changes by raising awareness of cybersecurity and promoting cyber literacy in educational institutions. *Cybersecurity Act*.

6. THE CYBER RESILIENCE ACT (CRA)

It establishes a robust cybersecurity framework aimed at enhancing the security of all products with digital elements (PDEs), including products with AI components, within the European Union, targeting particularly the Internet of Things. The Act aims to ensure that manufacturers maintain cyber security through the lifecycle of products, and provide appropriate information to consumers. *Cyber Resilience Act*.

7. THE ARTIFICIAL INTELLIGENCE ACT (AI ACT)

It addresses potential risks to citizens' health, safety, and fundamental rights. Based on a general risk-based approach, the Act pays particular attention to AI systems that are classified as high-risk, i.e. those which can negatively affect safety or fundamental human rights. The Act distinguishes between a provider (an entity that develops an AI system and makes it available) and a deployer (any user of an AI system except for personal and non-professional activities) and defines requirements and obligations for each. *Artificial Intelligence Act*.