Legal Newsletter August 2024

1. Legislation on artificial intelligence

Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (AI) was published on 12 July 2024 in the Journal of the European Union and has a gradual applicability, starting on 2 February 2025.

The rules of the Regulation will apply as follows:

- the prohibitions and general provisions of the Regulation should apply from 2 February 2025
- the provisions on notified bodies, governance structure, obligations of providers of general purpose AI models and penalties should apply from 2 August 2025
- the codes of best practice should be ready by 2 May 2025, in order to allow suppliers to demonstrate compliance in good time

Key aspects of the first two chapters of the Regulation:

- providers and implementers of AI systems shall take measures to ensure, to the greatest extent possible, a sufficient level of AI literacy among their personnel and other persons engaged in the operation and use of AI systems on their behalf, taking into consideration their technical knowledge, experience, education and training, and the context in which the AI systems are to be used and taking into account the persons or groups of persons in relation to whom the AI systems are to be used
- the Regulation prohibits the placing on the market, putting into service or use of an AI system that employs subliminal techniques that cannot be consciously perceived by a person or intentionally manipulative or deceptive techniques with the purpose or effect of significantly distorting the behaviour of a person or group of persons by significantly impairing their ability to make an informed decision, thereby causing them to take a decision that they would not otherwise have taken, in a manner which causes or is reasonably likely to cause significant detriment to that person, another person or group of persons
- the Regulation prohibits the placing on the market, putting into service for this specific purpose or the use of AI systems to infer the emotions of a natural person within the sphere of the workplace or educational institutions, except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons

Source: Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence

2. Cyber security legislative mechanisms – NIS 2

Directive (EU) 2022/2555 on measures for a high common level of cybersecurity in the European Union must be transposed into national law by 17 October 2024.

The Directive, known as NIS 2, establishes a common regulatory framework in the field of cybersecurity with the aim of increasing the level of cybersecurity in the European Union, requiring member states to strengthen cybersecurity capabilities and introducing cybersecurity risk management and reporting measures in critical sectors, together with rules on cooperation, information sharing, supervision and law enforcement.

Cybersecurity refers to the activities necessary to protect networks and information systems, the users of such

systems and other persons affected by cyber threats.

The Directive applies mainly to medium and large entities operating in sectors of high critical importance, such as:

- energy (electricity, including generation, distribution and transport systems and charging points; district heating and district cooling; oil, including production, storage and transport pipelines; gas, including supply, distribution and transport systems, and storage systems; and hydrogen)
- air, rail, sea and road transport
- the banking sector and financial market infrastructures, such as credit institutions, trading venue operators and central counterparties
- health, including healthcare providers, manufacturers of key pharmaceuticals and essential medical devices, and EU reference laboratories
- digital infrastructure, including providers of data centre services, cloud computing services, public electronic communications networks and publicly accessible electronic communications services
- business-to-business ICT service management
- public administration at central and regional level

Each member state must adopt a national strategy to achieve and maintain a high level of cybersecurity in critical sectors, such as:

- a governance framework clarifying the roles and responsibilities of relevant stakeholders at national level
- supply chain security policies
- vulnerability management policies
- policies on the promotion and development of cyber security education and training
- measures to improve citizens' awareness of cyber security

Source: Directive (EU) 2022/2555 on measures for a high common level of cyber security in the Union

This newsletter is a service of TPA Romania.

TPA Romania
Crystal Tower Building,
48 Iancu de Hunedoara Blvd.
011745 Bucharest, Romania
Tel: +40 21 310 06-69
Fax: +40 21 310 06-68
www.tpa-group.ro
www.tpa-group.com

To receive regular updates from TPA Romania, please sign up for our newsletter.

Dan Iliescu
Legal Services Partner
email: dan.iliescu@tpa-group.ro

Legal Newsletter August 2024

IMPRINT Information updated: January 2024. This information has been simplified and is not a substitute for individual advice.
TPA Romania is an independent member of the Baker Tilly Europe Alliance. Tel: +40 21 3100669. Homepage: www.tpa-group.ro. Concept and design: TPA Romania