

arendt enterprises



Navigating the digital legal landscape: exploring recent and upcoming tech regulations for business success

Les midis de l'entreprise

Arendt & Medernach SA, Luxembourg

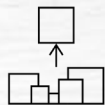
31 January 2024

arendt.com

CONFIDENTIALITY REMINDER

This document is confidential and is intended solely for its recipient.
Do not distribute outside your organisation.





arendt entreprises



Your contacts/speakers



Faustine Cachera
Senior associate
IP, Communication &
Technology



Sophie Calmes
Senior associate
IP, Communication &
Technology



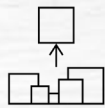
Sofia Franzina
Associate
IP, Communication &
Technology



Julien Pétré
Senior associate
IP, Communication &
Technology



Astrid Wagner
Partner
IP, Communication &
Technology



arendt enterprises



Table of contents

1. Introduction

2. The Digital Services Act

3. Cybersecurity/ICT

4. The Data Strategy

5. The AI Act

The European Digital Strategy



Digital Services Package:

- Digital Services Act
- Digital Markets Act

- Create a **safe digital space for consumers** establishing accountability of digital platforms;
- Allow **free and fair competition in the digital sector** by combating anti-competitive practices by Internet giants.

Cybersecurity/ICT:

- NIS2 Directive
- DORA

- Strengthen and establish a **common level of cybersecurity**;
- **Technical requirements for financial entities and ICT providers on ICT risk-management, incident reporting, operational resilience testing and ICT third-party risk monitoring.**

The Data Strategy:

- Data Act
- Data Governance Act

- Create a **single market for data** allowing it to flow freely within the EU and across sectors for the benefit of businesses, researchers and public administrations;
- Trusted mechanisms and services for **access, re-use, sharing and pooling of data.**

The AI Package:

- The AI Act
- AI Liability Directive
- Product Liability Directive

- **Global regulatory framework** applicable to all AI industry stakeholders with a link to the European market;
- **Adapt liability rules to the digital age**, ensuring that victims are compensated for damages caused by unsafe products, including digital products and AI systems.

The Digital Services Act

The Digital Services Act (DSA)



- Scope: applies to **all online intermediaries** who offer goods, content or services on **the European market** (regardless of their place of establishment). E.g. internet service providers, online platforms (*marketplaces*), travel platforms, social networks, etc.
- Application: **17 February 2024**
- Competent authority: **Digital Services Coordinator**
- Non-compliance with DSA: penalty payments of **up to 6% of worldwide annual turnover**



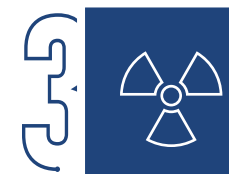
Combating illegal content

- Tool for reporting illegal content (once reported, removed or blocked)
- *Market places* must do a better job of tracking sellers on their platform + better informing consumers



Online transparency

- Internal complaints handling system
- Explain how algorithms work
- Very large platforms / search engines: offer a content recommendation system not based on profiling
- Targeted advertising to minors banned on all platforms
- *Dark patterns* + prohibited practices designed to mislead



Risk mitigation and crisis response

- Very large platforms / search engines:
 - Analysis of the systemic risks they generate
 - Independent risk reduction audits
 - Provision of algorithms and their interfaces to the Commission / national authorities
 - Access to key interface data for researchers
 - Better protection for minors

Cybersecurity / Cyber resilience

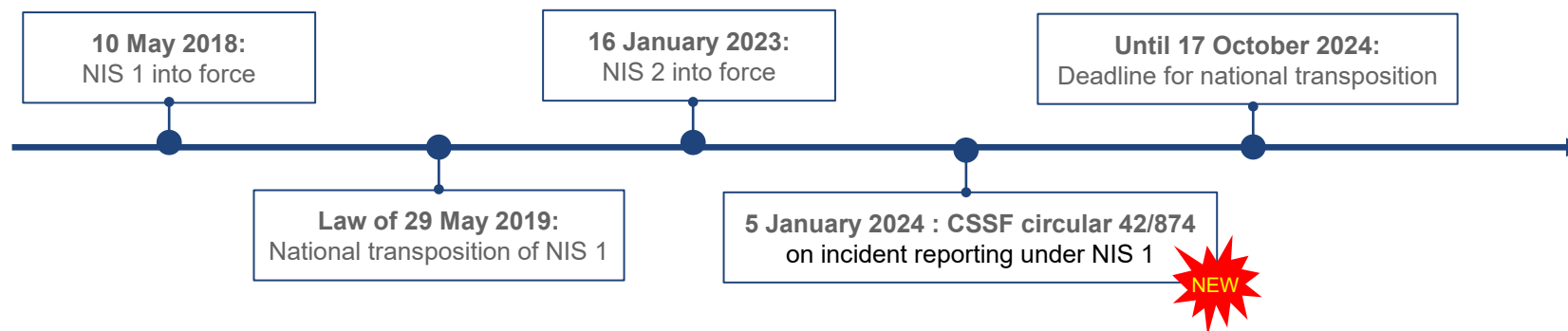
NIS 2 Directive (1/3)



I. Overview

➔ ‘Network and Information Society’ (NIS): achieve a high level of cybersecurity in sectors crucial to the functioning of our society

The NIS 2 Directive repeals and replaces the existing NIS 1 Directive, transposed into Luxembourg law by the law of 29 May 2019 & the recent CSSF circular 24/847. Member States have until 17 October 2024 to transpose NIS 2. No bill of law has been published yet.



- Competent authorities: **CSSF** and **ILR**
- Single point of contact: **ILR**
- CSIRT: Computer Incident Response Centre Luxembourg (**CIRCL**)




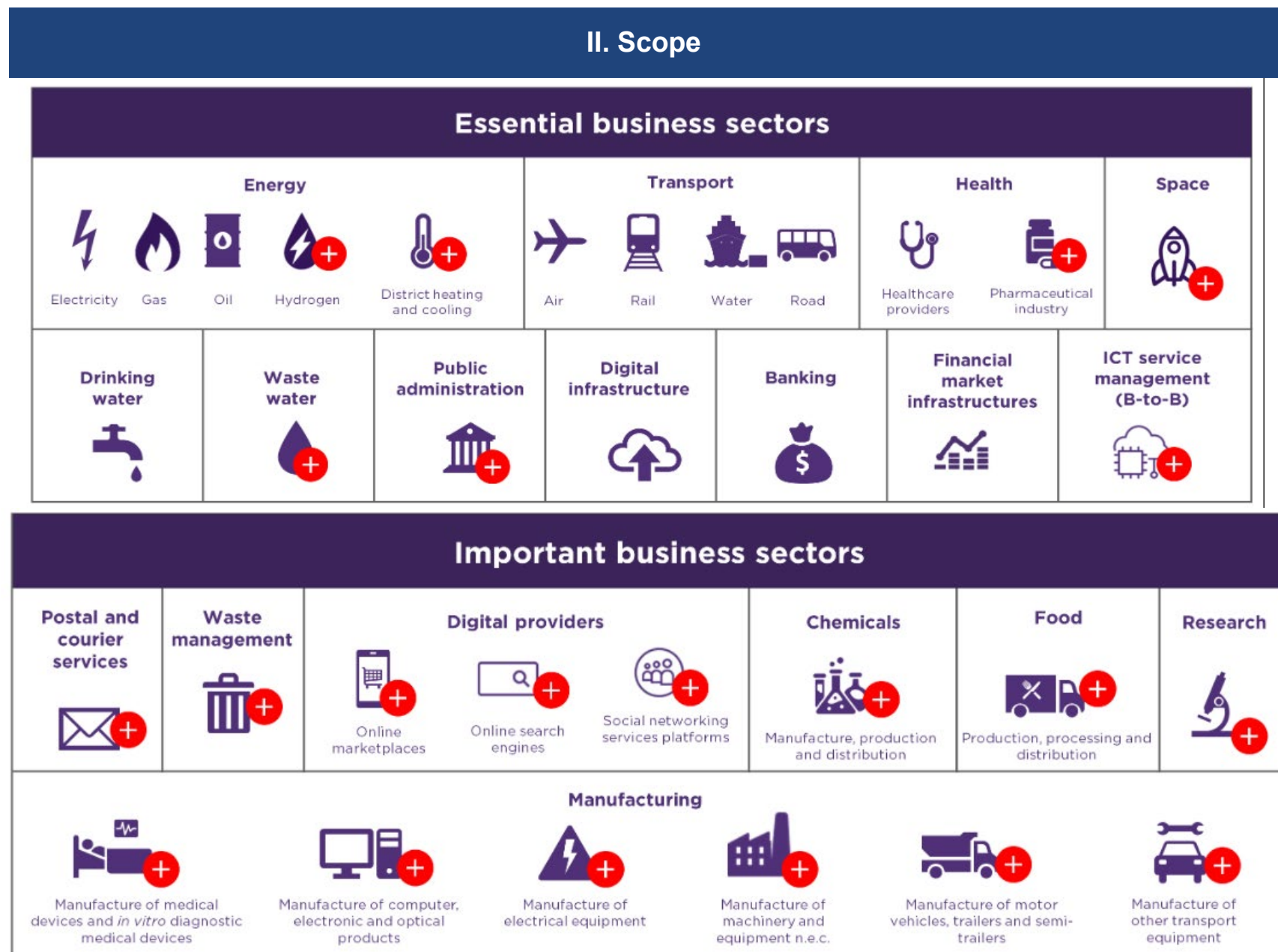
Non-compliance: Tougher sanctions with NIS 2: **10 million euros / 2%** total worldwide annual turnover for **EE** and **7 million euros / 1.4%** total worldwide annual turnover for **IE**.

NIS 2 Directive (2/3)

Essential sectors: sectors of high criticality that are essential for the maintenance of critical societal and/or economic activities

Important sectors: other critical sectors, including entities not attending the criteria under NIS 2 for the qualification as essential entities

 Sectors added by the NIS 2 Directive



NIS 2 Directive (3/3)

III. Obligations for in-scope entities



Cyber risk assessment



Implementation of **technological tools** to improve cyber security (data encryption, enhanced authentication solutions, access control, etc.)



Appropriate trainings for employees and management bodies



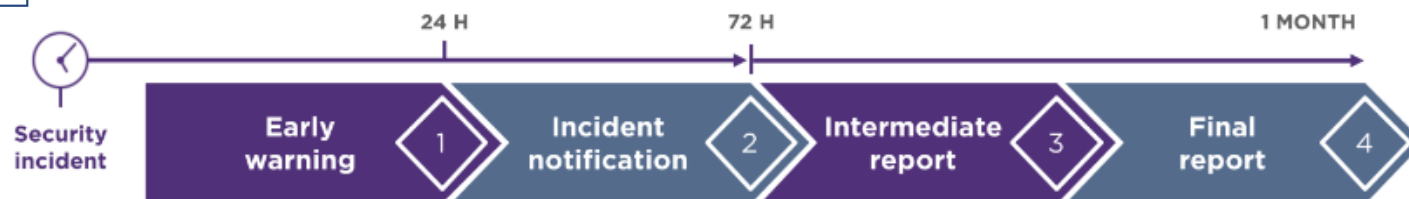
Regular testing to assess the effectiveness of the security measures deployed



Implementation of measures to guarantee **business continuity** in the event of a cyber incident



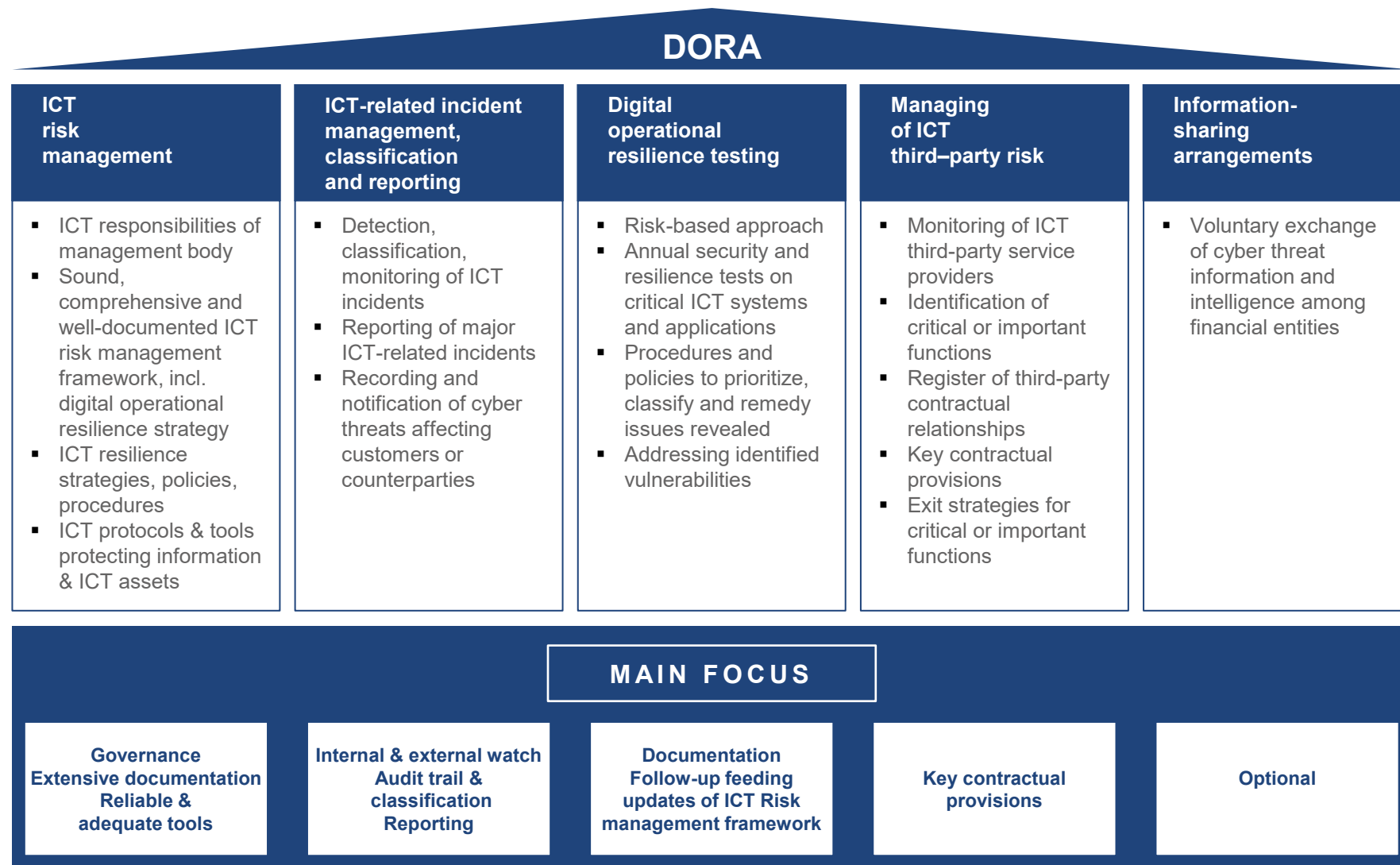
Reporting of significant cyber incidents within 24 hours to the appropriate authority



What is DORA?



DORA creates a regulatory framework on digital operational resilience whereby all EU financial entities are required to ensure they can withstand, respond to and recover from all types of ICT-related disruptions and threats.



DORA - Specific board focused provisions



Knowledge and skills:

Board members shall actively keep up to date with **sufficient knowledge and skills** to understand and assess ICT risk and its impact on the operations of the bank, including by following specific training on a regular basis, proportionate to the ICT risk being managed.

Senior ICT staff shall **report at least yearly** to the board on the findings of digital operational resilience testing and put forward recommendations



Administrative penalties and remedial measures to members of the board and to other individuals who are responsible for the breach



At least major ICT-related incidents are reported to relevant senior management and **inform the board of at least major ICT-related incidents**, explaining the impact, response and additional controls to be established as a result of such ICT-related incidents



The board shall **regularly review the risks identified in respect to contractual arrangements on the use of ICT services supporting critical or important functions**



Your legal “to do list” by 17 January 2025

- ☐ Map the ICT services used by the company.
- ☐ Classify services according to whether or not they concern critical or important functions.
- ☐ Review of agreements in place.
- ☐ Negotiate any contractual changes that may be necessary to comply with DORA.
- ☐ If a new service provider is used, check that the contract complies with DORA's contractual requirements.

The Data Strategy

First key pillar of the European strategy for data

- Scope: establishes conditions and frameworks for the **re-use of data held by public sector bodies** which are protected due to commercial or statistical confidentiality, intellectual property rights of third parties or the protection of personal data and seeks to **increase trust in data sharing**, strengthen mechanisms to **increase data availability** and overcome technical obstacles to the reuse of data.
- Application: **24 September 2023 (entry into force: 23 June 2022)**
- Competent authority: TBC by Luxembourg
- Non-compliance with the Data Governance Act: TBC by Luxembourg

Key elements

International data
flows

Re-use of data
held by public
sector bodies

Data intermediation
services (data
marketplaces)

European Data
Innovation Board

Data
altruism

Use cases

Re-use of data – Findata | **Data intermediation services** - Data Intelligence Hub, Deutsche Telekom | **Data altruism** - The Smart Citizen

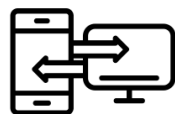
The Data Governance Act (DGA)

- Scope: establishes rules on the **sharing of data generated through the use of connected products or related services** (e.g. the Internet of Things (IoT) and industrial machinery) **and allows users to access the data they generate**.
- Application: **September 2025 (entry into force: 11 January 2024)**
- Competent authority: TBC by Luxembourg
- Non-compliance with the Data Act: TBC by Luxembourg

The Data Act

Complements the Data Governance Act

Clarifies who can create value from data and under which conditions



Data sharing

Grants users the right to access, port or share with a third party of their choice the data they contributed to generating – establishing clear rules => increase legal certainty



Public sector access

Public sector bodies are granted access to and use of privately held (personal and non-personal) data in circumstances of clear public interest – example: public emergency



Cloud markets

Provides for data and cloud interoperability rules allowing end users to effectively switch between cloud and edge service providers



Data markets

Data owners and data generators can monetize data by sharing, selling or licensing the generated data to other companies – mitigating the abuse of contractual imbalances



Trade secret protection

Specific provisions that concern safeguarding data related to trade secrets against possible abusive behaviour of data holders

Use cases

Industrial equipment - optimise operational cycles, production lines and supply chain management, leveraging machine-learning technologies | precision agriculture | insuretech | fintech

The AI Act

I. The AI Act



- **Horizontal effect** → sets out directly applicable rules on the development, marketing, commissioning and use of artificial intelligence systems, including *inter alia*, machine learning training, testing and validation datasets.
- **Global regulatory framework** → applicable to all AI industry stakeholders (e.g. providers, users, importers and distributors) with a link to the European market.
- **Risk based approach** → ranks AI systems according to the risks their use and outputs pose to a person's fundamental rights.
- **Very high penalties** → Up to 35 000 000 EUR or 7% of its total worldwide annual turnover in the previous financial year (whichever is higher) for prohibited practices

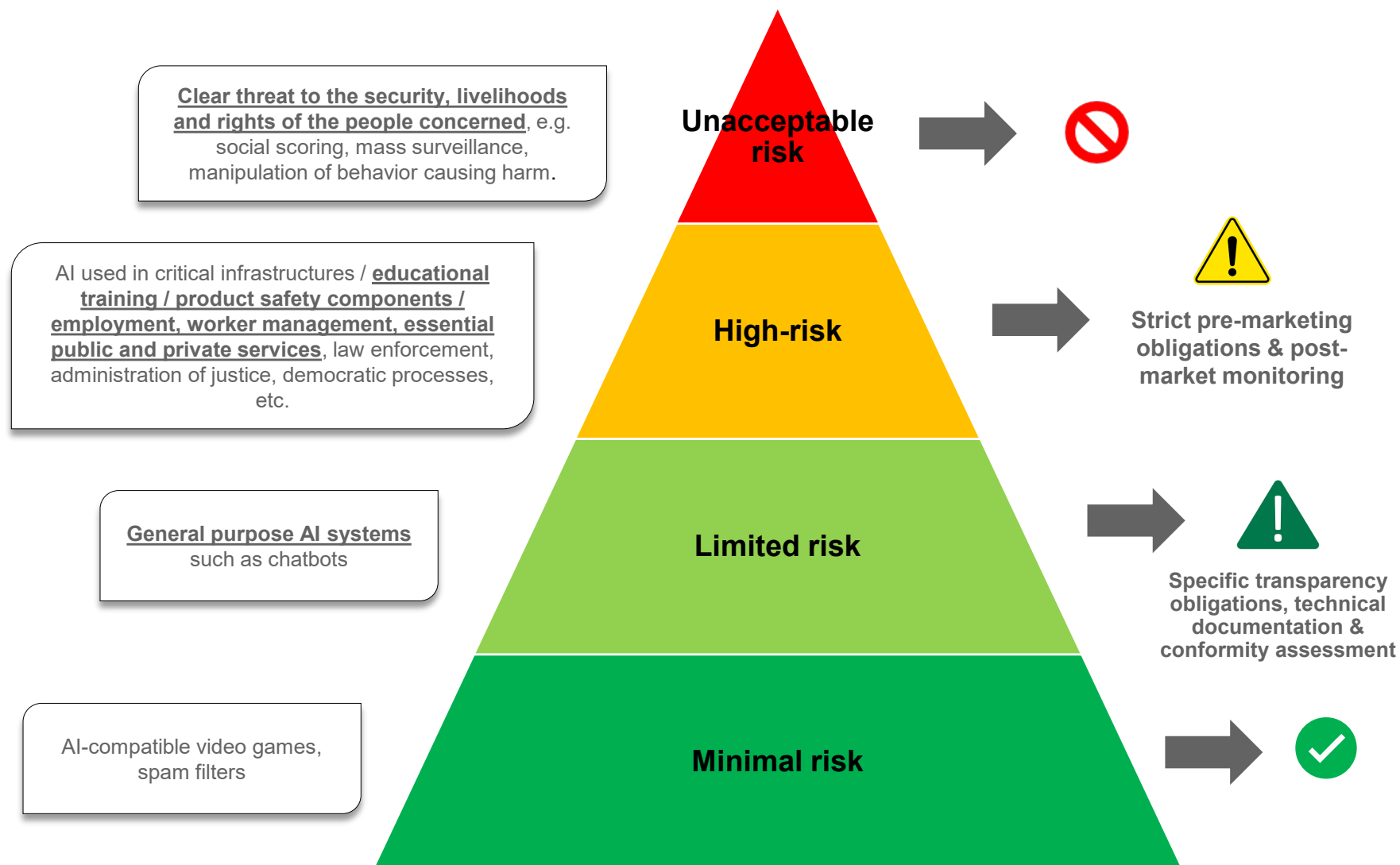
Broad and technology neutral definition of an “**artificial intelligence system**”:

“a **machine-based system** designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to **generate outputs** such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.”

Definition of a “**general purpose AI system**”:

“an AI model, including when trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable to competently **perform a wide range of distinct tasks** regardless of the way the model is placed on the market and that can be **integrated** into a **variety of downstream systems or applications**. This does not cover AI models that are used before release on the market for research, development and prototyping activities.”

II. The AI Act



Q&A

Save the date

-

Tuesday 27 February at 12.30pm

Luxembourg tax update: Modernisation of
the investment tax credit regime and
personal income tax changes

Your contacts/speakers



Faustine Cachera
Senior associate
IP, Communication &
Technology
faustine.cachera@arendt.com
+352 40 78 78 339



Sophie Calmes
Senior associate
IP, Communication &
Technology
sophie.calmes@arendt.com
+352 40 78 78 267



Sofia Franzina
Associate
IP, Communication &
Technology
sofia.franzina@arendt.com
+352 40 78 78 7437



Julien Pétré
Senior associate
IP, Communication &
Technology
julien.petre@arendt.com
+352 40 78 78 2139



Astrid Wagner
Partner
IP, Communication &
Technology
astrid.wagner@arendt.com
+352 40 78 78 698

