DEEP DIVE

DIGITAL LEGAL ACADEMY 2024

by TaylorWessing

CRA & PLD – new security requirements for digital products

Dr Michael Kieffer and Dr Paul Voigt

Agenda

DEEP DIVE
DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

1 Cyber Resilience Act

2 Product Liability Directive

3 Contacts

DEEP DIVE

DIGITAL LEGAL ACADEMY 2024

by TaylorWessing

1 Cyber Resilience Act

Introduction

DEEP DIVE
DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

- **Objective**
  - Introducing cybersecurity requirements for a broad scope of tangible and non-tangible products with digital elements, including non-embedded software
  - Horizontal, cross-sectoral regulatory approach

- **Timeline**
  - Published in EU Official Journal on 20 November 2024
  - Most provisions of CRA **apply from 11 December 2027**
    - Reporting obligation of manufacturers (Art. 14) applies from 11 September 2026
    - Provisions on the notification of conformity assessment bodies (Art. 35 to 51) apply from 11 June 2026

Scope of application (Art. 2 CRA)

DEEP DIVE
DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

- **Material scope:**
  - **Products with digital elements** the intended purpose or reasonably foreseeable use of which includes a **direct or indirect logical or physical data connection** to a device or network
  - Thus, the CRA does not apply to SaaS
- **Personal scope:** manufacturers, importers and distributors
- **Territorial scope:** making available on the market
- “manufacturer“ and “product with digital elements“ are intended to be understood broadly
- **Exceptions:**
  - E.g. for certain medical devices and product with military purposes
  - Free and open-source software only covered by CRA if it is intended for commercial activities

Obligations of manufacturers (Art. 13 CRA)

DEEP DIVE
DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

- **Design, development und production in accordance with Annex I,** e.g.
  - Ensure an appropriate level of cybersecurity
  - Only make available on the market products without known exploitable vulnerabilities
  - Secure by default configuration

For ‘critical’ products with digital elements (Art. 8, Annex IV), compliance with Annex I must be demonstrated by obtaining a certain **European cybersecurity certificate** under a European cybersecurity certification scheme adopted pursuant to Cyber Security Act (Regulation (EU) 2019/881)

Obligations of manufacturers (Art. 13 CRA)

DEEP DIVE
DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

Cybersecurity **risk assessment** to determine and mitigate potential risks

Due diligence when integrating components sourced from third parties

Systemical documentation of all relevant cybersecurity aspects

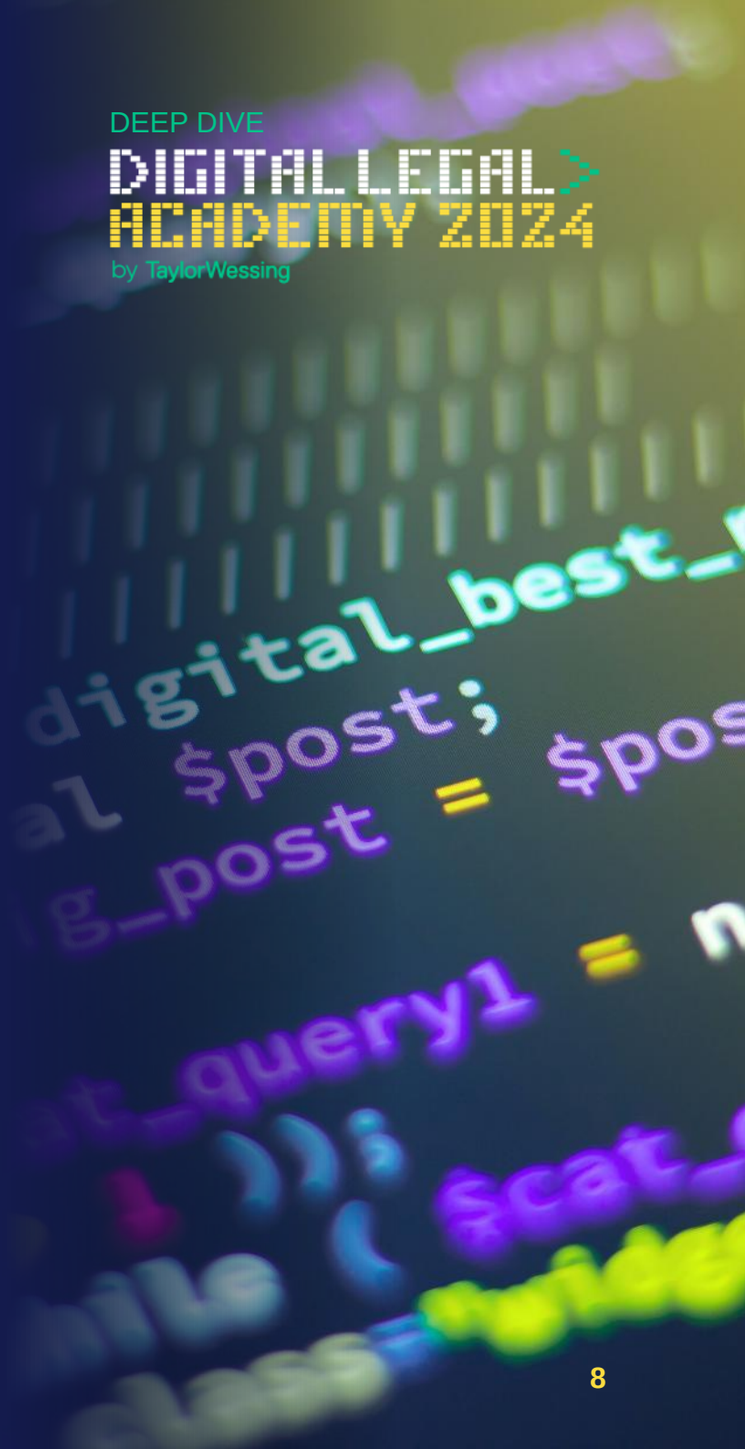
Providing **security updates** and **addressing/remediating vulnerabilites** during the support period (generally at least 5 years)

Obligations of manufacturers (Art. 13 / 14 CRA)

DEEP DIVE
DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

- (risk-based) **conformity assessment procedure**, and after successful completion:
  - CE marking
  - EU declaration of conformity

- Providing information and instructions (in accordance with Annex II)
  - E.g. early warning notification to ENISA within 24h after becoming aware of an actively exploited vulnerability



Obligations of importers (Art. 19 CRA)

DEEP DIVE
DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

- Importers must ensure that…

the manufacturer has carried out the appropriate conformity assessment procedures	the manufacturer has fulfilled all of his obligations regarding information of consumers	the product bears the CE marking and is accompanied by the necessary documents and information

- Importers must place on the market only products with digital elements that comply with the essential cybersecurity requirements (Part I of Annex I)

Obligations of importers (Art. 19 CRA)

- Indicate their name, registered trade name or registered trademark, the postal address, email address or other digital contact and the website at which they can be contacted on the product or on its packaging
- Keep a copy of the EU declaration of conformity for at least 10 years after placing a product on the market
- Obligation to take corrective measures if necessary and to report to the market surveillance authority if a product does not comply with the CRA
- Obligation to report to market surveillance authorities and – if possible – to users in case the manufacturer has ceased its operations

Obligations of distributors (Art. 20 CRA)

DEEP DIVE
DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

- Distributors must act with due care in relation to the CRA requirements when making a product available on the market

- Ensuring that…

the product bears the CE marking	the manufacturer and the importer have complied with their obligations and provided all necessary documents to the distributor

- Reporting obligations…

to manufacturer if distributor becomes aware of vulnerabilities	to market surveillance authorities if the product poses a significant cybersecurity risk	to market surveillance authorities and – if possible – users in case the manufacturer has ceased its operations

Market surveillance and penalties

DEEP DIVE
DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

Market surveillance authorities

- Tasked to supervise effective CRA implementation
- Each member state has to designate at least one market surveillance authority
- Evaluation of products that present a significant cybersecurity risk

Penalties (Art. 64 CRA)

▪ Non-compliance with the **essential cybersecurity requirements** (Annex I) ▪ Non-compliance with manufacturers‘ obligations (Art. 13 and 14)	→ administrative fines of up to **EUR 15.000.000** or, if the offender is an undertaking, up to **2.5 %** of the total worldwide annual turnover
▪ Non-compliance with obligations of **authorized representatives, importers or distributors** (Art. 18 bis 23) ▪ Non-compliance with requirements regarding the **EU declaration of conformity** (Art. 28) ▪ Non-compliance with requirements regarding the **CE marking** and **technical documentation** (Art. 30(1) to (4), 31(1) to (4), 33(5)) ▪ Non-compliance with requirements regarding the **conformity assessment procedure** (Art. 32(1) to (3)) ▪ Non-compliance with obligations of **notified bodies** (Art. 39, 41, 47, 49 and 53)	→ administrative fines of up to **EUR 10.000.000** or, if the offender is an undertaking, up to **2 %** of the total worldwide annual turnover
▪ Supply of **incorrect, incomplete or misleading information** to notified bodies and market surveillance authorities	→ administrative fines of up to **EUR 5.000.000** or, if the offender is an undertaking, up to **1 %** of the total worldwide annual turnover

DEEP DIVE

DIGITAL LEGAL ACADEMY 2024

by TaylorWessing

2 Product Liability Directive 2024

Introduction

DEEP DIVE
DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

- **Objective**
  - The aim of the Product Liability Directive (PLD) is to establish an EU-wide system for compensating people who have suffered personal injury or property damage as a result of defective products.

- **Timeline**
  - Publication in the Official Journal on 18 November 2024
  - **Entry into force** on 8 December 2024
  - Member States then have 2 years to **implement**
  - **Products** placed on the market or put into service after 9 December 2026 are covered (note exceptions)

Protected legal interests (Art. 6 PLD)

DEEP DIVE
DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

- **Death, bodily injury including injury to mental health**
- **Damage/destruction of property**
  - **Exceptions:**

not the defective product itself	not items that are used exclusively for professional purposes

- **Destruction or falsification of data** (only for non-professional purposes)

  However, if the data is only of sentimental value, the costs of recovering or restoring the data can be *claimed*

Product (Art. 4 No. 1 PLD)

DEEP DIVE
DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

Product

So far

- Any **movables** even if integrated into, or inter-connected with, another movable or an immovable and and **electricity**

In future: Expansion

- Also explicitly **software**
  - **Examples:** Operating systems, firmware, computer programmes, applications or AI systems
  - **Type of provision and use:** It does not matter whether the software is stored on a device, accessed via a communication network or cloud technologies or supplied through a software-as-a-service model.
- Purely digital **digital manufacturing files / construction files** (also 3D printing),
- **Raw materials**

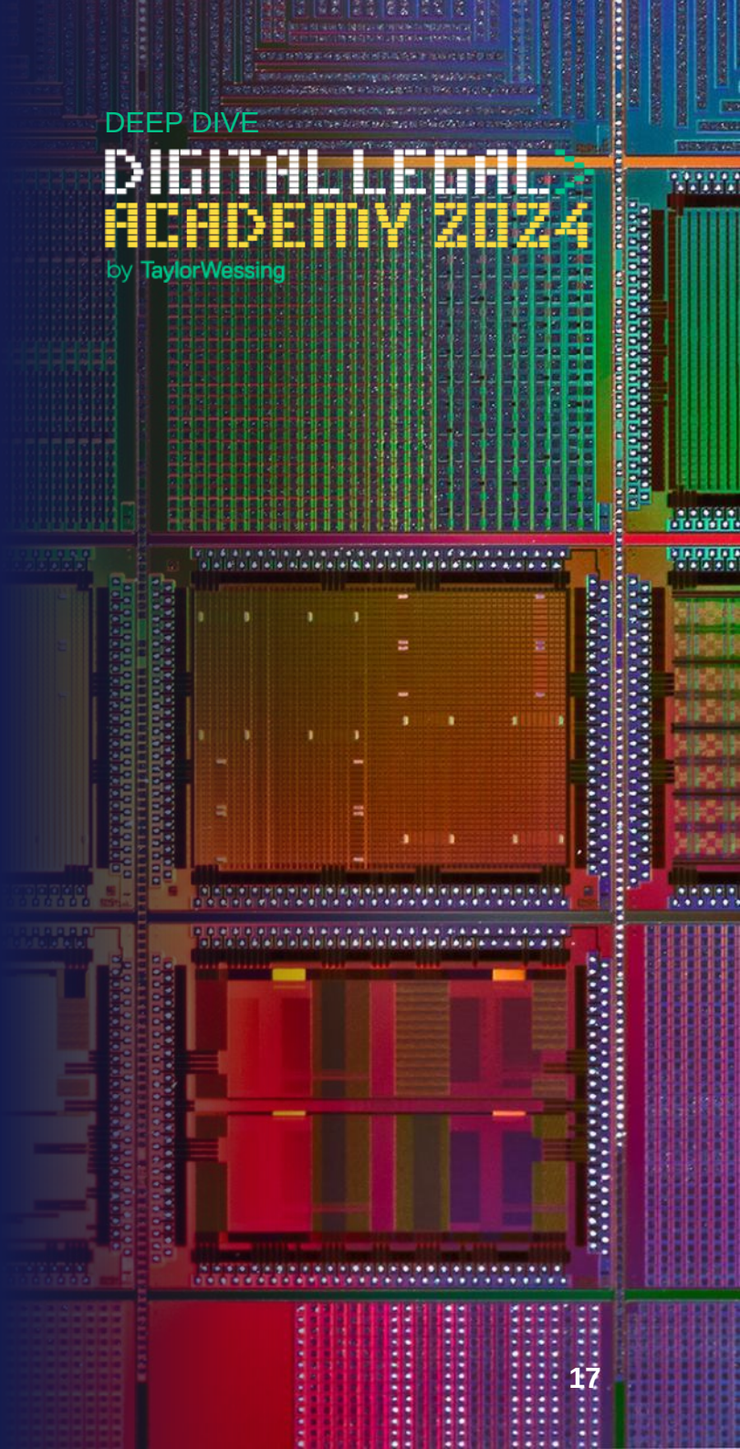
Product (Art. 4 No. 1 PLD)

No product

- **Open Source Software**
  There is an exception for open source software (OSS) in order not to hinder innovation and research. Free and open source software that is developed or provided outside of a commercial activity is excluded from the scope of the PLD.
  However: If the software is provided for a fee or if personal data is used that is not exclusively for the purpose of improving the security, compatibility or interoperability of the software, the PLD applies

- **Information**
  PLD does not apply to the content of digital files such as media files, e-books or the mere source code of software. For example, the PLD does not apply to false tips in a newspaper app

- **Pure digital services**
  Current problem: Differentiation between software-as-a-service model (covered) and pure digital services (not covered). This determines, for example, whether liability for psychological damage caused by online games



Product defects (Art. 7 PLD)

DEEP DIVE
DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

Error

So far

- Failure to maintain the level of safety that can reasonably be expected.
- Not simply because an improved product is later placed on the market (even in the future)
- To be considered:
- Presentation, labelling, design, composition, packaging, instructions (for use, assembly, installation, maintenance).

In future: Extension of circumstances eligible for consideration

- **"reasonably foreseeable"** use of the product
- **AI:** Learning ability after placing on the market: Relevant for software that in the case of AI the underlying algorithms must be designed in such a way that dangerous product behaviour is prevented
- **Combination hazards:** the interaction of two products can result in dangerous interactions without the individual product itself being defective. Example of IoT device and software
- **Product safety requirements** (including CRA)
- Etc.

Product defects (Art. 7 PLD)

DEEP DIVE
DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

Error Relevant date

So far

- Placing on the market (as before) or putting into service (clarification).

In future: Extension of circumstances eligible for consideration

- If the manufacturer **retains control of the product** after this date, the date from which the product is no longer under the control of the manufacturer also applies.
- For example, for updates/upgrades
- If the manufacturer is able to provide software updates or upgrades themselves or have them provided. Update capability of a product is sufficient. The manufacturer's decision to discontinue update support is not sufficient for loss of control.

Excursus: Obligation to update (Art. 7 PLD)

DEEP DIVE
DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

Eternal liability due to update obligation?

Claims are subject to an absolute limitation period of ten years from the date of placing on the market (Art. 17 I . a PLD).

Since after this time, despite control, no liability, update obligation expires

However, if an update leads to a significant change- to the product, the period begins again.

In the field of cyber security, discrepancy with CRA after at least 5 years and expected useful life.

Who is liable (Art. 8 PLD)

DEEP DIVE
DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

Who is liable?

So far

- **Manufacturer** of the end product, quasi-manufacturer, basic material manufacturer, partial product manufacturer
  - Example: In the event of errors in the software integrated into the product ("embedded software"), not only the end manufacturer but also the software manufacturer is liable
- **Importeur**,
- **Supplier** (subsidiary)

In future: Expansion

- the ("authorised") **representative**
- The **fulfilment service provider** (if not an importer or authorised representative established in the EU)
- **Online platforms** (subsidiary as well as retailers) with the possibility of concluding distance contracts with traders
- Anyone who significantly modifies a product and makes it available on the market or puts it into operation
- The original manufacturer is not liable if the safety properties of a product are adversely modified by third parties and the product defect did not exist when the product was placed on the market.

Please note, market players are always liable alongside each other. The injured party may choose the "best" one.

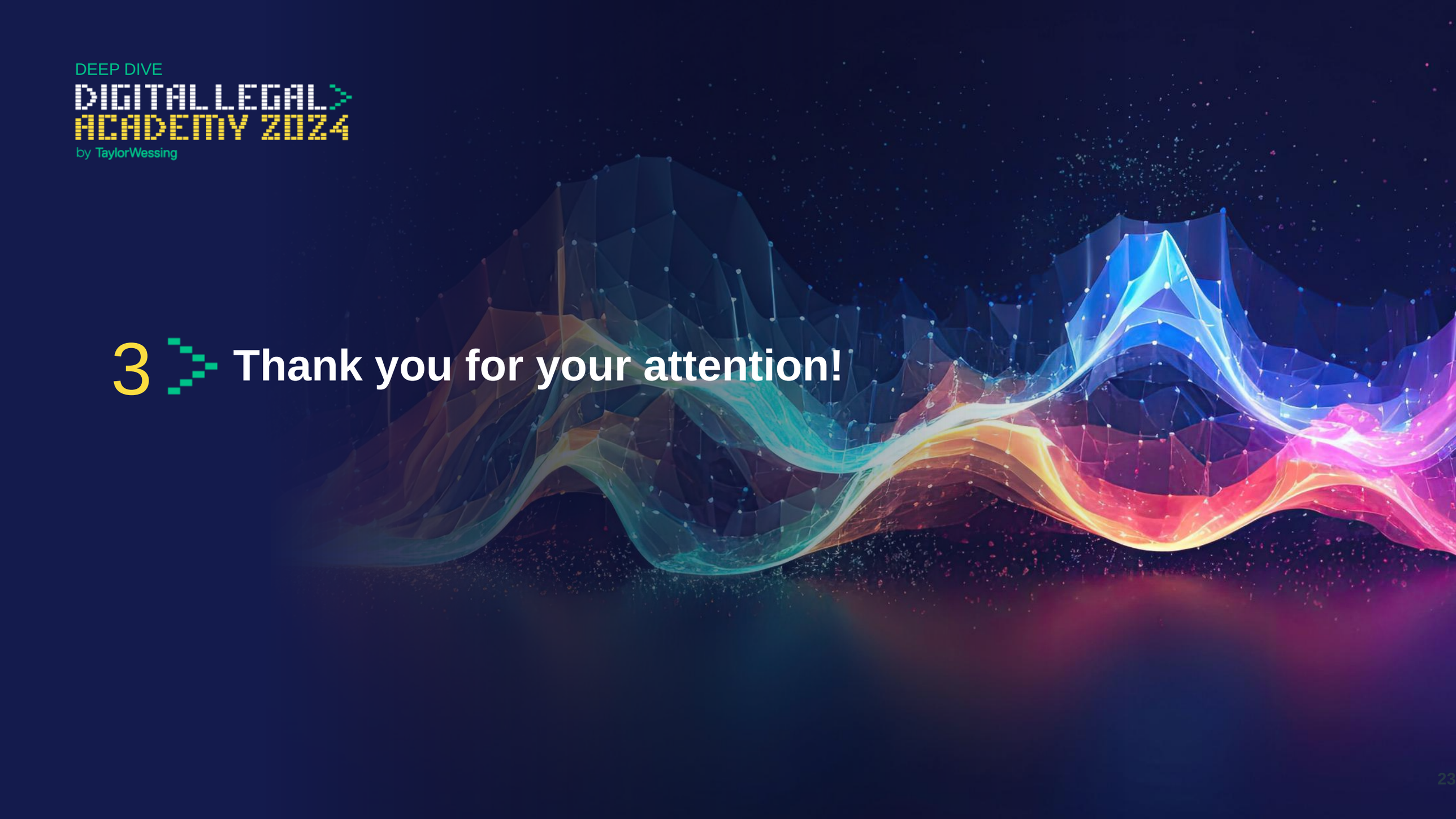
Damages

DEEP DIVE
DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

- **Scope**

Total repair now without upper liability limits	No deductible for property damage (previously EUR 500)	Compensation for immaterial damages

- **Facilitation of evidence**
- **New: Disclosure of evidence:** mutual obligations to disclose evidence where necessary and appropriate (protection of business secrets). The victim must make plausible the conditions on which the claim is based
- **New: Presumption of fault and causality**



3 Thank you for your attention!

Speaker

DEEP DIVE
DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

Dr Michael Kieffer

m.kieffer@taylorwessing.com

Dr Paul Voigt

p.voigt@taylorwessing.com

taylorwessing.com

© Taylor Wessing 2024

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.