

Regulatory Landscape Preparedness and the Lawyer's Role in Crisis Management

Tanguy Van Overstraeten & Gert-Jan Fraeyman

12 February 2026

Belgium-Japan Association
Chamber of Commerce
日白協会兼商工会議所



VB
Van Bael & Bellis

“

*There are only two types of companies:
those that have been hacked, and those
that will be.”*

Robert Mueller – FBI Director

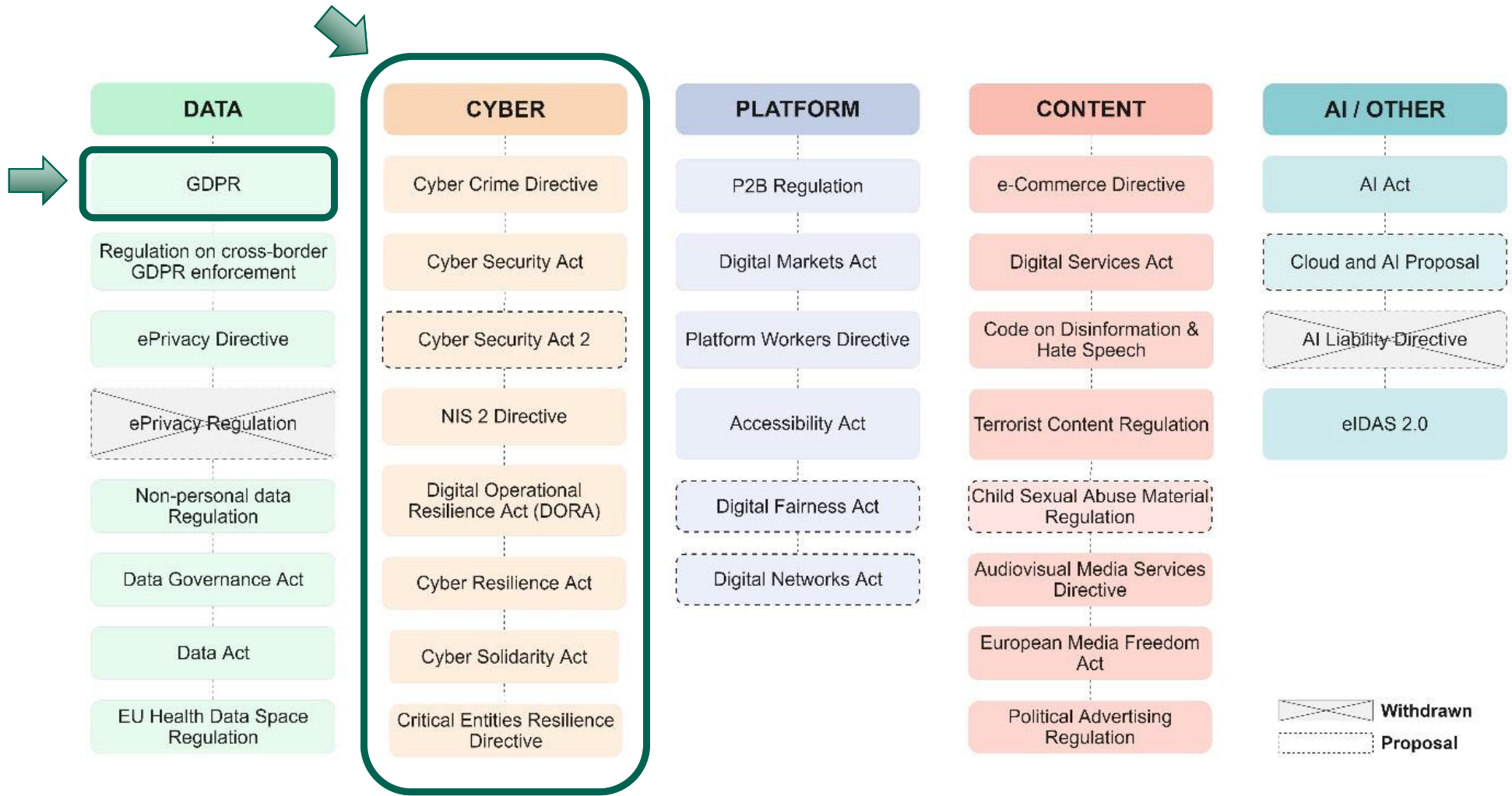
Overview

- 01 EU Cyber Regulatory Landscape
- 02 Cyber Preparedness / Crisis Management
- 03 Conclusions

Overview

- 01** EU Cyber Regulatory Landscape
- 02** Cyber Preparedness / Crisis Management
- 03** Conclusions

5 EU Cyber Regulatory Landscape



GDPR

- Protect data against unauthorised access, loss, destruction or disclosure
- Need to implement appropriate technical and organisational measures (Art. 32)
- Notifications of data breaches (Art. 33-34)
- Penalties (Art. 83)
 - Severe violations: up to (i) EUR 20 M or (ii) 4% of total global turnover
 - Other violations: up to (i) EUR 10 M or (ii) 2% of total global turnover

GDPR

- Protect data against unauthorised access, loss, destruction or disclosure
- Need to implement appropriate technical and organisational measures (Art. 32)
- Notifications of data breaches (Art. 33-34)
- Penalties (Art. 83)
 - Severe violations: up to (i) EUR 20 M or (ii) 4% of total global turnover
 - **Other violations: up to (i) EUR 10 M or (ii) 2% of total global turnover**

NIS2 Directive | 1

- Applies to essential entities and important entities → lists in two annexes
- Implementation in national laws – fragmentation risk
- Key obligations:
 - Preventive measures
 - Notification of cyber incidents
- Digital Omnibus: simplification – single entry-point for notifications

NIS2 Directive | 2

- NIS2 Directive: transposition deadline = 17/10/2024
 - Belgian NIS2 Law of 26 April 2024 – entry into force 18/10/2024
- Belgian Centre for Cybersecurity Belgium (CCB)
- Penalties:
 - Important entities: up to EUR 7 M or 1.4% of global annual turnover
 - Essential entities: up to EUR 10 M or 2% of global annual turnover
- Personal liability of directors

Cyber Resilience Act (CRA)

- Products with digital elements: software + hardware
- Mandatory cybersecurity requirements for manufacturers
 - Cybersecurity by design
 - Risk assessment
 - User information
 - Conformity assessment and CE marking
 - Reporting of vulnerabilities and serious cybersecurity incidents
- Progressive application as from 10/12/2024 → 11/12/2027

Cybersecurity Act	Cyber Solidarity Act	Digital Operational Resilience Act (DORA)
<p>Certification framework for ICT in products, services & processes (ECCF)</p> <p>NEW: CSA2 Proposal:</p> <ul style="list-style-type: none"> published on 20 January 2026 Horizontal framework for ICT supply chain security Updating and expanding the existing ECCF 	<p>Detection, preparation and response to cybersecurity threats</p> <ul style="list-style-type: none"> Cybersecurity Alert System to share intelligence across EU Cyber Emergency Mechanism to improve incident response capabilities European Cybersecurity Incident Review Mechanism to analyse incidents & provide lessons learned 	<p>Withstand, respond to, and recover from ICT-related disruptions</p> <ul style="list-style-type: none"> Reinforced by technical standards, guidelines, FAQs and implementation rules → complex Who? EU financial sector (banks, insurance companies, investment firms)
As of 27 June 2019	As of 4 Feb. 2025	As of 17 Jan. 2025

Overview

- 01 EU Cyber Regulatory Landscape
- 02 **Cyber Preparedness / Crisis Management**
- 03 Conclusions

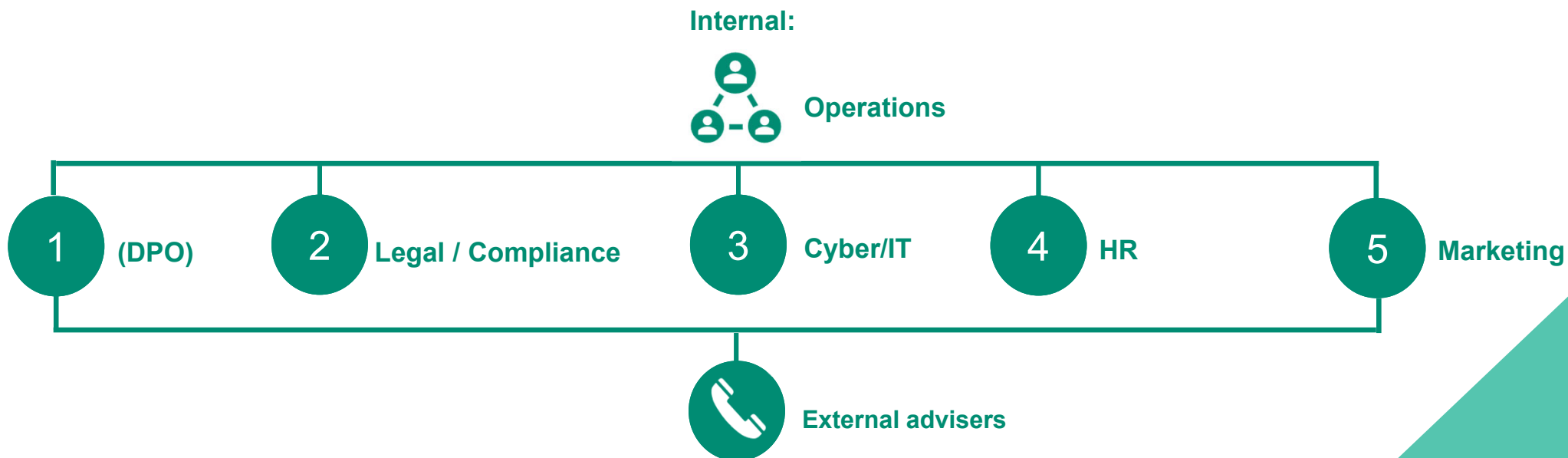
Senior Buy-In | Raising awareness

- Importance of having senior management (board) engaged
 - ➔ Allow budget: internal procedures, hiring (competences), security tools
- Spreading cyber aware culture = everyone's responsibility
- Training of personnel so they know *what* to do and *who* to contact
 - ➔ No blame culture
 - BUT** enforcement when deliberate

Governance – Competences (internal)

Set up of team with allocation of responsibilities

- Identify key internal stakeholders **early**, e.g.:



Governance – Competences (External)

- **Cyber insurance** - premium, coverage, etc.
- **Law firm** – ensure privilege, regulatory support, communication, etc.

+

- **Forensic agents** - restoration, segregation, root cause analysis (with evidence)
- **Document analyst** (e-discovery) - identify data (subjects) impacted + reporting
- **PR agent** – expert communication (with law firm's support)
- **Ransomware negotiators**

Governance – Procedures and documentation

- *Information Security Policy*
 - Responsibility allocation
 - Processes (e.g. document retention) and controls (e.g. supply chain)
 - Technical aspects (access rights, MFA, encryption, malware detection)
 - Resilience building (BCP/DRP)
 - Regulatory mapping (requirements, exposures - e.g. ransom payment)
 - Periodic vulnerability scanning (“pentest” and audit)
 - Etc.

Governance – Crisis management

- *Incident Response Plan*
 - Fact-finding and analysis
 - Triage and escalation
 - Teams involved and responsibilities
 - Containment, recovery and resilience
 - Internal and external communication (incl. press and social media)
 - Notification duties (relevant regulators – sectors and geographies)
- ➔ Need to protect and enable access (e.g. encryption, paper format)

Zoom in on communication

- Contractual reporting obligations (cyber insurer, customers, etc.)
- Notification to regulators and data subjects:
 - Assessment: low vs (high) risk
 - Geography: location of incident and of its impact
 - Sector: DPA + other regulators (e.g. BIPT, CCB)
 - Timeline is crucial
- Complaint filing (against “*John Doe*”) with police / prosecutor
- Other recipients may include personnel, shareholders, business partners, etc.
- To consider: press & social media (specific strategy)


Ransomware attack

- Blocked access / data loss / publication threat (e.g. on dark web)
 - ➔ back up assessment (recovery point objective “RPO”)
- Trust if you pay?
 - Some ransomware groups are known for ‘after sale service’ (!)
- Request advice from specialised ransomware negotiators
 - Communication / negotiations
 - Facilitate cryptocurrency payments
- Legal issue re. payment: possible legal offence (sanctions, AML)

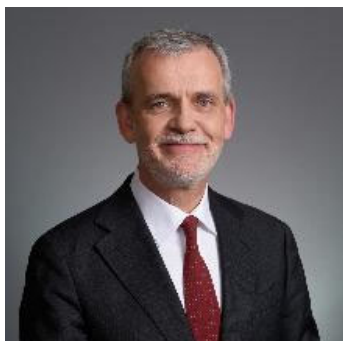
The Aftermath

- After-the-event investigation
 - Under privilege
 - Independently
 - Use of the output – lessons learned
- Prepare for litigation:
 - Supply chain issue towards suppliers / customers
 - Contractual failure (*force majeure?* – hardship)
 - Data subjects – collective redress (“*class action*”)

Conclusions

- Cybersecurity no longer optional → legal obligation across EU and beyond
 - Preparedness is essential - Be proactive, *not just* reactive
 - Governance is also crucial - need for structured coordination, documentation, crisis team (with internal and external competences)
 - Incident response to go fast and be compliant to reduce damage and liability
- 

Your speakers | 1



**Tanguy
Van Overstraeten**

Partner,
Head of DDC practice

T +32 2 27 90 49 00
M +32 478 40 15 69

tvanoverstraeten@vbb.com

Tanguy has over 30 years' experience advising national and international clients on a wide range of high-profile data protection/privacy, IT and cyber security matters (incl. the EU Digital Package: Data Act, AI Act, EHDS, etc.). He has extensive experience leading teams of lawyers and specialist consultants on complex national and international projects.

Tanguy has been a member of the EU Commission's Multistakeholder GDPR expert group since 2017. He has also been Data Protection Lead of the Digital Economy Committee of the American Chamber of Commerce to the EU for over a decade and is Emeritus Fellow of the International Association of Privacy Professionals (IAPP).

Tanguy was formerly a partner at a global law firm where he was Global Head of Data Protection and Brussels Head of TMT.



He truly thinks outside the box and consistently strives to find innovative solutions.

Client, Chambers Europe

Listed in the Hall of Fame for Privacy and Data Protection (Legal 500) & Band 1 for Data Protection (Chambers)

Your speakers | 2



Gert-Jan Fraeyman

Counsel

T +32 2 647 73 50

M +32 479 53 49 81

gfraeyman@vbb.com

Gert-Jan has a particular focus on data protection and information technology (including AI).

His areas of expertise include GDPR compliance, compliance with EU digital regulations including the AI Act, DORA, NIS2 and DSA, contracting (IT/outsourcing contracts, IP licensing agreements, data processing agreements, commercial contracts, etc.), intellectual property, e-commerce and market practices. In addition, Gert-Jan often represents clients in contentious matters before the courts.

He has particular experience in the financial services, energy, life sciences, retail and technology sectors.

The logo for VBB, consisting of the letters 'VBB' in a white, serif font, positioned in the upper right corner of a dark teal background. A large, light teal triangle is partially visible behind the logo.

VBB

Brussels

Glaverbel Building
Chaussée de La Hulpe 166
Terhulpesteenweg
B-1170 Brussels
Belgium
T: +32 (0)2 647 73 50

Geneva

26, boulevard des Philosophes
CH-1205 Geneva
Switzerland
T: +41 (0)22 320 90 20

London

Holborn Gate
330 High Holborn
London
WC1V 7QH
United Kingdom
T: +44 (0)20 7406 1471