



ACC ISRAEL CHAPTER · WEBINAR

Digital Regulation, Global Reach

The Role of the Privacy and Digital Governance Representative

In-House Counsel & Law Firm Attorneys · Prepared by Prighter



Digital Regulation, Global Reach

*The Role of the Privacy and
Digital Governance Representative*



Date: *Thursday 2 July*

Time: *11am IDT*



Assaf Gilad

Deputy General Counsel &
DPO at Lusha



Charlotte Mason

UK Head of Legal at Prighter



Andreas Matzler

CEO of Prighter
and Attorney at Law



Lital Nof-Sabbag

Director of Legal at Monday.com



Itamar Cohen

Partner at APM Law

What We'll Cover

From first principles to practical next steps



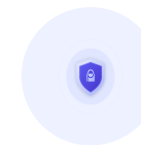
01

**Why the Representative Exists
Exists**



02

The Regulatory Landscape



03

**Risk & the Value of a
Representative**



04

Quality Criteria



05

Applicability by Industry



06

Panel Discussion & Q&A

SEGMENT 2

Why Does the Representative Exist?

Building the conceptual foundation before the rules.



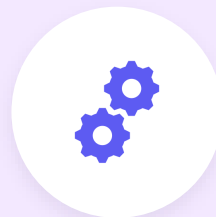
Protective Purpose...

The type of protection a law sets out to give shapes the representative's role



Individual-Protective

Grants rights to individuals allowing exercise of their rights and interest.



Systemic & Functional

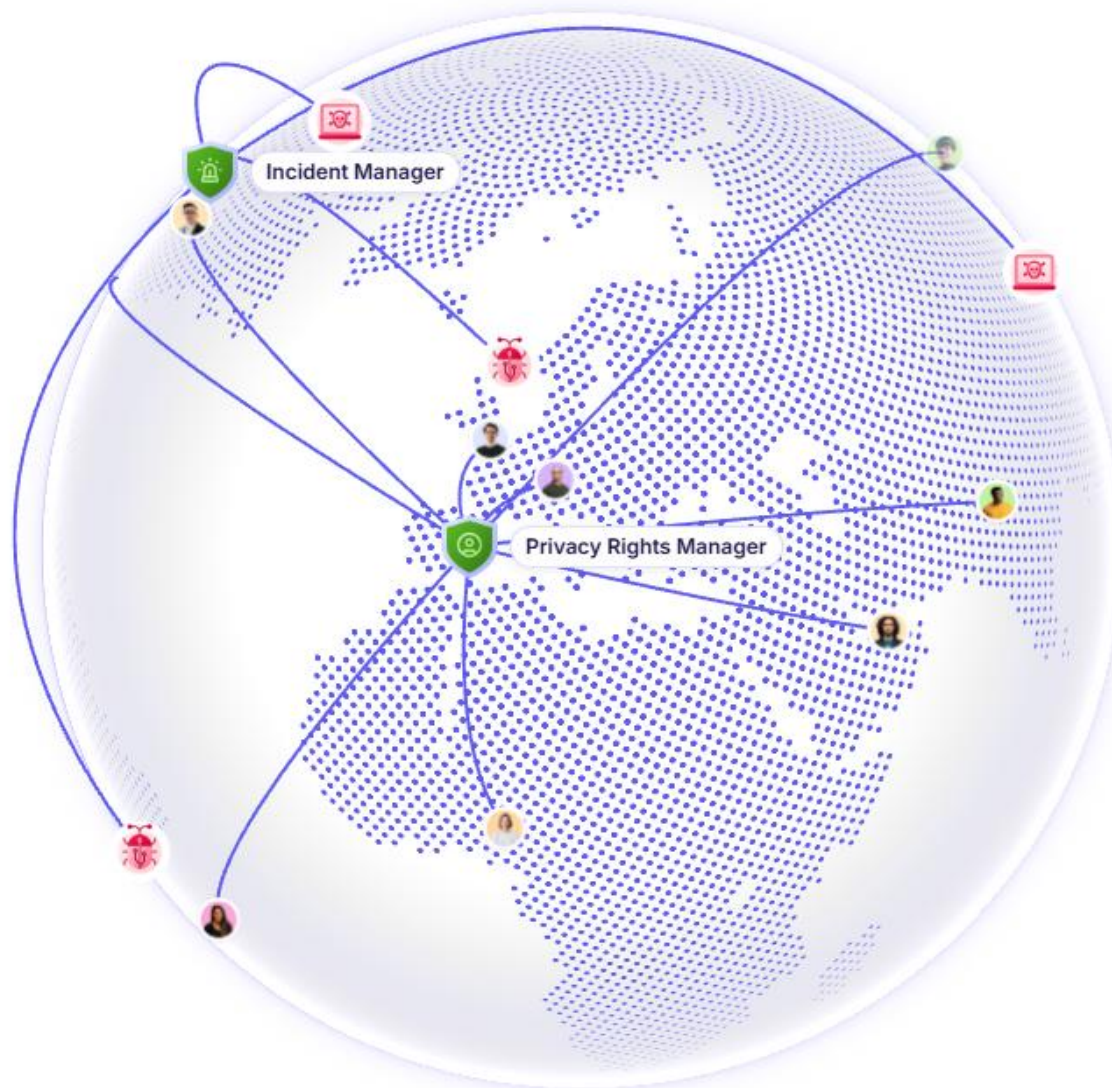
Protects the proper functioning of the market and critical assets.



Extraterritorial Scope

Digital economy is global by default

- The protective purpose requires extraterritorial scope of the regulations.
- Expansion of the scope alone does not create a functioning tie to the territory.



The link is the representative

- The representative is the hub linking overseas companies with the territory.
- The role of representative depends on what the law protects.

SEGMENT 3

The Landscape: Which Regulations?

This is not a GDPR-only story — the requirement spans 10+ frameworks.



Our Solution



Prighter delivers expertise, solutions, and products to support four core areas of compliance:

Privacy Representation



EU GDPR

UK GDPR

Swiss FADP

Turkey KVKK

China PIPL

Korean PIPA

Thai PDPA

Digital Governance Representation



EU NIS 2

UK NIS

EU DSA

EU Data Act

EU TCOR

EU DGA

EU CRA

EU e-Evidence

AI Governance Representation



GPAI Rep

AI Systems Rep

AI Literacy

AI Documentation

Compliance Software



PRM Manager

Incident Manager

DSA Transparency Report

Three Functional Roles

A representative may carry one, or several, depending on the law



Authority Contact

Compliance Role

Facilitating

Case handling with Authorities

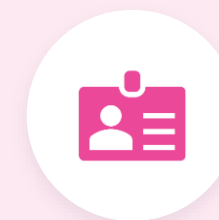


Individual Rights

Operational Role

Facilitating

Trust & Efficiency



Product / Market

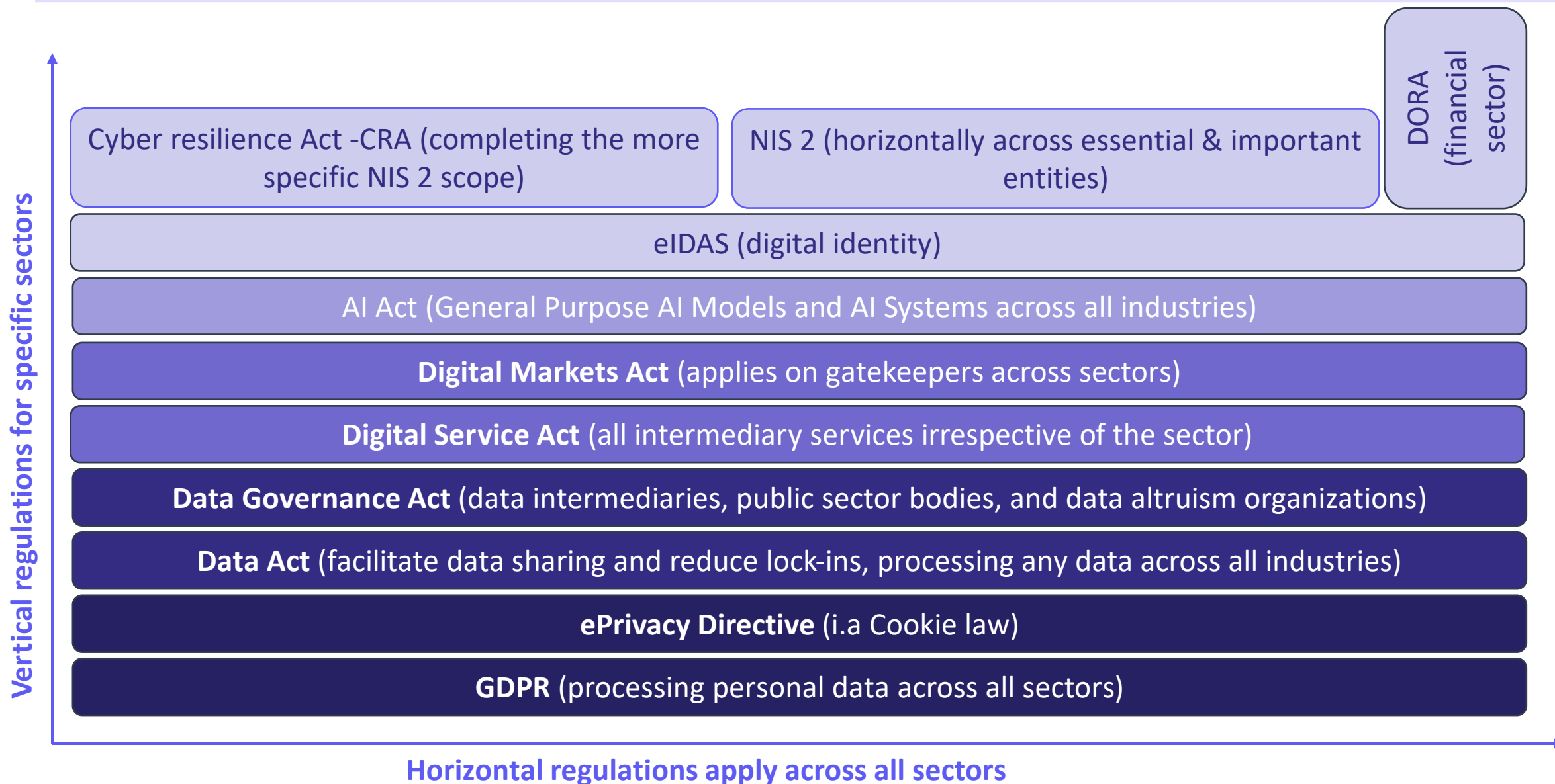
Specific Compliance

Facilitating

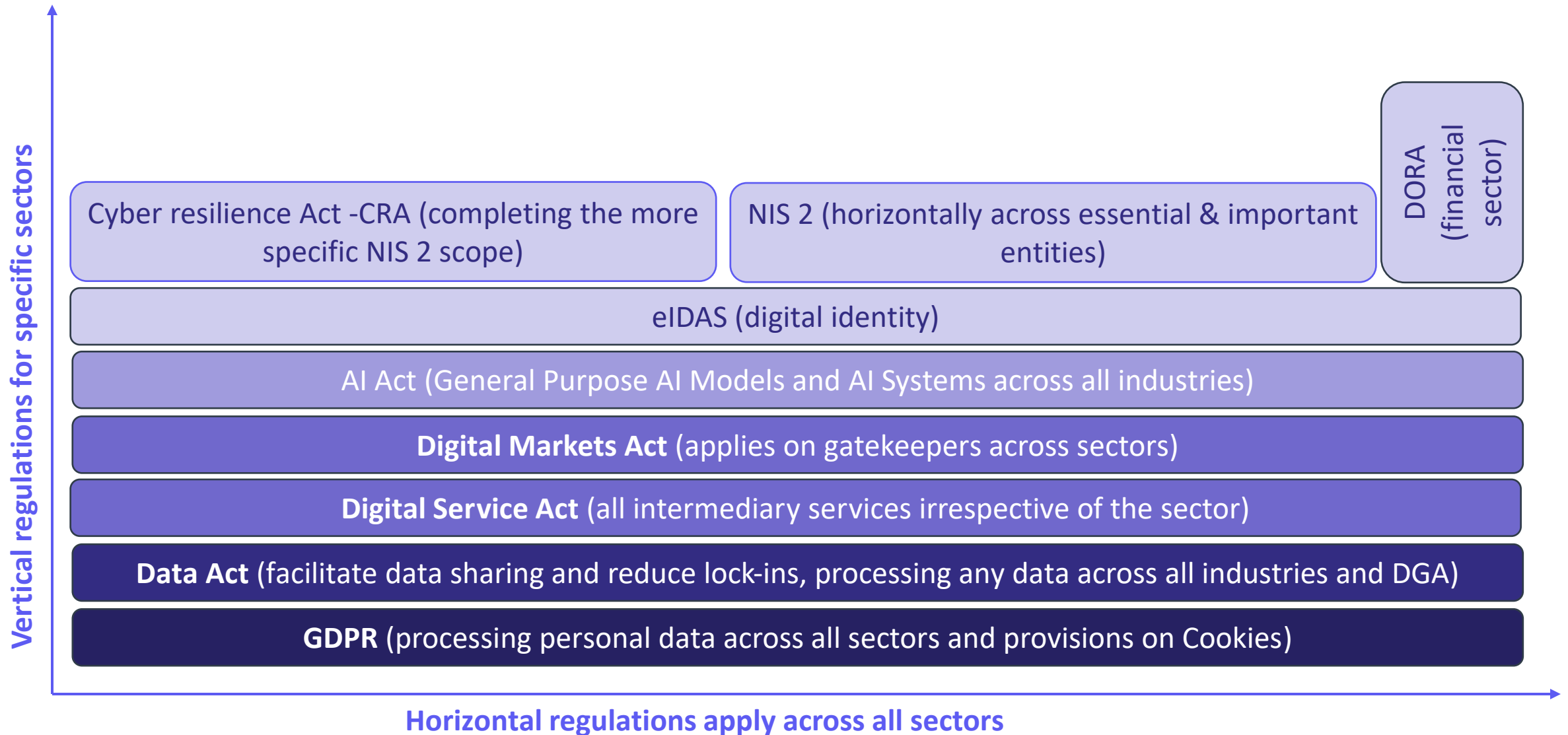
**Product Safety, Incident Reporting, ...
Reporting, ...**

Regulation	Jurisdiction	Protection	Rep Terminology	Main Focus	Specific
EU GDPR	EU	Individual	Representative	Data protection and privacy	Uncertain liability
UK GDPR	UK	Individual	Representative	Data protection and privacy	Amended version of the GDPR
Swiss FADP	Switzerland	Individual	Representative	Data protection and privacy	Effect doctrine
Türkiye KVKK	Turkey	Individual	Data Controller Rep	Data protection and privacy	VERBIS registration complicated appointment
Korean PIPA	Korea	Individual	Domestic Agent	Data protection and privacy	Very active authority
China PIPL	China	Both	Agency/Representative	Data protection and privacy	Implementing Regulation missing
EU Data Act	EU	Systemic	Legal Representative	Data sharing and IoT	Multiple Chapters with different scopes
EU NIS 2	EU	Systemic	Representative	Cybersecurity based on the type of entity	Directive with Member State transpositions
UK NIS	UK	Systemic	Representative	Cybersecurity based on the type of entity	Head office not in the UK
EU CRA	EU	Systemic	Authorised Representative	Cybersecurity based on the type of product	Not yet in force
EU AI Act (GPAI)	EU	Systemic	Authorised Representative	Safety of foundational models	Already in force – grace period ends August 2, 2026
EU AI Act (Systems)	EU	Both	Authorised Representative	Deployment of AI applications	Postponed by the Digital Omnibus
EU DSA	EU	Both	Legal Representative	Content moderation	Quality Requirements - uncertain liability
EU TCOR	EU	Systemic	Legal Representative	Law enforcement	Removal orders within 1 hour – uncertain liability
EU e-Evidence	EU	Systemic	Legal Representative	Law enforcement	Communication through the decentralised IT system

Regulatory Landscape



Regulatory Landscape



Data

Data (Use and Access) Act 2025

- Post-Brexit UK divergence from EU Regs
- UK specific changes to GDPR
- Includes:
 - **New right to complain** direct to controller, before ICO
 - **Wider rules** for automated decision-making
 - **Cookies relaxation** consent for specific purposes



Security

Cyber Security and Resilience (NIS) Bill

- **Expanded scope** – inc. relevant managed service providers and data centre operators
- **New 2-stage incident reporting:**
 - Initial notification 24hr
 - 72hr full report
- **Stronger sanctions** - fines up to £17m or 4% of turnover
- Expected to pass 2026 with phased roll out to 2028



SEGMENT 4

The Role & the Value of a Representative

Making the risk real, and the value concrete.





Four Pillars of Value

What a quality representative delivers



**Stakeholder
Shield**



**Commercial
Enabler**



**Operational
Effectiveness**



**Knowledge
Transfer**

Stakeholder Shield

Authorities:

Two-side communication hub (investigations/incident reporting) and case preparation/handling.

Users/Data Subjects:

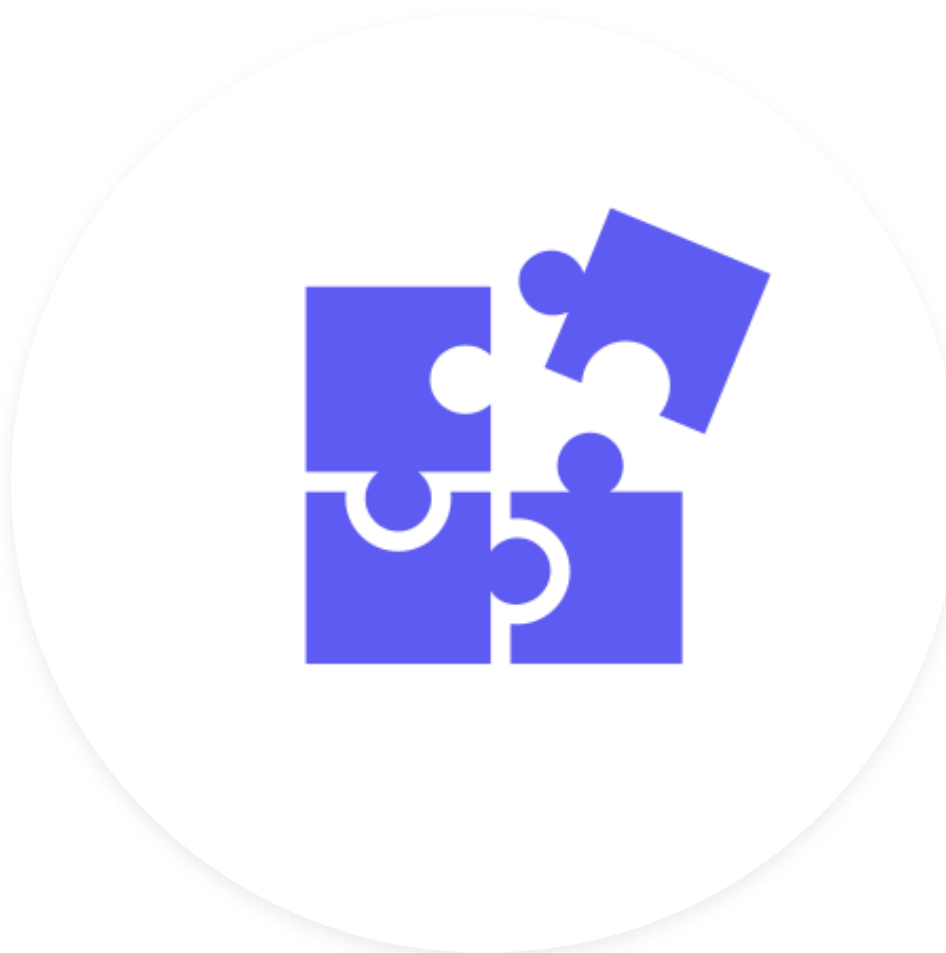
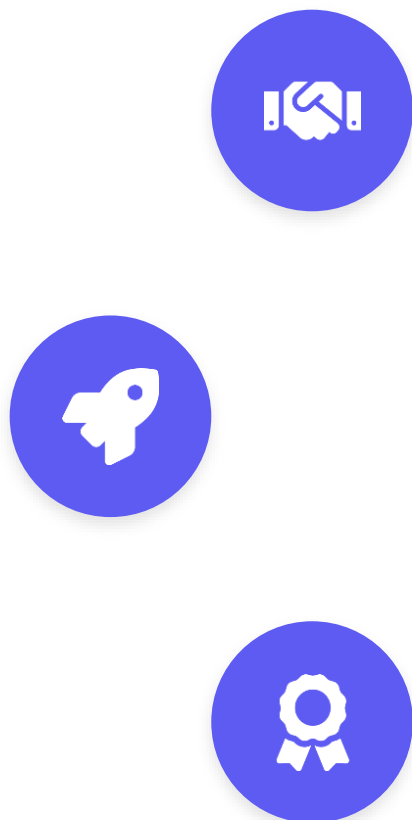
Point of contact and intake of requests.

Other Stakeholders

- B2B clients: DPA/SCC
- Trusted Flaggers
- ...



Commercial Enabler



Building Trust

Famous quote from UK court case. case.

Sales Enabler

Clears compliance roadblocks so so deals close faster and smoother. smoother.

Brand Reputation

A representative is your face in market – make it a good one.

Operational Effectiveness

Working Channels

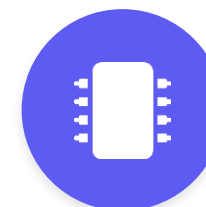
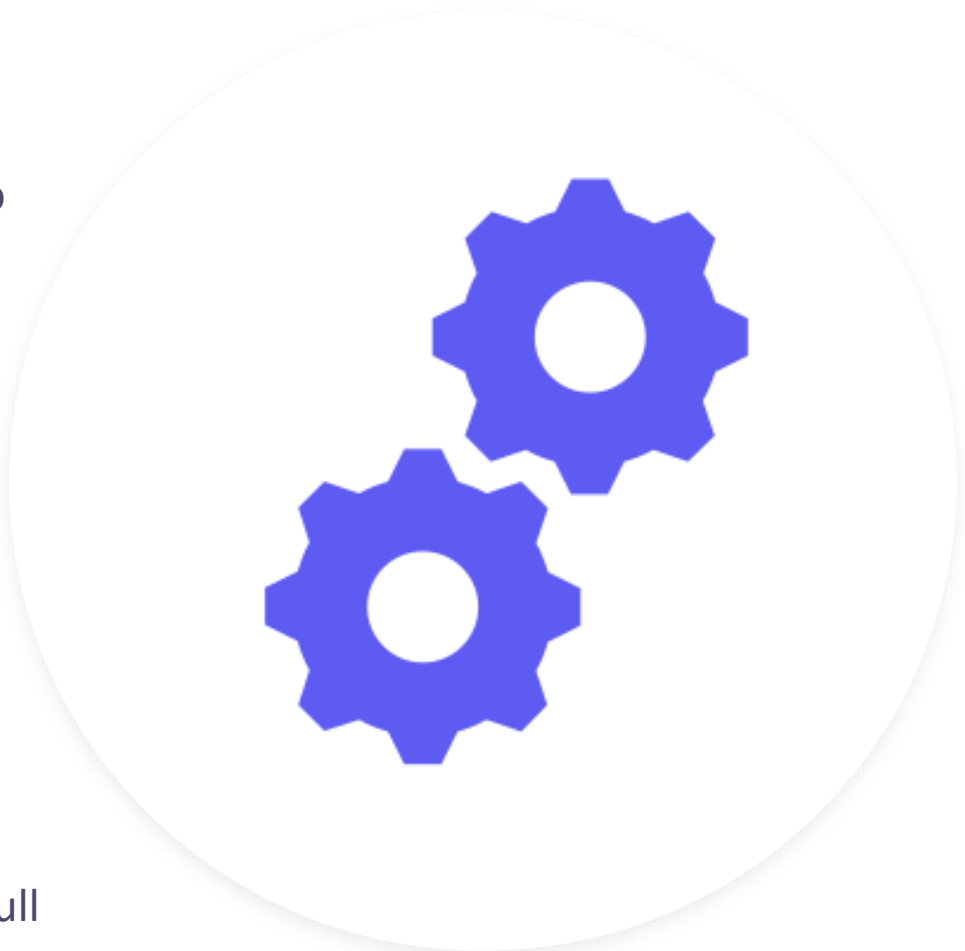
Direct communication channels to regulators and tested working relationships.

Proven Processes

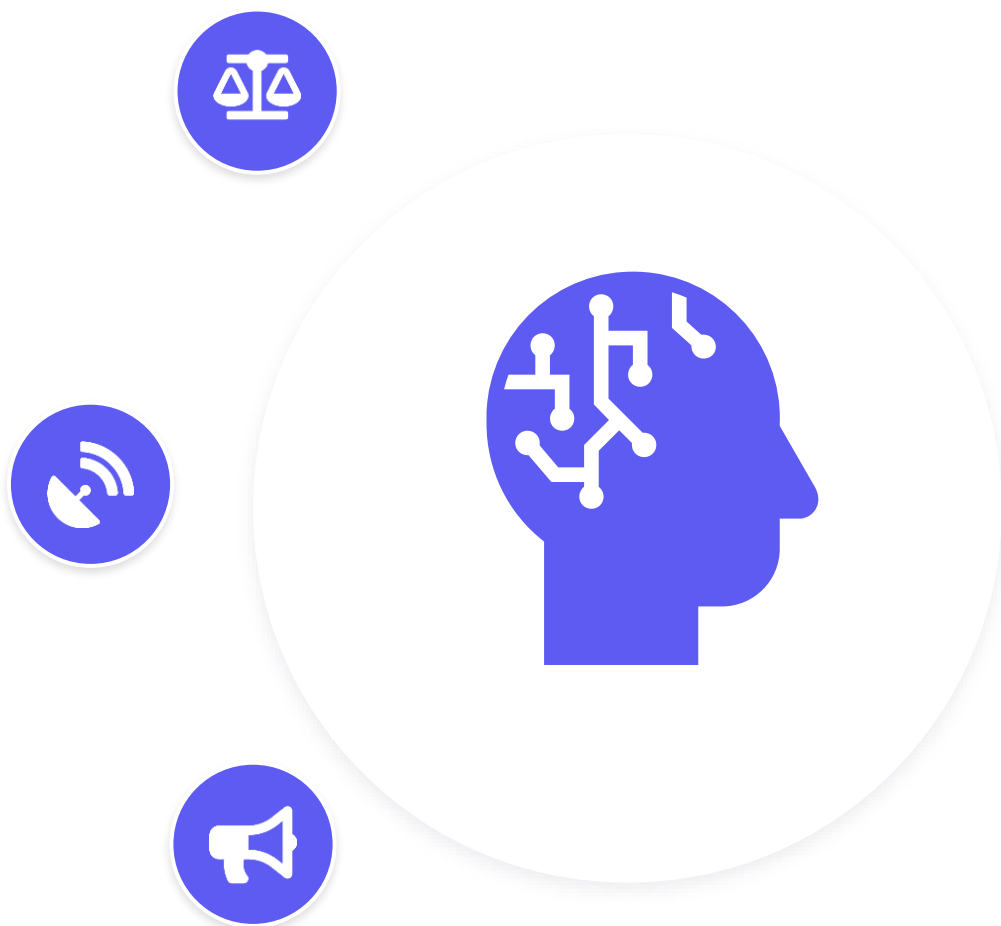
Structured, repeatable workflows deliver consistent handling in every jurisdiction.

Tech Augmented

A platform-backed process gives full visibility and a clear audit trail.



Knowledge transfer



Legal Knowledge at Scale

Insight drawn from 1,000+ cases handled across privacy, digital, and AI regulation.

Regulatory Monitoring

Continuous tracking of regulatory change across every market you operate in.

Amplifying Your Voice

Submissions to public consultations that help shape the rules before they land.

Without a Representative, Risk Escalates

Regulators have a broad toolkit before reaching fines



An unreachable company is not a free pass — absence of a representative is treated as an aggravating factor.

SEGMENT 5

Quality Criteria: What Makes a Good Representative?

A postbox is not a representative.



Quality Requirements When Appointing a Representative

What separates a genuine, trustworthy representative from a compliance risk



Genuine Local Presence

Registered entity with legal standing —
— not a mailbox



Expert, Multilingual Team

Local legal knowledge and language skills



Regulatory Relationships

A working track record with supervisory
authorities



Single Point of Contact

One relationship across every jurisdiction



Proactive, Not Reactive

Ahead of change with guidance and
webinars



Auditable Technology

End-to-end platform with full visibility



Stability & Longevity

A stable, ongoing business — not a
compliance risk



Partner Firm Network

Local coverage where there is no own
office

A trustworthy representative **meets every one of these criteria.**



SEGMENT 7

Panel Discussion & Q&A

Ask your questions.





Get in touch:

Dr Andreas Maetzler

CEO and Attorney at Law

Andreas.Maetzler@prighter.com

Charlotte Mason

Head of Legal and Regulatory

Charlotte.Mason@prighter.com

Operate Globally, Compliantly, and with Confidence.

Vision and Mission



Prighter helps global organisations navigate the fast-changing landscape of privacy, AI, and digital governance.

We combine proven legal expertise with innovative technology to simplify compliance and build trust across global markets.

Prighter was founded in response to the GDPR in 2018 and has since become a one-stop shop for global privacy, AI, and digital compliance, helping companies to navigate the changing regulatory landscape with confidence and ease.

Our Vision

To empower companies to operate globally, compliantly, and with integrity.

Our Mission

To make compliance with complex privacy, AI, and digital governance regulations accessible for global organisations and their stakeholders through innovative, trust-building solutions.

Privacy Representation Services



The GDPR is the EU's core data protection law, setting rules for how organisations handle personal data of individuals in the EU. Applies globally where EU residents' data is processed or monitored.



Who It Addresses

- Organisations offering goods or services to EU individuals
- Organisations monitoring EU user behaviour (e.g. cookies, profiling)
- **Extra-territorial scope:** Applies even without an EU presence.

Rep Requirements

- **Article 27** mandates a local **EU Representative** for non-EU entities.
- Acts as official contact for regulators and individuals
- Maintains records of processing (RoPA) and supports data subject requests.

Risks of Non-Compliance

- Fines up to **€20M or 4% of global turnover**.
- Enforcement actions, operational disruption, and reputation.
- **Examples:** Clearview AI (€20M) and Locatefamily.com (€525K) for failing to appoint a representative.

The UK's post-Brexit data protection framework, mirroring the EU GDPR but regulated by the UK Information Commissioner's Office (ICO). It governs how organisations process personal data of individuals in the UK.



Who It Addresses

- Any organisation handling data of UK residents
- Organisations offering goods or services to UK individuals
- Organisations monitoring behaviour of users located in the UK

Rep Requirements

- **Article 27 UK GDPR** requires non-UK organisations to appoint a **UK Representative**
- Serves as the local contact for the ICO and data subjects
- Manages communications, records, and compliance obligations on behalf of the controller or processor

Risks of Non-Compliance

- Fines up to **£17.5M or 4% of global annual turnover**
- Investigations and enforcement actions by the ICO
- Increased scrutiny for organisations serving UK users without representation

Switzerland's revised Federal Act on Data Protection (FADP) governs how personal data of individuals in Switzerland is collected, processed, and transferred. It aligns closely with the GDPR but includes distinct national obligations.



Who It Addresses

- Organisations processing data of individuals in Switzerland
- Foreign entities offering goods or services to Swiss residents or monitoring their behaviour
- Applies even if a company has a Swiss branch but no local headquarters

Rep Requirements

- **Article 14 FADP** requires some non-Swiss organisations to appoint a **Swiss Representative**.
- Acts as contact for the FDPIC
- Maintains compliance documentation and supports authority communication

Risks of Non-Compliance

- **Fines of up to CHF 250,000** for violations
- Reputational impact and potential suspension of data processing
- Authorities may restrict operations for repeated/serious breaches.

Türkiye KVKK

The Law on the Protection of Personal Data (KVKK) is Türkiye's primary privacy regulation, aligning with EU principles but tailored to local legal and administrative frameworks.



Who It Addresses

- Organisations processing personal data of individuals in Türkiye
- Foreign entities acting as data controllers, not merely processors
- Companies without a legal presence in Türkiye but engaging Turkish users

Rep Requirements

- Non-Turkish data controllers must appoint a **Data Controller Representative (DCR) in Türkiye.**
- DCR liaises with the Data Protection Authority
- Manages communications and ensures record maintenance

Risks of Non-Compliance

- Fines for non-compliance and failure to appoint a representative
- Enforcement actions and data-handling restrictions.
- Risk of reputational damage and loss of local market access

A One-Stop Shop for Global Privacy Compliance

Privacy regulations are evolving fast, and so is our coverage.

Prighter's representation services are expanding to meet the growing demand for global compliance.

Privacy Representative Services coming soon:



China (PIPL)

Support for companies handling data of Chinese residents, including representation and cross-border data transfer compliance.



Thailand (PDPA)

Local representation and guidance for organisations engaging with Thai data subjects or monitoring online activity in Thailand.



South Korea (PIPA)

Representation and advisory services to help companies align with Korea's Personal Information Protection Act and strengthen accountability in one of Asia's most advanced privacy regimes.



Digital Governance Representation Services



EU Digital Services Act

The DSA establishes accountability rules for online platforms, marketplaces, and intermediaries operating in the EU, aiming to create a safer and more transparent digital environment.



Who It Addresses

- Providers of intermediary services (e.g. hosting, cloud, platforms, marketplaces).
- Non-EU companies offering services accessible to EU users or targeting EU markets
- Applies to both B2C and B2B online environments.

Rep Requirements

- **Article 13 DSA** mandates non-EU providers to appoint an **EU Legal Representative**
- Acts as the official contact for authorities, trusted flaggers, and users
- Must have sufficient powers, expertise, and local presence to manage compliance duties

Risks of Non-Compliance

- Fines of up to **6% of global annual turnover**
- Investigations and service restrictions imposed by EU regulators
- Reputational damage arising from enforcement

EU Data Act

The EU Data Act sets out rules for fair access to and sharing of data generated by connected products and related services. It expands data rights beyond personal data to promote transparency and innovation.



Who It Addresses

- Manufacturers, service providers, and users of connected devices
- Non-EU organisations making products or digital services available to EU users
- Data holders required to grant access to users, third parties, or public bodies.

Rep Requirements

- **Article 37(11)** requires non-EU entities to appoint an **EU Legal Representative**.
- Serves as the local contact for competent authorities.
- Ensures cooperation, documentation, and ongoing compliance under the Act.

Risks of Non-Compliance

- Regulatory investigations and potential fines
- Restrictions on data-sharing activities within the EU
- Loss of trust due to non-compliance

EU NIS 2 Directive

The NIS2 Directive strengthens cybersecurity and resilience across essential and digital service sectors in the EU.

It broadens the original NIS scope and introduces stricter security and reporting obligations.



Who It Addresses

- Essential and important entities in sectors such as energy, transport, banking, digital infrastructure, and ICT services
- Non-EU organisations providing digital or network services impacting EU users
- Applies across both public and private operators

Rep Requirements

- **Article 26(3)** requires non-EU entities to appoint an **EU Representative**.
- Acts as the local contact for authorities and CSIRTs.
- Manages incident reporting, compliance communication, and oversight activities.

Risks of Non-Compliance

- **Essential entities:** Fines up to €10M or 2% of global turnover
- **Important entities:** Fines up to €7M or 1.4% for important entities
- Possible operational restrictions and reputational harm

UK NIS Regulations

The UK Network and Information Systems (NIS) Regulations 2018 enhance the security and resilience of critical infrastructure and digital services operating within the UK.



Who It Addresses

- **Operators of Essential Services (OES):** sectors such as energy, transport, health, water, and digital infrastructure
- **Digital Service Providers (DSPs):** including online marketplaces, cloud providers, and search engines.
- Applies to non-UK DSPs offering services to UK users

Rep Requirements

- **Article 14A** requires non-UK DSPs to appoint a **UK NIS Representative**.
- Acts as local contact for authorities (ICO and NCSC).
- Handles incident notifications, investigations, and compliance correspondence.

Risks of Non-Compliance

- **Fines up to £17 million** depending on severity and negligence
- Regulatory investigations and potential service restrictions
- Loss of trust and market access for non-compliant providers

AI Governance Representation Services



The EU AI Act is the world's first comprehensive regulation on AI. It recognises two types of AI providers:

- **General-Purpose AI models (GPAI):** Foundational models like large language models
- **AI Systems:** Applications built on GPAI models, such as chatbots, assistants, or analytics tools.

The AI Act has **extra-territorial reach**, so if a providers' outputs are used in the EU, the Act applies, regardless of where they are based.

What are the penalties for non-compliance?

- Up to €35m or 7% global turnover for prohibited practices or data requirements
- Up to €15m or 3% for other obligations, incl. GPAI model rules
- Up to €7.5m or 1.5% for misleading or incomplete information

SMEs face the lower threshold, larger companies the higher one.



General-Purpose AI (GPAI) Representation

Prighter's Authorised Representative Services ensure that you to comply with the law, maintain required documentation, and ensure cooperation with market surveillance authorities.

Prighter delivers:

- **A legally established representation in the EU**
- **An official contact point** and cooperates with competent authorities and provides all required information or documentation.
- **Prompt notifications of any requests** from market surveillance authorities.
- **Support for post-market obligations**, including Article 26 reporting and Article 61 cooperation duties.

Our Authorised Representative Services give you the peace of mind that your business is compliant, so that you can focus on what you do best.

