Compliance & Risks

RINA

Product Safety in the Digital Age: Understanding New Cybersecurity Rules

Author:
Ashley Weeks, Senior Regulatory Compliance Consultant,
RINA Tech UK Ltd

9th September, 2025

Further regulatory developments may have occurred after publication. To keep up-to-date with the latest compliance news, sign up to our newsletter.

Table of Contents

Product Safety in the Digital Age: **Understanding New Cybersecurity Rules**

01. Introduction
02. The Escalating Threat of Cyber Attacks
03. The UK Product Security and Telecommunications Infrastructure (PSTI) Act
04. The EU Cyber Resilience Act (CRA)
05. The Radio Equipment Directive (RED) Delegated Regulation
06. The Overlap with Data Protection Laws
07. Vulnerability Disclosure: A Mandated Practice
08. Webinar Q&A
09. Conclusion

01. About The Author

Ashley Weeks, Senior Regulatory Compliance Consultant, RINA Tech UK Ltd

Ashley is a Senior Regulatory Consultant at RINA with a strong technical background in industry product legislation. He has expertise in CE Marking Directives/Regulations and UK equivalents such as EMCD, LVD, RED, Machinery and many others.

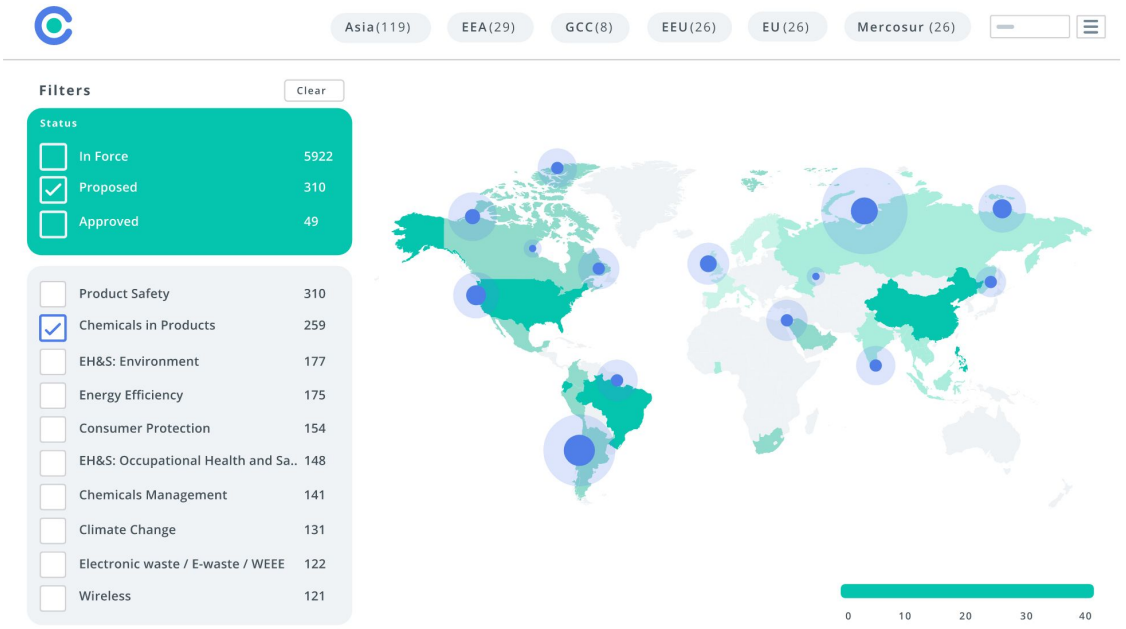
Ashley provides advice to economic operators including manufacturers, importers and distributors to help them understand their specific product legislation requirements related to their products.

He also has co-operation with government departments such as the department for Business and Trade, communicating feedback from many SMEs to allow the relevant departments to ensure any updates to legislation are communicated in the clearest way possible.

Prior to joining RINA, Ashley also has years of experience in the EMC (Electromagnetic Compatibility) world, originally working as a test engineer in different industries such as Military/Aerospace, Automotive & Commercial.

Unlocking Market Access

Compliance & Risks empowers global enterprises to unlock market access and confidently navigate regulatory complexity. With a 20-year legacy in regulatory intelligence, we help beloved global brands manage product and corporate sustainability obligations, transforming compliance into a force multiplier for enterprise growth.



Our solution includes:

- **C2P:** The most advanced product compliance and corporate sustainability software on the market, helping you streamline your compliance process and unlock market access around the world.
- **Regulatory Content:** We provide the broadest and most comprehensive product compliance regulatory content on the market, monitoring 195+ countries, 20 industry sectors, 45 topics and 100,000+ regulatory sources.
- **Ask our Experts:** Direct access to our team of experts for support
- **C&R Sustainability:** Our new platform doesn't just track regulatory change; it generates intelligence next steps, tailored to your business. It's not just a dashboard. It's your ESG compliance brain: AI-native, human-verified, globally aware and ready with answers. Try a free trial **here**.

Why choose C2P?

- ✓ **Stay ahead** of regulatory changes with the world's most comprehensive regulatory database
- ✓ **Avoid delays** with alerts of changes to regulations & requirements in real time
- ✓ **Improve efficiency with powerful collaboration and workflow tools** to keep compliance evidence up-to-date & live linked back to Regulations, Standards & Requirements

Contact us to speak to one of our team today to learn how you can simplify your regulatory compliance process.

01. Introduction

In an increasingly connected world, where the number of IoT devices is expected to double by the end of the decade, the threats from cyber attacks are escalating.

This rise is accelerated by geopolitical conflicts that aim to destabilize digital infrastructures, exposing essential data and services to serious risks.

This guide, based on the webinar "**New Rules, New Risks: Latest Cybersecurity & Data Protection Impacts on Product Compliance**," provides a comprehensive overview of the latest cybersecurity and data protection legislation impacting product compliance in the UK and Europe.

It outlines the key regulatory changes, their implications for manufacturers, importers, and distributors, and how these new rules align with existing data protection principles.

Watch the **full webinar** for more details.

This guide serves as an essential companion for anyone seeking to understand this evolving legal landscape.

It will cover a number of key topics, including a deep dive into the UK Product Security and Telecommunications Infrastructure (PSTI) Act, which came into effect in April 2024 to provide a baseline for IoT device security.

You will learn about the definitions of "internet-connectable" and "network-connectable" products and the three mandatory security requirements.

The guide will also explore the EU Cyber Resilience Act (CRA), which entered into force in November 2024 and aims to make products with digital components secure throughout their entire life cycle and supply chain.

It details the risk-based classification system and the corresponding conformity assessment procedures. In addition, the guide examines the Radio Equipment Directive (RED) Delegated Regulation 2022/30/EU, which entered into force on August 1, 2025, and adds mandatory cybersecurity measures to radio equipment.

Finally, it will discuss how these new cybersecurity requirements increasingly align with core data protection principles like integrity, confidentiality, and accountability.

02. The Escalating Threat of Cyber Attacks

The digital landscape is facing a rapid increase in cyberattacks, with a **23% rise in global attacks** during the first half of 2024 alone.

This translates to an average of nine serious incidents per day, reaching a total of **1,637 attacks globally in the first six months of the year.**

The **Americas and Europe are the primary targets, accounting for 41% and 29% of all serious attacks**, respectively. This escalation is often fueled by geopolitical conflicts, which aim to destabilize digital infrastructures and expose critical data and services to severe risks.

While the manufacturing sector has been the most affected, the healthcare sector is rapidly catching up, experiencing an **83% increase in attacks since 2023**.

These attacks often exploit **human error**, which is estimated to be the **cause of 95% of cyberattacks**.

Common errors include using weak passwords and opening malicious email attachments. A significant concern is the lack of security support for IoT devices.

One survey found that manufacturers often stop providing security support after just two years, despite the products having a much longer lifespan.

These vulnerabilities can be easily exploited, as demonstrated by the 2016 Distributed Denial of Service (DDoS) attack that used thousands of compromised internet-connected products to disrupt services from major news and media organizations like the BBC and Netflix.

This highlights the urgent need for robust, mandatory legislation to ensure products are secure from the outset.

03. The UK PSTI Act

The UK has taken a proactive stance on cybersecurity with the Product Security and Telecommunications Infrastructure (PSTI) Act, which came into effect on April 29, 2024.

This act provides a baseline of security requirements for internet of things (IoT) devices sold to UK consumers.

It defines two categories of products that fall within its scope: "internet-connectable products" and "network-connectable products." Internet-connectable products are those capable of sending and receiving data over the internet using standard protocols like TCP/IP via Wi-Fi, Ethernet, or cellular networks. Network-connectable products, on the other hand, do not connect directly to the internet but can connect to other internet-connected devices, either directly or as part of a local network.

This second definition is crucial as it captures devices that might serve as a "backdoor" into a network, ensuring local-only gadgets also meet minimum security standards.

To comply with the PSTI Act, manufacturers must meet three minimum security requirements.

- First, they must ban universal default and easily guessable passwords, requiring unique passwords for each product.
- Second, manufacturers must publish information on how to report security issues, providing a free point of contact to manage vulnerability reports and offer status updates until a resolution is reached.
- Finally, they are required to publish information about the minimum security update periods for their products.

A key takeaway for manufacturers, importers, and distributors is that a Statement of Compliance must accompany the product, as per Schedule 4 of the PSTI regulations.

It is important to note that unlike some other regulations, the PSTI Act does not require a UKCA label to be affixed to the product.

04. The EU Cyber Resilience Act (CRA)

The EU Cyber Resilience Act (CRA) was published in the official journal on November 20, 2024, with its primary aim being to strengthen the security of products with digital components throughout their entire lifecycle and supply chain

The CRA has a broad scope, applying to "Products with Digital Elements (PDEs)" that have a direct or indirect logical or physical data connection to a device or network. This covers not only end-user devices such as laptops and mobile apps, but also individual components like CPUs, firmware modules, microcontrollers, network interface cards, and embedded libraries.

The CRA classifies products into three tiers - Non-Critical, Important, and Critical - which determine the conformity assessment procedure.

For most consumer products, falling into the **Non-Critical** category, manufacturers can use a self-assessment to demonstrate compliance.

Important products, such as those with VPN functions or password managers, have more stringent requirements and may still use a self-assessment if a harmonized standard is applied in full.

The most demanding category is Critical, encompassing products such as hardware security modules and smart meter gateways.

If a European Common Criteria (EUCC) certification scheme has been established, these products must undergo a third-party conformity assessment and obtain EUCC certification; if no such scheme exists, they should instead follow the conformity assessment route via a notified body.

The CRA also sets out essential requirements, including performing risk assessments, ensuring products are made available without known vulnerabilities, and implementing a coordinated vulnerability disclosure policy.

The act provides a more generous timeline for compliance compared to the UK PSTI, with the main obligations taking effect in December 2027.

The exception is the CRA's vulnerability-reporting requirements, which kick in on 11 September 2026, and that includes publishing a public point of contact for vulnerability disclosures by that date.

To comply, you will need to provide a public vulnerability-disclosure channel and report actively exploited vulnerabilities and severe security incidents without undue delay. This can be done on the ENISA reporting platform.

It also sets significant administrative fines, starting from €5 million for infringements.

05. The Radio Equipment Directive (RED) Delegated Regulation

The RED Delegated Regulation 2022/30/EU, which came into force on August 1, 2025, adds mandatory cybersecurity measures to the existing Radio Equipment Directive (RED).

It retains the same scope and conformity procedures as the original directive but introduces three new essential requirements under Article 3.

These requirements mandate that radio equipment must:

- not harm the network, its functioning, or misuse its resources (Article 3.3(d));
- incorporate safeguards to protect the personal data and privacy of users (Article 3.3(e)); and
- support features to protect against fraud (Article 3.3(f)).

It is important to understand that not all products in the scope of the original RED are subject to these new cybersecurity rules.

The new requirements only apply to radio equipment with the capability to connect to the internet or process personal data.

For example, an LTE module with internet connectivity would be subject to the new rules, while a simple RF garage door opener that does not connect to the internet would not.
To demonstrate compliance, manufacturers can use the harmonized EN 18031 series of standards. However, there are restrictions; for instance, devices that ship with blank or unchangeable default passwords will lose the presumption of conformity and must undergo a full Notified Body assessment.

Similarly, for certain child-oriented devices, specific parental controls are required to retain presumption of conformity.

06. The Overlap with Data Protection Laws

Cybersecurity legislation and data protection laws share a common goal: to protect individuals' personal data and ensure privacy in an increasingly interconnected world.

While they are distinct, they are also deeply intertwined. Cybersecurity laws, such as the PSTI and CRA, require secure product design to prevent unauthorized access and data breaches. This directly supports data protection principles outlined in laws like the GDPR and UK GDPR, which demand the lawful handling and security of personal data. Compliance with cybersecurity standards thus helps meet key data protection principles like integrity, confidentiality, and accountability.

The EU Cyber Resilience Act, for instance, directly references data protection in its essential requirements by mandating the protection of personal data confidentiality and integrity.

It also aligns with GDPR principles such as data minimization. The RED Delegated Regulation directly links cybersecurity to personal data processing by requiring radio equipment to incorporate safeguards for user privacy.

Even the UK PSTI, which does not explicitly mention data protection, indirectly supports it by mandating "secure by design" principles, which mirror the GDPR "privacy by design" rule.

By building products with these security principles in mind, manufacturers are effectively ticking off key GDPR requirements, reducing the risk of data breaches and subsequent enforcement actions.

07. Vulnerability Disclosure: A Mandated Practice

One of the key themes that has emerged across both UK and EU cybersecurity legislation is the requirement for a Vulnerability Disclosure Policy (VDP).

A VDP is defined as a process for identifying, reporting, and patching weaknesses in software, hardware, or services that could be exploited.

The best practice for this is called Coordinated Vulnerability Disclosure (CVD), which is mandated by the EU Cyber Resilience Act. This process involves a researcher contacting a company with a vulnerability report, the company acknowledging it within 24 to 48 hours, and then working to address the issue, typically within 30 to 90 days.

Despite being considered an industry best practice and standardized for years, a 2024 report by the IoT Security Foundation found that over **64% of companies surveyed did not have a way for security researchers to contact them.** While this is a significant negative, there is a positive upward trend in VDP adoption, particularly in regions like the UK, Europe, and the USA, where legislation is being introduced.

This suggests that mandatory legislation is effectively driving greater compliance. However, with the UK PSTI Act now in force, a large number of non-compliant products may still be on the market.

08. Webinar Q&A

During the live webinar, numerous questions were sent in by our live audience. Our webinar presenter, **Ashley Weeks, from RINA,** provided expert answers to the most popular queries below.

Q1. Are storage equipment covered within the Cyber Resilience Act?

Storage devices such as HDDs, SSDs, storage arrays, NAS and SAN appliances, all of which contain firmware or embedded controllers and connect via USB, Ethernet or Fibre Channel, qualify as "products with digital elements" and are therefore regulated under Article 2(1)

Q2. Regarding CRA, will there be any DoC update required in Sep 2026 (regarding Vulnerability handling requirements)?

No. While vulnerability-reporting obligations under the CRA become applicable on 11 September 2026, there is no standalone requirement to revise your Declaration of Conformity (DoC) on that date. The formal DoC (accompanying the CE mark) only becomes mandatory from 11 December 2027.

Q3. How should a manufacturer handle vulnerability disclosure for products with only proprietary code? Are they only required to focus on vulnerabilities related to third-party components?

Even if your product consists solely of proprietary code, the Cyber Resilience Act's vulnerability-handling requirements apply in full. You cannot limit your focus only to third-party or open-source components.

Q4. Which access control system components, such as readers, that do not directly connect to a network but instead connect to a controller with a LAN connection, fall under the new regulations?

Access control readers that don't plug straight into your LAN, yet feed into a controller with a network link, still count as "products with digital elements" under Article 2(1). Because they embed firmware or microcontrollers and enable data exchange (even indirectly), they fall within the CRA's scope.

Q5. How can we ensure the cybersecurity compliance of spare parts?

Any spare part containing its own firmware, microcontroller or update mechanism that, directly or indirectly (for example via a controller), interfaces with a LAN or wider network is subject to CRA requirements.

However, spare parts manufactured as exact technical replicas of the original, without any added or modified embedded logic, remain outside the Act's scope.

Any spare part that's in scope must meet the same CRA requirements (secure-by-design, vulnerability handling, updates, CE marking, etc.) as any other product with digital elements.

Q6. Do bluetooth speakers that can only connect to one phone at a time, and not the internet, fall under cyber security regulations?

EU CRA: Bluetooth speakers embedding firmware that pair directly with a phone qualify as "products with digital elements" under the Cyber Resilience Act and must meet its cybersecurity requirements.

UK PSTI: Even if they only use Bluetooth, speakers that can connect to a phone (which itself is internet-connectable) fall within the "network connectable product" definition and are in scope.

Q7. Are TWS speakers or earphones under the scope of Network connectable products?

Under the UK PSTI regime, true-wireless (TWS) earbuds and speakers that pair via Bluetooth with an internet-capable device qualify as "network-connectable products."

True-wireless earbuds or speakers that pair via Bluetooth are only out of scope if the sole device they ever connect to truly cannot access any network.

In practice that means they'd need to pair exclusively with an offline audio transmitter or "dumb" handset that has no Wi-Fi, cellular or other network link, otherwise, as long as their master device can go online, the TWS kit sits on a potential network path and falls within scope.

Q8. CRA: Could you give us the essential obligations for manufacturers from 11 sept. 2026?

The CRA's vulnerability-reporting requirements kick in on 11 September 2026, and that includes publishing a public point of contact for vulnerability disclosures by that date.

To comply, you will need to provide a public vulnerability-disclosure channel and report actively exploited vulnerabilities and severe security incidents without undue delay. This can be done on the ENISA reporting platform.

Q9. Are CRA requirements replacing the cybersecurity of the EU RED?

Yes. From December 2027 the CRA will take over all of RED's cybersecurity requirements.

RED will still apply for non-cyber rules (like spectrum and safety), but its cyber clauses move into the CRA.

Q10. Do you have a view of certain IEC standards that already ask cybersecurity obligations?

- IEC 62443 series: industrial automation/control system security
- IEC 62351 series: power-grid protocol protection
- IEC 62443-2-4: secure processes for IACS service providers
- IEC 62443-4-1: secure-by-design requirements for IACS products
- ISO/IEC 27001: risk-based information security management system

Non IEC standards of note

- ETSI EN 303 645: baseline cybersecurity for consumer IoT devices
- ETSI TS 103 645: technical specification underpinning EN 303 64
- US NIST Cybersecurity Framework (CSF): voluntary, risk-based guide around Identify, Protect, Detect, Respond, Recover

Q11. Do you have some elements about the Cybersecurity Act in Australia especially on involved products?

The Australia Cyber Security Acts mandatory security requirements for "relevant connectable products" (consumer IoT and smart-home devices) will apply by 29 November 2025.

It's aimed squarely at manufacturers of internet- or network-enabled consumer gadgets, obliging them to enforce unique credentials, publish vulnerability-disclosure processes, and declare update-support periods.

In principle it mirrors the UK's PSTI regime.

Q12. How does ETSI EN 303 and ISO 27001 fit in with RED delegated Act and CRA? Would they be sufficient to demonstrate compliance?

ETSI EN 303 645 serves as the harmonised standard under the RED Delegated Regulation 2022/30 - albeit scoped to consumer IoT with wireless connectivity - granting legal conformity presumption for RED's cyber security clauses. Under the EU Cyber Resilience Act, formal standardisation requests have now been issued, so EN 303 645 and its methodologies will feed into CRA harmonised standards; however, given CRA's broader remit across all digital products, EN 303 645 alignment is likely to apply primarily to internet-connected radio-equipment categories.

ISO 27001 isn't a harmonised product standard like ETSI EN 303 645 under RED, but you can use the same principle of re-using an existing framework to satisfy CRA requirements, albeit at the organizational-management level rather than for individual devices.

Q13. If you had a bluetooth device such as ear buds that can only connect to one device and not multiple at the same time, would these be out of scope of PTSI?

Under the UK PSTI regime, bluetooth earbuds and speakers that pair via Bluetooth with an internet-capable device qualify as "network-connectable products."

Earphones that pair via Bluetooth are only out of scope if the sole device they ever connect to truly cannot access any network. In practice that means they'd need to pair exclusively with an offline audio transmitter or "dumb" handset that has no Wi-Fi, cellular or other network link, otherwise, as long as their master device can go online, there is a potential network path and falls within scope.

Q14. For the PSTI - it came into effect in 2024 but is there a date where you must have applied the regulation?

The UK PSTI regime came into force on 29 April 2024, and from that date any "relevant connectable product" placed on the UK market must comply with its security requirements and be accompanied by a Statement of Compliance.

There is no extended grace period - if you supply new consumer-connectable devices on or after 29 April 2024, you must already have applied the PSTI rules.

Q15. Desktop PCs without cellular connectivity are exempt from UK PSTI - what about those with WI-FI or Ethernet? Do the rules not apply?

This exemption applies regardless of whether they have Wi-Fi or Ethernet ports: as long as they cannot natively attach to a mobile/cellular network, they fall outside the “relevant connectable product” scope.

One caveat: devices designed exclusively for children under 14 lose this exemption, even if they’re purely Wi-Fi/Ethernet-only.

Q16. I missed the EU-Data-Act dealing with IoT-Data and coming September 2025?

The EU Data Act and the Cyber Resilience Act both apply to the same set of connected products - while the Data Act grants users the right to access, share, and port IoT-generated data, the CRA ensures that those very data-sharing interfaces and processes are built on secure-by-design cybersecurity foundations, creating an overlapping regime where interoperability and data portability rest upon mandatory resilience and protection measures.

Q17. If a product is supplied in both UK and EU, and is CRA compliant, does that mean the CRA compliance overrides the PSTI, or does the product need to comply to both?

The EU Cyber Resilience Act imposes a higher technical bar, with risk-based classification, tighter vulnerability-response deadlines and a CE-marked Declaration of Conformity on a phased timeline, whereas the UK PSTI applies the same core security measures earlier (from April 2024) via a self-declaration (UKCA marking).

Consequently, a CRA-compliant product will technically cover PSTI’s requirements, but you must still meet each regime’s separate deadlines and paperwork.

Q18. Is statistical data generated by a product, classed as private protected data if it doesn't include private data like names addresses etc?

Statistical data that contains no information about an identifiable person (no user IDs, no device serial numbers tied to a user, no timestamps or geo-coordinates that could single out someone) is generally treated as anonymized data and not “private protected data” under GDPR or the UK Data Protection Act.

Only if those stats can be linked (directly or indirectly) to an individual would they become personal data and thus fall under the usual privacy-protection rules.

Q19. Based on the EU Cyber Resilience Act (CRA) classification, do non-consumer products, such as industrial machinery, fall under the 'default' (non-critical) Products with Digital Elements (PDEs)?

Agreed, most B2B or industrial equipment outside those two high-risk buckets falls into the default PDE category and only has to meet the Act’s baseline security requirements. Standard IoT Devices were just an example of what we would not deem to class as important or critical (which for now, have a very specific lists.)

Q20. Is it correct that the EU Cyber Resilience Act (CRA) does not exclusively aim to protect personal data, but also networks and information systems, even when there are no personal data risks?

You're right that the CRA's mandate extends well beyond personal data.

It sets cybersecurity requirements for all digital products to keep networks and systems resilient. That said, one of its core pillars is confidentiality, which inevitably includes personal data.

In practice, measures like secure-by-design, vulnerability management, and mandatory updates not only shore up network integrity but also reinforce the GDPR's confidentiality and integrity requirements for personal data.

Q21. Does the new EU RED Cyber security regulation / compliance to EN18031 series of standards apply to IOT devices sold in Northern Ireland? If so, products sold prior to 01 Aug, within warehouses not yet installed that are non-compliant be recalled or does the regulation only apply to new sales?

Yes, the RED delegated regulation applies to products made available in Northern Ireland.

It applies to products that are placed on the market for the very first time. This is first making available of a product for distribution, consumption or use within the EU.

Radio equipment already placed on the market in Northern Ireland before 1 August 2025 is grandfathered; any device first made available thereafter must meet the new cybersecurity requirements from day one.

Any radio equipment in scope that entered NI distribution before 1 August 2025 remains governed by the RED obligations in force at that time.

Q22. Will EV Chargers with Wi-Fi/BLE connection full under non-critical category under EU CRA?

An EV charger, even one with a BLE radio, doesn't map to any of the Class I or Class II categories in Annex III.

Its core functionality is electric charging, not identity/access management, networking hardware, security software or any of the other "important products" technical descriptions.

Because the BLE link is likely ancillary (supporting the charger's main role of energy deliver) it stays in the CRA's default (non-important, non-critical) bucket and follows the baseline Article 7 self-assessment route.

09. Conclusion

The landscape of product compliance is undergoing a fundamental shift, with cybersecurity and data protection moving from voluntary best practices to mandatory legal requirements.

The UK PSTI Act and the EU's Cyber Resilience Act and RED Delegated Regulation demonstrate a global commitment to securing digital products and protecting consumer data.

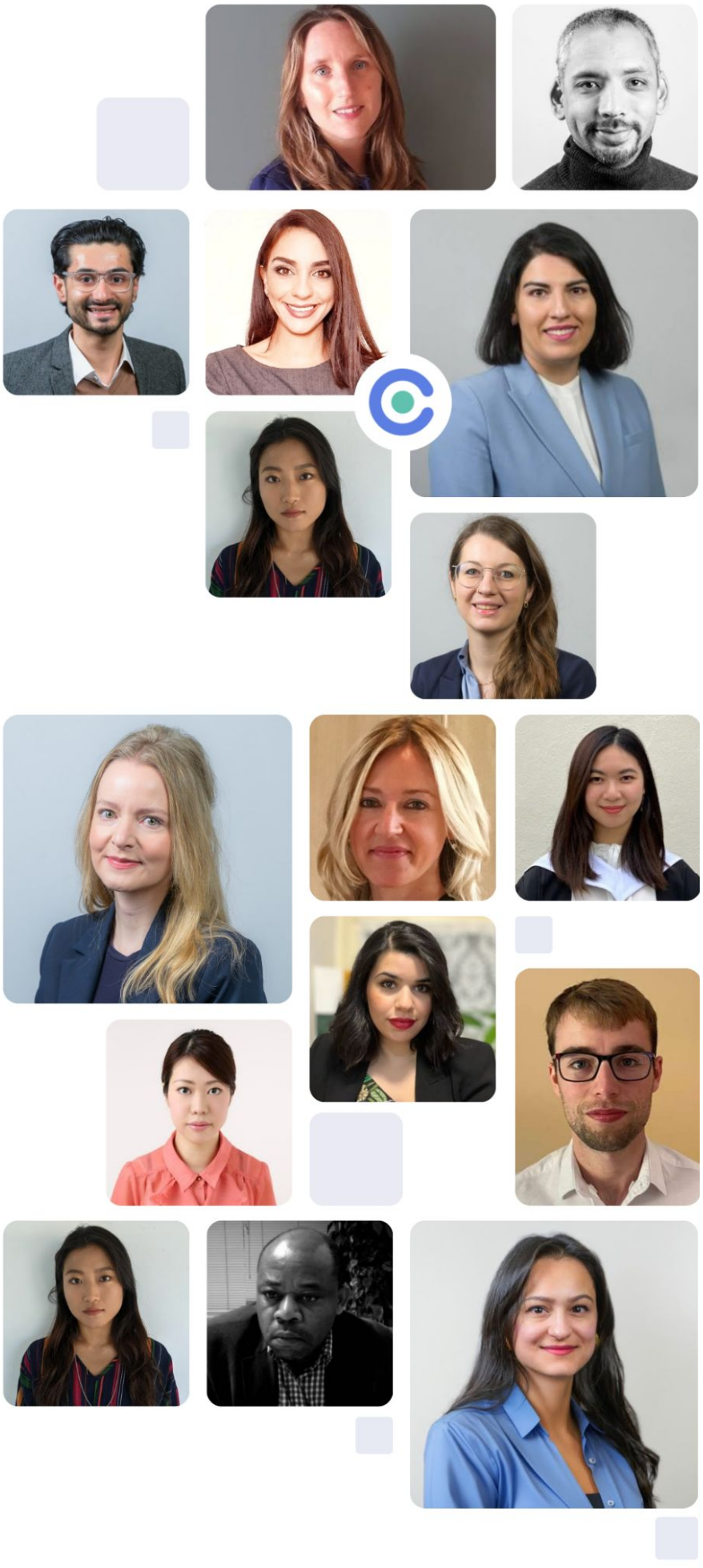
While there are differences in their scope, timelines, and documentation requirements, these legislative frameworks share a common goal: to ensure products are secure by design.

For manufacturers, importers, and distributors, understanding and proactively complying with these new rules is no longer optional.

It is essential for safeguarding consumer trust, protecting against cyber threats, and ensuring legal market access.

Stay informed. Stay compliant. Stay competitive.

Compliance & Risks



Add 80+ Experts to Your Team

Stop Drowning in Regulatory Updates and Get Back to Business.

Feeling overwhelmed by the ever-changing world of global regulations? You're not alone. Keeping up with complex legislation like ESPR, RoHS, and China RoHS can feel like a full-time job, draining valuable resources from your core business.

What if you could add **80+ compliance experts** to your team?

With our Ask the Experts service, you can. Our global team of **50+ subject matter experts** and 30+ knowledge partners provides unparalleled expertise across a diverse range of products, geographies, and policy areas. We monitor regulatory changes daily and provide clear, concise answers to your most pressing compliance questions.

Gain instant access to:

- **In-depth knowledge:** Our experts possess deep understanding of complex regulations, including ESPR, RoHS, and China RoHS.
- **Rapid response:** Get quick answers to your questions, often within 30 minutes, freeing up your team to focus on other priorities.
- **Confidence and clarity:** Navigate regulatory complexities with assurance, knowing you have a team of experts backing you up.

Boost your compliance capabilities without expanding your headcount.

Empower your business today - begin your journey and **speak to a regulatory expert.**

Compliance & Risks

OUR NUMBERS

300+

CUSTOMERS WORLDWIDE

195

COUNTRIES COVERED

100,000+

REGULATIONS

→| complianceandrisks.com