CRA Article 14: Reporting Obligations in Practice

IAPP European Privacy KnowledgeNet · Munich · 12 October 2026

Alexander Wagner – Jones Day
Daniel Nunn – FTI Consulting
Adrian Fonger – FTI Consulting

The views set forth herein are the personal views of the speakers and do not necessarily reflect those of Jones Day or FTI Consulting.



Legal Baseline

The Cyber Resilience Act and Article 14

The Cyber Resilience Act in One Page

Product with digital elements – Article 3(1) CRA

"A software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately."

What this means

- Products with software or a network connection sold in the EU – devices and stand-alone software
- Including the cloud service the product needs to work, for example the app backend of a smart doorbell (Article 3(2))
- Reporting also covers products placed on the market before 11 December 2027 – the other CRA requirements do not (Article 69(3))

Who has to act

- **Manufacturer** – carries the reporting duty
- **Importers, distributors** – inform the manufacturer; become manufacturer when selling under their own brand (Articles 19–21)
- **Open-source stewards** – limited duty (Article 24(3))

Article 14 applies since 11 September 2026 – all other obligations from 11 December 2027

Article 14: Triggers and “Awareness”

Actively exploited vulnerability	Severe incident
Reliable evidence that an attacker has used a security flaw of the product without permission (Articles 3(42), 14(1)). **Not enough:** a researcher showing that an attack would work.	An incident that harms the product's ability to **protect data or functions**, or lets **malicious code** in (Article 14(3), (5)). **Example:** attackers take over the server that distributes the product's software updates.

When is the manufacturer “aware”? – Commission CRA guidance of 27 July 2026, C(2026) 5252 (not binding)

When, **after a first assessment of a suspicious event**, it has a **reasonable degree of certainty** that a vulnerability in its product is being actively exploited, or that a severe incident has occurred and has affected the security of the product.

The first assessment must start promptly. Attacks known before 11 September 2026 need not be reported.

Article 14: Three Reports, One Platform

Within 24 hours

Early warning

- That an exploited vulnerability or incident exists
- Countries where the product is sold
- Incident: whether an attack is suspected

Within 72 hours

Notification

- Product affected and what happened
- Measures taken and what users can do
- How sensitive the information is

14 days / one month

Final report

- Vulnerability: 14 days after a mitigating or corrective measure is available
- Severe incident: one month after the 72-hour notification

All deadlines run from awareness.

Where to report

ENISA's Single Reporting Platform – reaches the national CSIRT of the main establishment and ENISA (Articles 14(7), 16)

Inform users – Article 14(8)

Affected users – where appropriate all users – and what they can do

Fines: up to EUR 15 million or 2.5 % of worldwide annual turnover (Article 64(2)).

The Case: ACME Smart Home – Friday Evening

ACME Smart Home GmbH (fictitious)

- Based in Munich – decisions on product security are taken there
- Sells video doorbells across the EU, including older models; a retailer also sells them under its own brand
- The doorbells work with the ACME app and cloud, which store video clips of visitors
- ACME is an "important entity" under NIS2 and the German BSI Act

Fri 18:40 A security researcher e-mails ACME: attackers can take control of the doorbell over the internet. Working attack code is attached.

Fri 19:15 Several customers call the hotline: their doorbell restarts by itself and an unknown device is logged in to their app.

Is the clock running? Since when? Who decides?

How the case unfolds

Fri 18:40 Researcher reports a working attack

Fri 19:15 Customers report strange behaviour

Sat 01:30 Attack traces found on doorbells

Sun Attackers accessed the video cloud

Mon 16:00 Workaround published in the app

The Case: Hour 0 to 24

From the first signal to the early warning

Establishing Awareness: Reliable Technical Evidence

How technical teams turn an initial warning into reliable evidence of active exploitation

ACME case: from warning to evidenced exploitation



Fri 18:40 — **Fri 19:15** — **Sat 01:30**

Ingest the warning

Researcher disclosures, customer reports, security-provider intelligence and product telemetry should route into one product-security response path.

Preserve the original warning, source and receipt time so the signal can be investigated and reconstructed.

Technical action

Secure disclosure intake
Case logging
Evidence preservation
Timestamping
Source validation

Possibility vs proof

Validate the affected product and version, reproduce safely where possible, and correlate the report with logs, telemetry and known indicators.

A working exploit shows an attack can happen; corroborating evidence is needed to prove it.

Technical action

Vulnerability validation
Controlled exploit reproduction
Software and firmware comparison
Log review
Threat intelligence correlation

Confirm real-world use

Look for traces on real devices: exploit execution, unauthorised logins, persistence, session or token abuse, and other forensic artefacts.

In ACME, traces on customers' doorbells on Sat 01:30 move the case from a possible exploit to evidenced active exploitation.

Technical action

Device forensics
Log correlation
Behavioural device comparison
Network traffic analysis
Authentication analysis

Evidence awareness

Preserve logs, device images and relevant artefacts before containment or remediation changes the environment.

Record confirmed facts, assessments and unknowns - plus the technical basis and timestamp that Legal can rely on.

Technical action

Forensic imaging
Evidence hashing
Timeline reconstruction
Chain-of-custody recording
Confidence assessment of findings

TECHNICAL → LEGAL Reliable evidence supports the moment of awareness

Hour 0 to 24: When Is ACME Aware?

Fri 18:40	Fri 19:15	Sat 01:30	Sun 01:30
Researcher sends a working attack Shows that an attack is possible – not that an attacker has used it	**Customers report strange behaviour** A suspicious event – the first assessment must start now	**Technical analysis finds attack traces on doorbells** Reasonable degree of certainty: ACME is aware – the clock starts	**Early warning due at the latest** Safer: count from Fri 19:15 – so report on Saturday during the day

Safer: count from Friday 19:15 and submit the early warning on Saturday during the day

In the same hours

- Record when ACME became aware, on what evidence, and who decided
- Brief the crisis team and Communications: what was reported, what may be said

Preparedness enables rapid and coordinated communication in the first 24h

Communications templates on hand:
Holding statement · customer talking points, Q&A · communication to the researcher · security advisory · internal briefing · monitoring setup

01
Build the communications baseline

- Turn initial technical evidence and assessment of vulnerability into holding language
- Work in lockstep with technical and legal teams to prepare communications for signoff by ACME

02
Equip front line for incoming inquiries

- Activate inquiry management process, e.g. shared managed inbox, reactive messaging, escalation protocol
- Establish backchannel to update crisis team on incoming critical questions/potential misinformation

03
Edit prepared stakeholder templates

- Make amendments to material according to priority stakeholders, e.g. customers, researcher, retailer
- Edit communications templates for further non-CRA related stakeholders
- Plan communications cadence and channels

Bottom line: The perception of the issue by key stakeholders is shaped by ACME **getting their narrative out first**, before others do. The first 24 hours establish the communications foundation for all stakeholder engagement that follows.



Remember: the clock is running since Friday, 19:15!

Hour 24: Where We Need to Be

Done by now

- Awareness assessed and recorded
- Early warning submitted
- Evidence secured, attack contained
- Crisis team running
- Holding statement ready
- Researcher: receipt confirmed, publication timing agreed

Where the hand-overs matter

Technical team → **Legal:** evidence for the moment of awareness

Legal → **Communications:** what was reported, what may be said

Communications → **all:** incoming questions, leaks, the researcher's plans

The Case: Hour 24 to 72

From the full picture to the notification

Hour 24 to 72: Which Products and Customers Are Affected

As the investigation matures, the technical answer becomes more specific - and so does the report

Notification – due Mon 19:15

- **Product affected**; the flaw and the attack, in general terms
- **Measures taken**; what users can do
- **How sensitive** ACME considers the information
- **Affected models and software versions** (as per the current state of the investigation)
- In line with the Early Warning, **explain changes, but do not contradict**
- Legal (ideally not operational) answers **follow-up questions from the CSIRT**

Sun

Video cloud accessed

Possibly a second report as severe incident – GDPR and BSI Act deadlines may also run

Sun to Mon

More doorbells affected

Retailer sells under its own brand: that counts as a manufacturer and so it reports itself (Article 21)

Mon 16:00

Workaround in the app

The 14 days for the final report may start now – and it is the core of the message to users

Scope narrows

- ACME testing finds the exploit affects older models on firmware branch 3.x and the retailer-branded equivalent using the same codebase.
- Newer 4.x builds can be excluded, turning a broad product concern into a defined affected set.

Impact clarifies

- Device compromise allows remote control and unauthorised login
- Sunday cloud logs show compromised sessions reached stored video clips.
- The team separates device compromise from cloud / data impact so Legal can assess each consequence.

Population maps

- Firmware/build records, device IDs, telemetry and retailer sales are correlated to identify affected or potentially affected customers and countries.
- The technical team can now distinguish confirmed affected, potentially affected and positively excluded populations.

Response qualifies

- The Monday workaround blocks the vulnerable path
- Supported devices move to a firmware patch or upgrade path; unsupported versions need replacement.
- The response is now specific enough to tell users what to do and to report measures taken with current confidence.

Hour 24 to 72: Notification and Developments

Notification – due Mon 19:15

- Product affected; what the flaw and the attack are, in general terms
- Measures taken; what users can do
- How sensitive ACME considers the information
- Affected models and software versions as the current state of the investigation
- In line with the early warning – explain changes, do not contradict
- The platform's countdown starts when the early warning is submitted
- Someone answers follow-up questions from the CSIRT

Sun

Video cloud accessed

Possibly a second report as severe incident – GDPR and BSI Act deadlines may also run

Sun–Mon

More doorbells affected

Retailer sells under its own brand: it counts as manufacturer and reports itself (Article 21)

Mon 16:00

Workaround in the app

The 14 days for the final report may start now – and it is the core of the message to users

Communications depend on technical findings and legal assessment

Article 14(8): inform everyone affected (models, versions, countries) – as identified by the technical scoping – and say what they can do to protect themselves.

Technical findings → **Legal & risk assessment** → **Actionable stakeholder information** (in particular customers)

Key principle: translate technical findings for the affected users

User message must be ready before the workaround goes live – the 72-hour notification (Mon 19:15) will refer to it

CRA-specific: If users are not informed in time, the CSIRT may inform them itself.

Once users are informed, every answer must tell the same story

One fact base for authority reports, user messages and press statements – whatever the deadlines

Who asks	What they ask
Customers	*Am I affected? What do I do? Was my video seen?*
Retailer with own brand	*Our customers, our report, our message?*
Business customers	*What do we tell our own authorities and customers?*
Researcher	*When is it published?*
Media	*How many devices or users are affected? Since when? How could this happen?*
Employees	*What do I need to do? What does it mean for us? What should I tell customers?*
Investors	*What is the operational, financial and reputational impact?*

01 One fact base, one consistent story

The reports are the benchmark: what you say must hold up against what you filed (CRA, GDPR, NIS2) – also months later.

02 Warn without arming attackers

Enough for users to protect themselves, no guide for attackers.

03 Expect leaks

Researcher, authority or others may go first. Reactive statement ready.

Mandatory under the CRA: authority and affected users.
Addressing other stakeholders (press, investors, partners etc.) not required under CRA but in most cases still very important from a strategic perspective.

Hour 72: Where We Need to Be

Done by now

- Notification submitted
- Affected models and customers known – as of hour 72
- Users informed or message scheduled
- Video cloud incident assessed – reported if required
- GDPR and BSI Act decisions taken and documented
- Stakeholder communications updated, aligned with reporting obligations and delivered through the right channels

Deadlines still running

CRA – vulnerability: final report 14 days after the workaround (Monday 16:00)

CRA – severe incident, if reported: one month after the notification

BSI Act: final report one month after the notification

GDPR: notification to the authority within 72 hours (Art. 33) and affected individuals without undue delay after becoming aware (Art. 34), and responses to inquiries, where needed

What Now?

Recommendations for companies in scope

Detection and Evidence

The first 24 hours disappear quickly if signals sit in separate queues or nobody knows to escalate.

01

Know how you will establish awareness

- Know where product-security signals arrive (researcher reports, customer support, SOC monitoring, cloud telemetry and suppliers).
- Ensure they converge quickly into one incident process.

Possible is not the same as real

- Separate exploitability or proof-of-concept from evidence of malicious use on real systems.
- That distinction is central to technical qualification and to a defensible awareness decision.

Reporting and user action depend on knowing precisely which products and people are affected.

02

Make products traceable

- Be able to move from a vulnerable component or firmware version to the affected model and ultimately to the customers using it.
- If that takes weeks of spreadsheet reconciliation, the 72-hour process will fail when it's needed most!

Component | Version | Product | Customer

- Follow the chain until affected deployments and users can be identified.
- Each step adds specificity Legal and Communications need for the 72-hour notification and user action.

Article 14 is an operating process, and a policy; lockstep collaboration must work under pressure.

03

Exercise the process

- Do not test Cybersecurity, Legal and Communications separately.
- Run an ambiguous scenario and make the teams decide when awareness occurs, what must be reported, what users should be told and who approves each step.

One technical base, continuous updates

- Maintain one current record of confirmed facts, assessments, unknowns, scope and mitigations.
- Legal filings, customer messages and press statements must evolve without contradiction.

Six Legal Steps Before Friday Evening

01

Know your authority

Document which country's CSIRT is responsible (Article 14(7)).

02

Platform access ready

Tested EU Login accounts for more than one person.

03

Write the awareness rule

Who decides that the clock has started, and how it is recorded.

04

Prepare templates

Early warning, notification, final report, message to users.

05

Bind your suppliers

Contracts ensure attack information and fixes arrive quickly.

06

Map all reporting duties

One internal overview of what an incident can trigger – CRA, GDPR, NIS2, DORA – with deadlines and authorities.

Three key communication steps to prepare for a CRA-related crisis event

01
Prepare for known vulnerability types

- Sit down with Cybersecurity and Legal and ask which flaw types are realistic for your (current and future) products
- Pre-draft templates for advisories, user notices (also machine-readable) and Q&A for them.

02
Know your stakeholders

- Prepare the list of who must be informed – and when, by whom
- Include authorities, partner brands (e.g. retailers), business customers, researchers.
- Check: Can you reach your end users, including those who bought through retailers?
- Keep authority appraised of facts as situation develops

03
Set clear decision paths and responsibilities

- Who does what, when: define roles, people and deputies
- One approval process incl. Tech & Legal that also works at night and on weekends
- Test processes & interfaces before you need them to work under pressure

Conclusions:

1. Communications need a deeper understanding of products, and a seat at the table early in their lifecycle.
2. More and earlier than ever, mitigating reputation risk hinges on IT, Legal and Comms teams' lockstep work.

Questions and Discussion

Alexander Wagner – awagner@jonesday.com

Daniel Nunn – daniel.nunn@fticonsulting.com

Adrian Fonger – adrian.fonger@fticonsulting.com

Speaker: Alexander Wagner



Alexander Wagner
Jones Day, Munich
awagner@jonesday.com

Alexander Wagner is a lawyer at Jones Day, advising German and international organizations on privacy, data protection, cybersecurity, artificial intelligence, and digital regulation. His practice focuses on EU data and digital regulation, including the GDPR, Data Act, AI Act, Digital Services Act, NIS2 Directive, Cyber Resilience Act, and DORA.

He helps businesses prepare for emerging regulatory requirements and build practical data governance frameworks, and advises on the IT and data protection aspects of M&A, carve-out, and outsourcing transactions. In the cybersecurity space, he guides clients through incident response, including notification duties, regulatory investigations, and IT-forensic workstreams.

Speaker: Daniel Nunn



Daniel Nunn
FTI Consulting, London
daniel.nunn@fticonsulting.com

Daniel Nunn is a senior cybersecurity and risk leader with extensive experience in advanced threat defence, cyber risk management, regulatory compliance and operational resilience. At FTI Consulting, he advises organisations on cybersecurity strategy, threat and risk management, regulatory readiness and complex technology regulation.

Prior to joining FTI, he held senior roles at Bank of America, where he established and operated its Global Threat Defence function, protecting one of the world's largest financial institutions against sophisticated cyber threats. He previously served as a Principal Technical Specialist at the UK Financial Conduct Authority, working on cybersecurity supervision, policy and regulatory engagement. Daniel has three patents for technology innovation.

Speaker: Adrian Fonger



Adrian Fonger
FTI Consulting, Frankfurt
adrian.fonger@fticonsulting.com

Adrian Fonger works in the Strategic Communications practice at FTI Consulting in Frankfurt. He frequently serves on international engagements, including cyber incidents, investigations, and litigation cases in the Critical Infrastructure, Healthcare, and Automotive sectors.

He regularly works alongside legal, technical and management teams coordinating crisis response strategies, regulatory notifications and stakeholder communications, combining his expertise in Strategic Communications in special situations with his interest in data privacy, cybersecurity, and the effects of regulatory frameworks on organizations handling emerging risks and crises.

Disclaimer (Jones Day)

Any presentation by a Jones Day lawyer or employee should not be considered or construed as legal advice on any individual matter or circumstance. The contents of this document are intended for general information purposes only and may not be quoted or referred to in any other presentation, publication or proceeding without the prior written consent of Jones Day, which may be given or withheld at Jones Day's discretion. The distribution of this presentation or its contents is not intended to create, and receipt of it does not constitute, an attorney-client relationship. The views set forth herein are the personal views of the authors and do not necessarily reflect those of Jones Day.