IAPP UK Intensive 2026

Privacy | AI governance | Cybersecurity law

Training 23-24 February

Workshops 24 February

Conference 25-26 February

LONDON

#IAPPIntensive26

Many Laws, One Product

GDPR, CRA and DORA for Engineering and Product Management

WELCOME AND INTRODUCTIONS

Iiris Kivikari

Dittmar & Indrenius Attorneys

Partner, Head of IP Media & AI and Marketing & Consumers

Hannes Saarinen

RELEX Solutions

Director of Privacy & AI governance

Antti Vähä-Sipilä

Wolt

Director, Product Security

Product creation

Product Management and Service Design

- Building the business case & designing the solution

Implementation and Deployment

- Building and launching the product

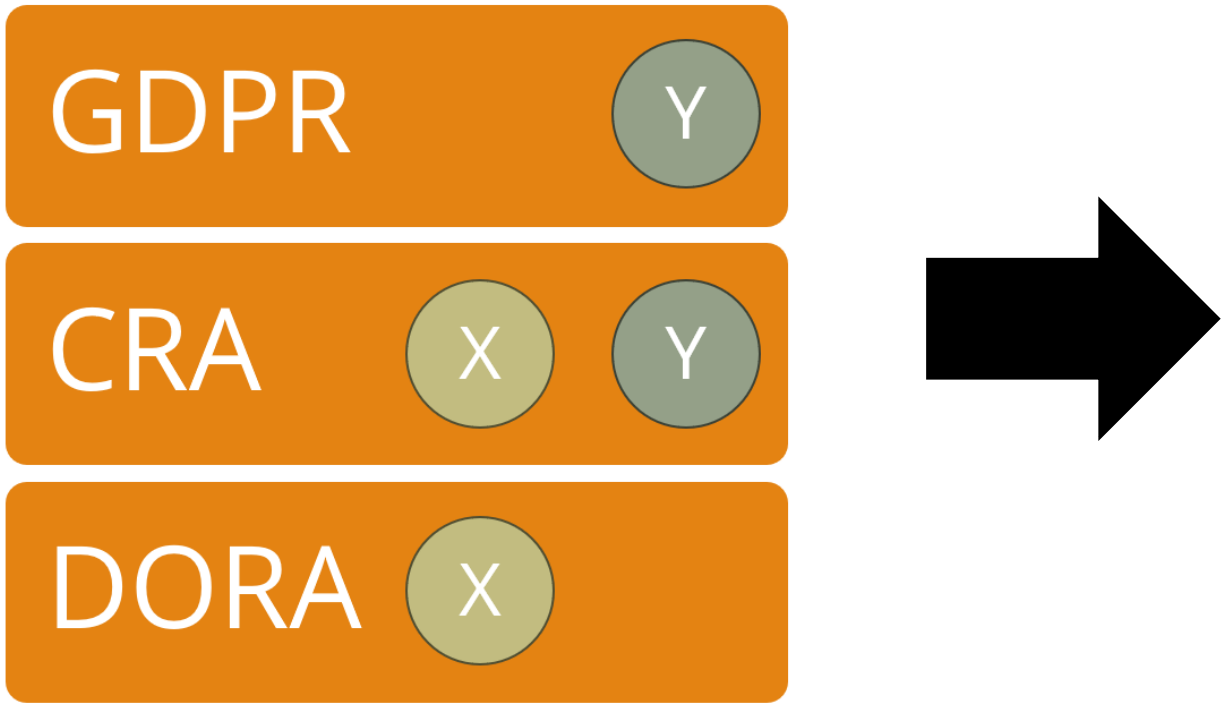
Production, Operations and Post-sales

- Running and supporting the service

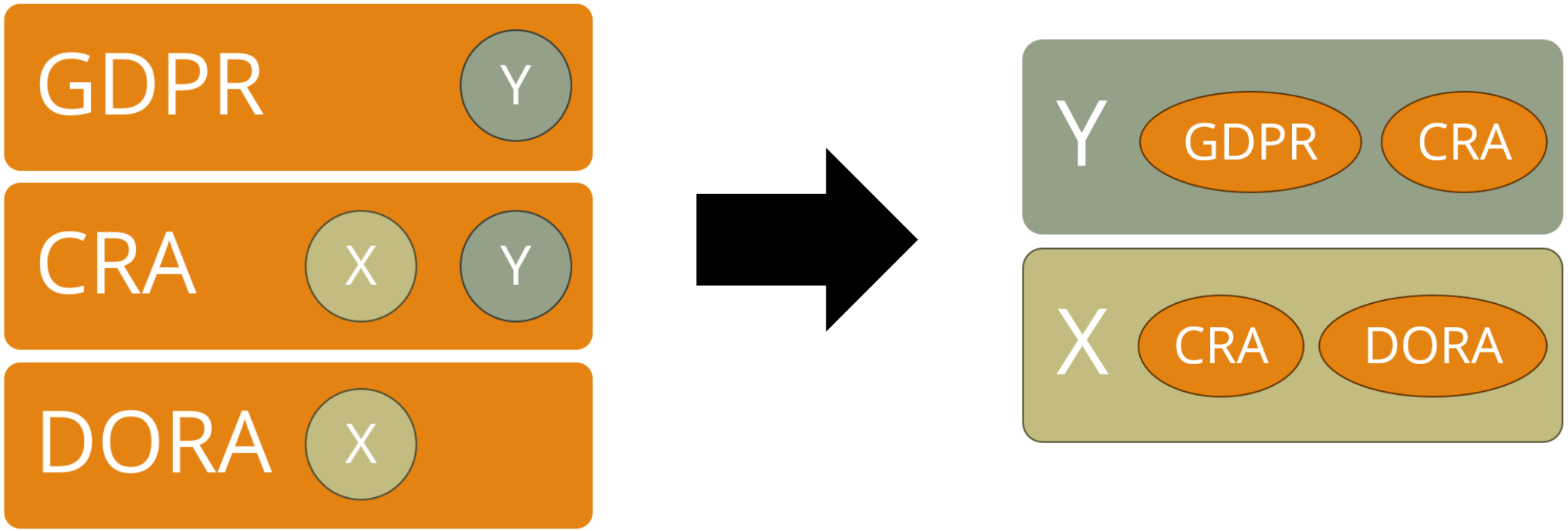
The Challenge

- The legalisation of data security
  - The expanding regulatory landscape: GDPR, DORA, CRA, NIS2, DA, …
- The growing complexity for product engineering teams
- The cost of fragmented compliance approaches
  - Direct costs, indirect costs and risks

From laws to product development activities, or …



… from product development activities to laws?



Our Approach – Integration Not Isolation

- The ”one stop shop” approach to data protection and security
- Building on the overlap with existing security requirements
- Benefits: cost efficiency, comprehensive risk mitigation, reduced friction, team motivation
- Prerequisites: teams’ capability to take responsibility, central management’s ability to trust teams.

In a Nutshell: GDPR, DORA and CRA

General Data Protection Regulation ("GDPR")

- Applies to the processing of personal data
- Aims to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data

Digital Operational Resilience Act ("DORA")

- Applies to financial entities (e.g. banks, insurance companies, investment firms and other) and service providers
- Aims to ensure that financial entities can withstand, respond to, and recover from ICT disruptions

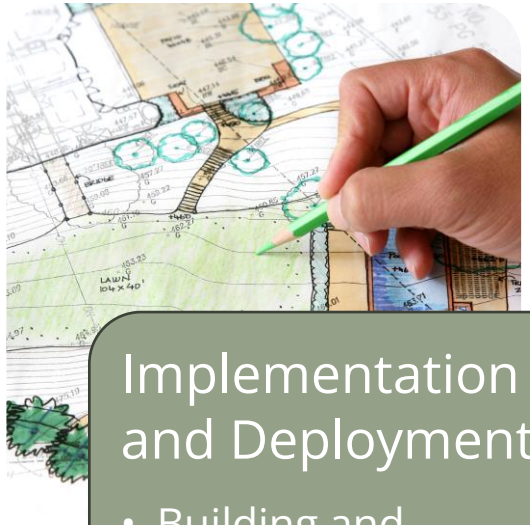
Cyber Resilience Act ("CRA")

- Applies to products with digital elements made available on the market that include a data connection to a device or network
- Aims to safeguard consumers and businesses buying software or hardware products with digital elements
- Entry into force: gradually 11/2024 – 12/2027

Product creation

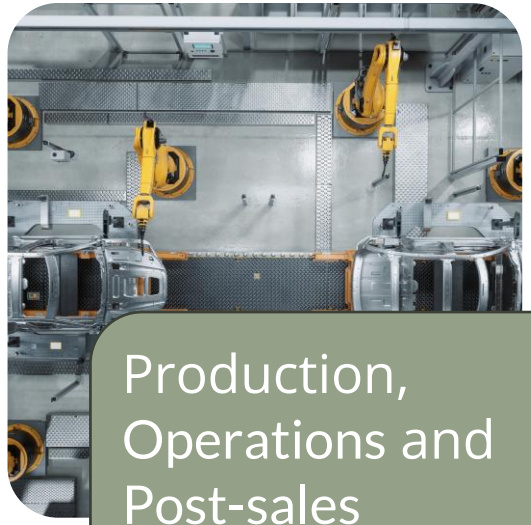
Product Management and Service Design

- Building the business case & designing the solution



Implementation and Deployment

- Building and launching the product



Production, Operations and Post-sales

- Running and supporting the service

Product Management and Service Design: Focus points

- Key question for product management and service design:
  "What do we want to build and how do we make money out of it?"
- Key question for lawyers:
  "What are the requirements? Can this be done compliantly? If so, how?"
- Typical impacts per regulation to engineers:
  - GDPR: impacts whether or not it can be done lawfully
  - DORA: affects the way it is done – if in scope
  - CRA: affects the long-term business case and its viability. Also, the type of our products and our customer relationship impact what we can do in the maintenance phase

Product Management and Service Design: Practical implications

- DORA and the GDPR impact especially broader processes, and are (merely) applied to products
  - Each product is a ”reflection” of the process as a whole
- Costs of compliance and avoiding “the compliance bottleneck”
  - Who needs to be “at the table”? (product owners, lawyers, privacy professionals, information security, developers, engineering management…)
  - Asset management and/or visibility to infrastructure are critical
  - CRA’s potential maintenance requirements to engineering

Ne bis in idem

- Multiple regulations multiply the risks
- Even regulations with different aims can have corresponding obligations
- EUCJ C-205/23 - *Engie Romania* sets out prerequisites for transposing two penalties:
  1. there are clear and precise rules making it possible to predict which acts or omissions may be subject to a duplication of proceedings and penalties, and to ensure coordination between the two competent authorities;
  2. the two sets of proceedings concerned have been conducted in a sufficiently coordinated manner and within a proximate timeframe; and
  3. all the penalties imposed correspond to the seriousness of the offences

Product creation

Product Management and Service Design

- Building the business case & designing the solution

Implementation and Deployment

- Building and launching the product

Production, Operations and Post-sales

- Running and supporting the service

Implementation and Deployment: Focus points

- Key compliance design principle:
  ”Minimal engineering impact, maximum gain”
- Key question for lawyers:
  “What are the risks? Can we live with them?”
- Typical impacts per regulation to engineers:
  - GDPR: implementing (existing) compliance processes – are the existing processes viable / sufficient?
  - DORA: Being in-scope should be a conscious decision and not an accident
  - CRA: Cyber security level must reflect the level of actual risks

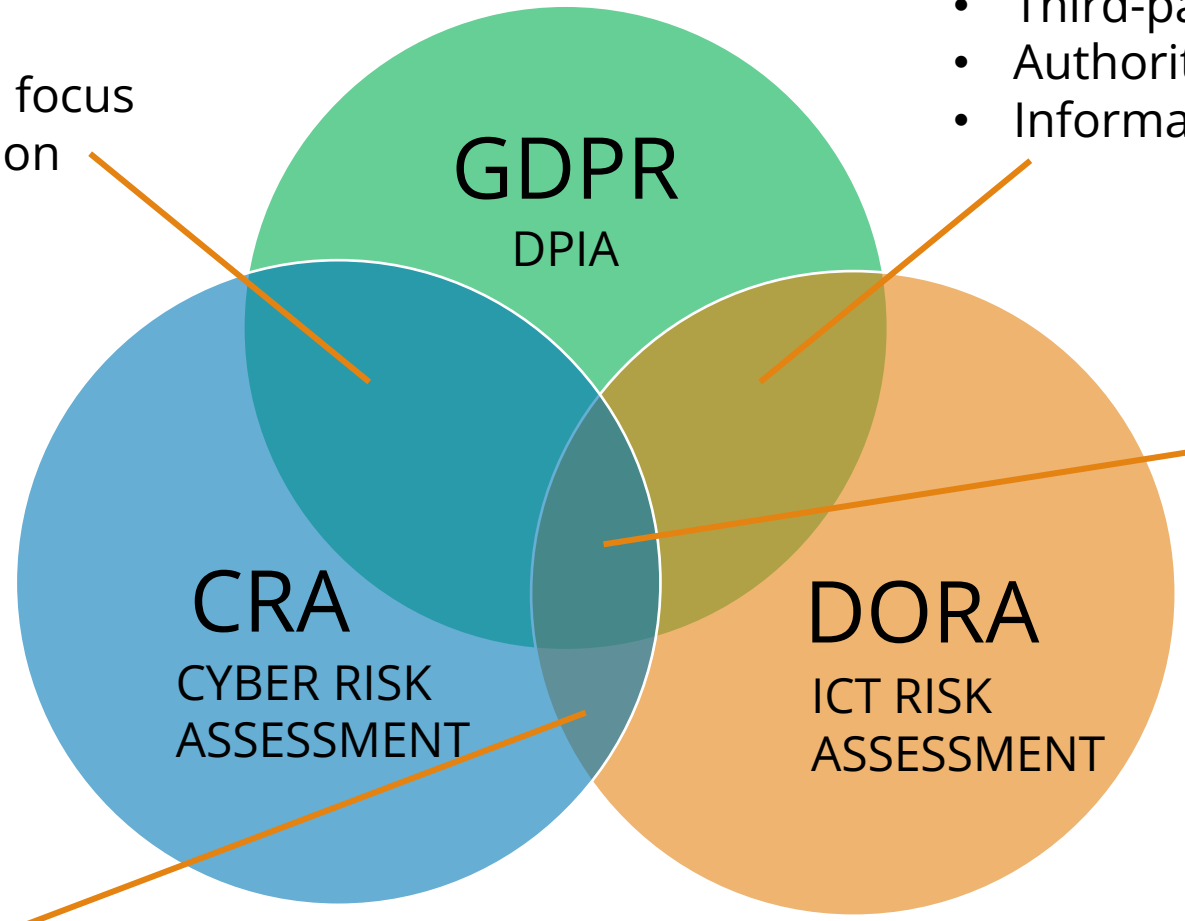
Implementation and Deployment: Practical implications

- Integration into centralized compliance i) processes and ii) technologies
  - Using standard components or consulting centralized compliance teams
  - Compliance verification check-points (legal-security-privacy collaboration review gates) can be reduced as the trust to engineering increases
- Ensuring data security: security requirements vs. legal security requirements
  - How much do you defend against actual attackers / vulnerabilities vs. in preparation of an authority inquiry
  - Document management and evidence generation (for audits)
  - Control, accept or transfer
- Vendor management: build or buy (and resort to legal security requirements)
  - Effectiveness of task delegation and integration measures
  - Focus changes from own work to vendor management: visibility, testing, monitoring, audits…
  - Dependencies (practical vendor lock, CRA's bill of materials)
- Legal viewpoint: the challenges of accountability, defensible evidence, and the division of responsibilities

Implementation and Deployment: Risk assessments

- End-user protection focus
- High-risk identification

- Third-party assessment
- Authority reporting
- Information asset risks



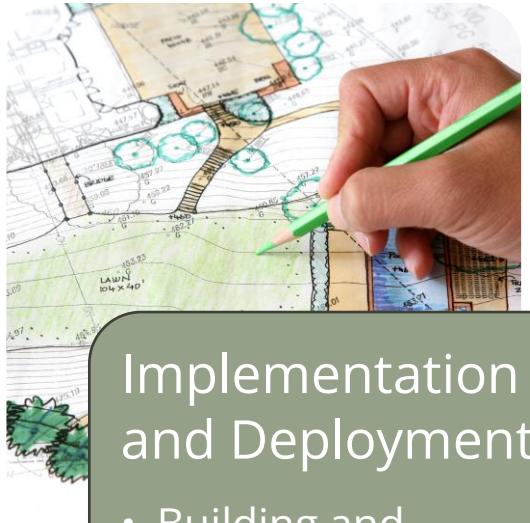
- Technical cyber assessment
- Lifecycle approach
- Conformity verification

- Risk identification required
- Documentation mandatory
- Ongoing reassessment
- Vulnerability identification
- Techical & organizational measures

Product creation

Product Management and Service Design

- Building the business case & designing the solution



Implementation and Deployment

- Building and launching the product

Production, Operations and Post-sales

- Running and supporting the service

Production, operations and post-sales: Focus points

- Key question for service operations:
  ”How many allocated engineers are needed to maintain the product?”
- Key question for lawyers:
  “Do we have the processes etc. in place to react to incidents?”
  “Who is responsible for legal upkeep and incident management?”
- Typical requirements towards engineers:
  - GDPR: Knowledge and relationship management, and the right to process the resulting data
  - DORA: Low effort vulnerability management
  - CRA: Deployment (and customer relationship) must allow for fixes
    - *Can we collect and retain more personal data when operating under CRA?*

THANK YOU

Iiris Kivikari

Dittmar & Indrenius Attorneys

Partner, Head of IP Media & AI and Marketing & Consumers

Hannes Saarinen

RELEX Solutions

Director of Privacy & AI governance

Antti Vähä-Sipilä

Wolt

Director, Product Security

Key Takeaways

1. Integration beats fragmentation
2. Collaboration and a high level of legal understanding for engineers is essential
3. Plan your operational model based on whether you build or buy
4. Build evidence as you go
5. Real security delivers compliance

How Did Things Go?
(We Really Want To Know)

Did you enjoy this session? Is there any way we could make it better? Let us know by filling out a speaker evaluation.

1. Open the IAPP Events app.
2. Select **IAPP Intensive 2026**.
3. Tap "Schedule" on the bottom navigation bar.
4. Find this session. Click "Rate this Session" within the description.
5. Once you've answered all three questions, tap "Done".

Thank you!