

PROGRAMME

---

# Data Protection specialist with CIPT certification

---

Become a Data Protection specialist with the globally recognised CIPT certification.

Certified Information Privacy Technologist (CIPT) training offers a robust, interactive opportunity to learn about critical privacy concepts. While not purely an “exam prep” course, it is appropriate for professionals who plan to certify as Certified Information Privacy Technologists, as well for those who want to deepen their privacy knowledge. Both the course and the exam are based on the same body of knowledge.

The CIPT course runs over two days and will be divided into 8 modules.

## TIME AND PLACE

Tuesday 17 March and Wednesday 18 March 2020 from 9:00 - 17:00  
Kromann Reumert  
Sundkrogsvej 5  
DK-2100 Copenhagen

## TRAINER



Tim Clements works with Kromann Reumert as an independent consultant. He is also an official IAPP trainer delivering courses directly for IAPP at various IAPP events across Europe and for training partners globally. He also works as a GRC and Privacy Program Manager across Europe. Tim has experience from multiple Industry sectors, including construction, printed media, digital agencies, financial services, IT facility management, FMCG, biotech, emergency services, aviation and martech. Since 2005 he has worked with multi-national corporations driving global projects and programs to operationalise legal/policy requirements using structured approaches, pragmatism, systems thinking, visual communication, and strong stakeholder management.

## COURSE MATERIAL

On the first day of the course, participants will receive printed course material, which will also be sent electronically a few days before the course starts.

*Please note that the course and all course material are in English.*

## CERTIFICATION PROCESS

You can read more about the certification process on IAAP's website [here](#).

*Read more about the modules on the next page >*

## MODULES

**Module 1: Fundamentals of information privacy** reviews the modern history of privacy, foundational privacy concepts, data protection roles and fair information practices; explores the impacts of privacy and data protection regulations on information management.

**Module 2: Privacy in the IT environment** describes compliance requirements, IT risks, and stakeholder privacy expectations; differentiates between privacy and security.

**Module 3: Core privacy concepts** explains foundational elements for embedding privacy in IT and provides an overview of general privacy principles; summarises data protection by design and default.

**Module 4: Privacy considerations in the information life cycle** explores privacy considerations throughout the stages of the information life cycle.

**Module 5: Privacy in systems and applications** examines the risks inherent in the IT environment and options for addressing them, including: identity and access management; credit card information and processing; remote access, BYOD and telecommuting; data encryption; and other privacy-enhancing technologies in the enterprise environment.

**Module 6: Privacy techniques** describes the strengths and weaknesses of authentication techniques as well as the use of identifiers; reviews and illustrates privacy by design.

**Module 7: Online privacy issues** explores the unique challenges that come from online privacy issues, including specific laws and regulations, online threats, social media, e-commerce, tracking technologies, and web security protocols.

**Module 8: Technologies with privacy considerations** describes specific privacy considerations associated with a variety of technologies including cloud computing, wireless IDs, location-based services, "smart" technologies, video/data/audio surveillance, and biometric recognition.