Halderstone

Training module

Operational Privacy Controls

Implement role-based privacy controls & data subject rights handling within an ISO/IEC 27701-aligned PIMS

Are your privacy controls lived or just documented?

Overview

ISO/IEC 27701 requires privacy controls to be defined, assigned, executed, and evidenced. The real challenge is not documenting controls, but making them work in daily operations.

This module focuses on implementing and sustaining operational privacy controls and data subject rights processes within a Privacy Information Management System (PIMS). Participants learn how to translate ISO/IEC 27701 role-based requirements for PII controllers and processors into workflows, ownership models, documented procedures, and reliable records.

The emphasis is on operational clarity: clear responsibilities, structured handoffs, consistent request handling, and traceable evidence that controls are functioning as intended.

Target audience

- People involved in implementing, operating, or improving a PIMS aligned with ISO/IEC 27701
- Executives and department heads accountable for the effectiveness and performance of a PIMS
- Those responsible for processes, policies, IT systems, risks, and controls related to data protection
- Auditors of ISO/IEC 27701 who want to deepen their understanding of management-side best practices (not audit technique)

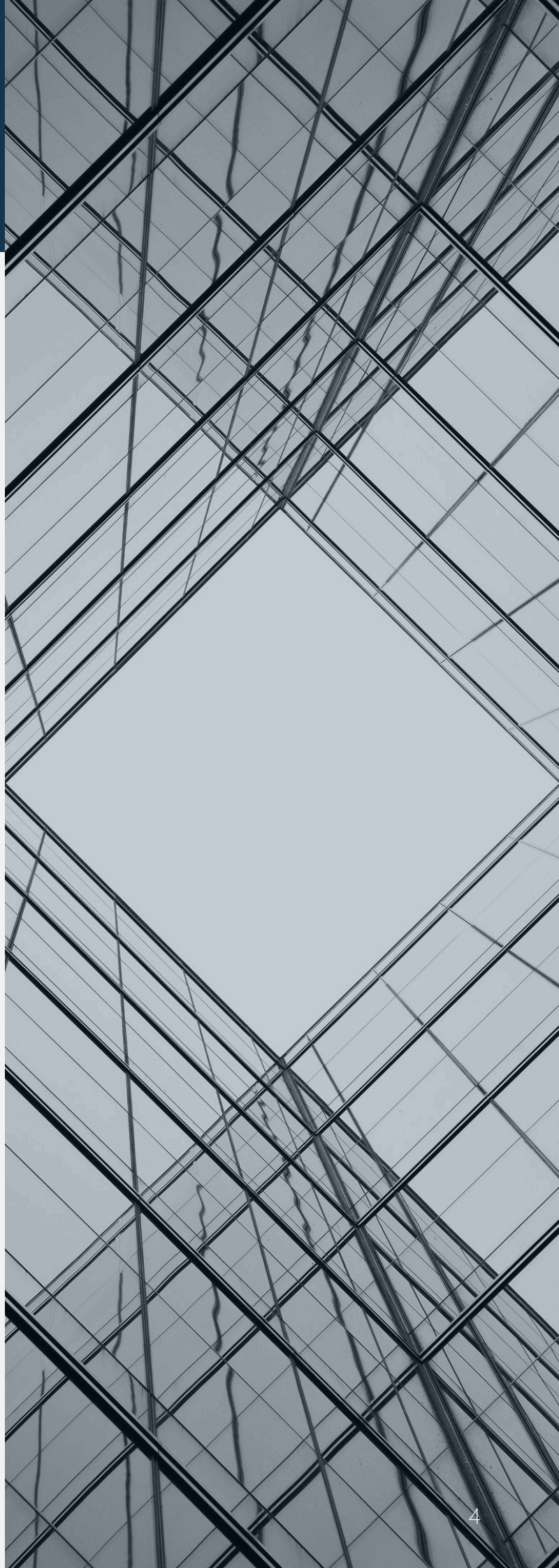
Is this module for you?

It is a good fit for you if you...

- need to operationalise privacy controls across real workflows.
- want clear role-based handling of data subject rights.
- need consistent evidence for privacy controls in daily operation.
- coordinate privacy execution across teams and suppliers.
- support audit-ready, repeatable privacy operations in a PIMS.

It may be less suitable for you if you...

- are looking for privacy fundamentals or role definitions.
- want DPIA methods or risk assessment logic.
- expect legal interpretation or jurisdiction-specific guidance.
- already run mature, stable operational privacy controls at scale.



Learning outcomes

Key outcomes

- Operationalise ISO/IEC 27701 controls in a stand-alone PIMS
- Design and run a structured data subject rights process
- Establish and govern privacy control interfaces across roles and suppliers

Additional capabilities

- Define proportionate, auditable evidence
- Manage complex DSAR cases
- Clarify controller and processor operating patterns
- Maintain control effectiveness as environments change

Agenda

Operationalising ISO/IEC 27701 controls in a stand-alone PIMS

How to turn ISO/IEC 27701 control intent into concrete, owned operational practices in a stand-alone PIMS without diluting controller and processor responsibilities

From control statements to workflows and evidence

How to translate control requirements into simple workflows and define just enough evidence to show decisions were made and followed

Controller controls: operating patterns

How controllers run transparency, purpose alignment, retention, and disclosure as routine processes with explicit exception handling

Processor controls: operating patterns

How processors operationalise “acting on instructions”, manage sub-processors, and operate shared platforms without role confusion

Supplier and sub-processor interfaces

How to split privacy control responsibilities between internal operations and enforceable supplier requirements across the lifecycle

Data subject rights handling as a managed process

How to run DSAR handling end to end with clear intake, routing, decision ownership, and consistent response logic

Special cases and failure modes

How to recognise and handle complex DSAR scenarios and avoid common breakdowns such as incomplete searches or unmanaged dependencies

Sustaining operational controls over time

How to keep privacy controls current as products, data uses, vendors, and tooling change through lightweight ownership and review routines

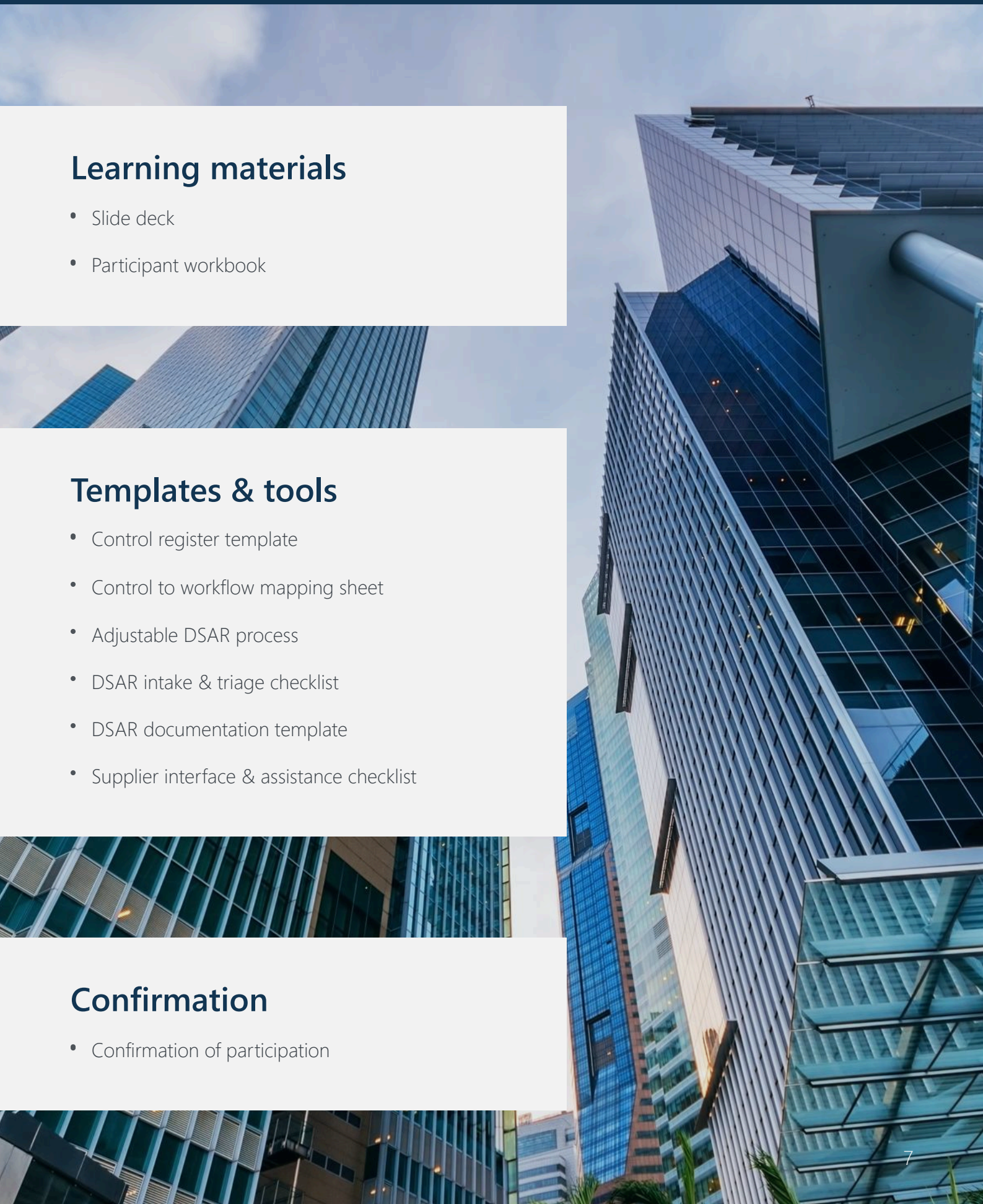
Technology as an enabler

How tooling supports execution and traceability of privacy controls while keeping human judgement central

Case-based workshop

Applying the learned concepts, methods, and approaches in a realistic case setting

Included materials



Learning materials

- Slide deck
- Participant workbook

Templates & tools

- Control register template
- Control to workflow mapping sheet
- Adjustable DSAR process
- DSAR intake & triage checklist
- DSAR documentation template
- Supplier interface & assistance checklist

Confirmation

- Confirmation of participation

Preparation guidance

Assumed background

This module assumes participants can already work with core privacy concepts and can navigate their organisation's processing reality.

Helpful background includes:

- Basic privacy / data protection concepts and terminology (PII, processing, recipients, retention, disclosure)
- Clarity on processing context, roles, and scope artefacts (at least at a high level)
- Familiarity with internal workflows and systems where PII is handled (ticketing, CRM, HRIS, support tooling, shared drives)

Preparatory modules

Foundation (depending on background)

Useful if you are new to the underlying concepts

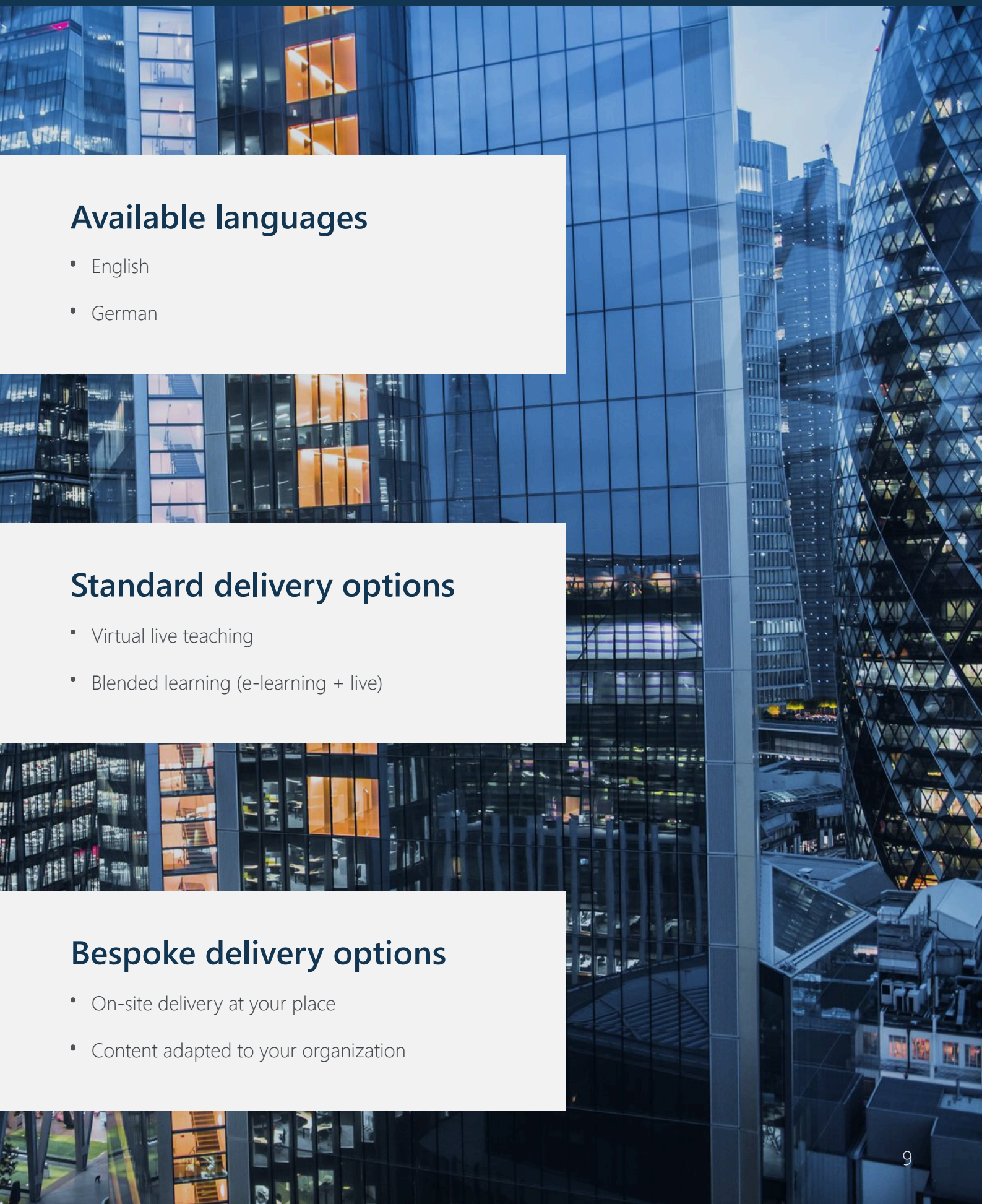
- Data Protection Principles
- Operational Control

Supporting (optional)

Helpful but not required to participate effectively

- PII Processing: Context, Roles & Scope
- Governance Design

Logistics



Available languages

- English
- German

Standard delivery options

- Virtual live teaching
- Blended learning (e-learning + live)

Bespoke delivery options

- On-site delivery at your place
- Content adapted to your organization

Halderstone

Halderstone by Langer & Co
Zürcherstrasse 2
CH-8852 Altendorf
Switzerland
info@halderstone.com
www.halderstone.com