Halderstone

Trainingsmodul

Datenschutz-Folgenabschätzung (DSFA)

Datenschutzrisiken bewerten, Auswirkungen begründen und DSFA in einem an ISO/IEC 27701 ausgerichteten PIMS dokumentieren

Sind Ihre DSFA systematisch und belastbar?

Überblick

ISO/IEC 27701 legt klare Anforderungen an die Bewertung von Datenschutzrisiken und deren Behandlung innerhalb eines PIMS fest und ist nicht länger von einer ISO/IEC 27001-Zertifizierung abhängig. In der Praxis haben Organisationen weniger Mühe damit, eine DSFA durchzuführen, als die Bewertungslogik wiederholbar zu machen: konsistente Auslöser, belastbare Begründungen für Auswirkungen, dokumentierte Annahmen und klare Entscheidungs-rechte für Restrisiken.

Dieses Modul fokussiert die DSFA-Logik als Fähigkeit des Managementsystems in einem PIMS: Bewertungen strukturieren, Auswirkungen auf betroffene Personen begründen, Ergebnisse mit Behandlungsentscheidungen verknüpfen und Bewertungen aktuell halten, wenn sich die Verarbeitung ändert. Vermittelt werden weder Grundlagen des Datenschutzes, Abgrenzung und Rollenbestimmung, operative Datenschutzmassnahmen noch die Ausübung von Betroffenenrechten; diese Themen sind in angrenzenden Spezialisierungsmodulen abgedeckt. Auch die allgemeine Risikomethodik (Skalen, Bewertungsmodelle, Auslegung der Risikobereitschaft) wird nicht erneut behandelt; sie ist in den Grundlagen des Risikomanagements verankert.

Zielgruppe

- Personen, die an der Umsetzung, dem Betrieb oder der Verbesserung eines Datenschutz-Informationsmanagementsystems (PIMS) nach ISO/IEC 27701 beteiligt sind
- Geschäftsleitung und Bereichsleitende, die für die Wirksamkeit und die Leistungsfähigkeit eines Datenschutz-Informationsmanagementsystems (PIMS) verantwortlich sind
- Personen, die für Prozesse, Politiken, IT-Systeme, Risiken und Steuerungsmassnahmen im Bereich Datenschutz verantwortlich sind
- Auditorinnen und Auditoren von ISO/IEC 27701, die ihr Verständnis für Best Practices auf der Managementseite vertiefen wollen (nicht Audittechnik)

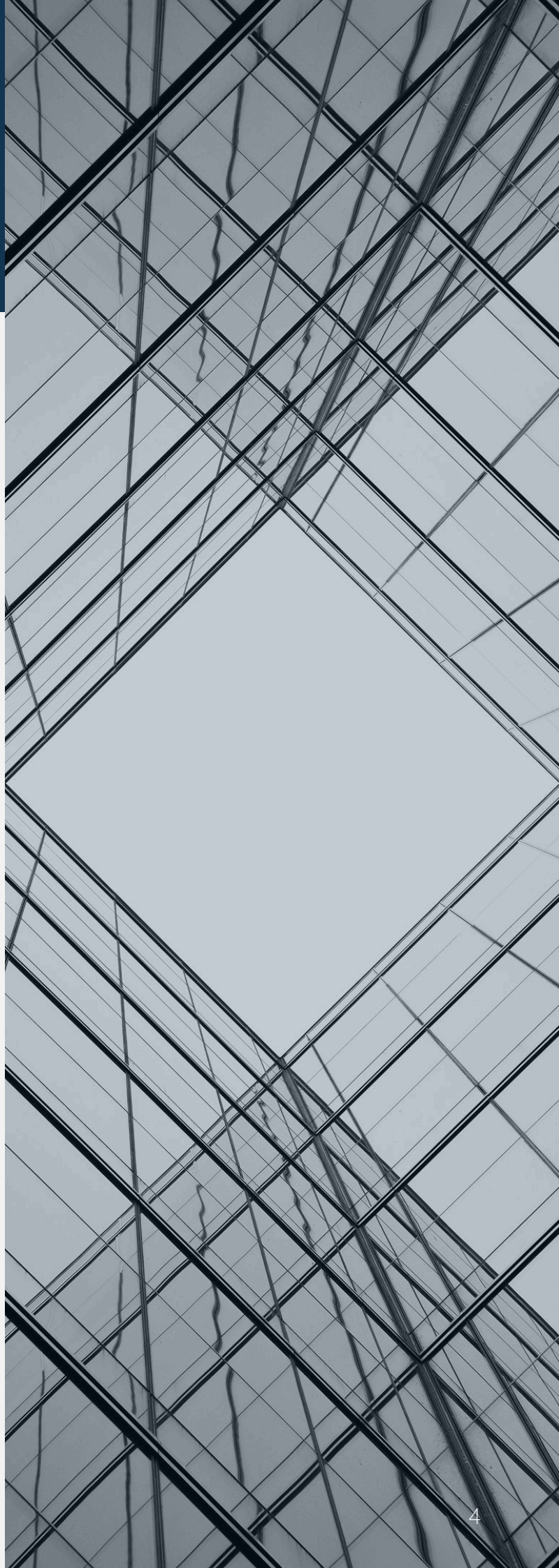
Ist dieses Modul für Sie das Richtige?

Es passt gut für Sie, wenn Sie...

- eine wiederholbare DSFA-Logik statt ad hoc erstellter Bewertungen brauchen.
- klare Auslöser, Rollen und Entscheidungszuständigkeiten für DSFA wünschen.
- belastbare Begründungen für Auswirkungen bei Freigabe- und Akzeptanzentscheidungen brauchen.
- DSFA bei Änderungen in Verarbeitung und Systemen aktuell halten wollen.
- eine auditfähige, konsistente DSFA-Governance in einem PIMS unterstützen.

Es passt möglicherweise weniger gut für Sie, wenn Sie...

- nach Grundlagen des Datenschutzes oder rechtlicher Theorie suchen.
- eine allgemeine Risikomethodik oder ein Bewertungsmodell erwarten.
- detaillierte Orientierung zu technischen Datenschutzmassnahmen erwarten.
- bereits stabile, fest verankerte DSFA-Prozesse im grossen Massstab betreiben.



Lernergebnisse

Zentrale Lernergebnisse

- Verständnis der Erwartungen aus ISO/IEC 27701 an Bewertung von Datenschutzrisiken und Behandlung innerhalb eines PIMS
- DSFA-Auslöselogik und Verhältnismässigkeitsregeln organisationsweit konsistent definieren
- DSFA-ähnliche Bewertungen um reale Verarbeitungstätigkeiten mit gemeinsamen Diensten und Lieferanten strukturieren

Zusätzliche Fähigkeiten

- Disziplinierter Umgang mit Begründungen zu Auswirkungen auf betroffene Personen und transparenten dokumentierten Annahmen
- Übersetzung von Bewertungsergebnissen in klare Behandlungsentscheidungen und Kriterien zur Akzeptanz von Restrisiken
- Ein wartbares DSFA-Aktenset mit Nachvollziehbarkeit und Überprüfungsanlässen erstellen, damit DSFA aktuell bleiben

Agenda

Wo die Bewertung von Datenschutzrisiken im PIMS verankert ist

Wie die Bewertung von Datenschutzrisiken im PIMS entscheidungsreife Eingaben für Behandlung und Begründung liefert, statt als separate Pflichtübung zu laufen

Bewertungsgrenzen und Eingangsgrössen

Wie klare Bewertungsgrenzen auf Basis des gepflegten Verarbeitungskontexts, der Rollen und der Artefakte zum Geltungsbereich definiert werden und generische Checklisten oder meinungsbasierte Eingaben vermieden werden

Auslöselogik: wann eine DSFA-ähnliche Bewertung nötig ist

Wie Änderungsanlässe erkannt werden, die eine vertiefte Bewertung auslösen, und wie zwischen leichter Überprüfung und voller DSFA-ähnlicher Bewertung mit belastbarer Begründung verhältnismässig triagiert wird

Den Bewertungsgegenstand definieren

Wie Bewertungen rund um konkrete Verarbeitungstätigkeiten aufgebaut werden, damit Verantwortung und Ergebnisse klar bleiben

Auswirkungen auf betroffene Personen begründen

Wie Auswirkungen auf Rechte und Freiheiten anhand von Schwere, Umfang, Rückgängigmachbarkeit und Verletzlichkeit beurteilt werden, während Annahmen explizit und nachweisbasiert bleiben

Wahrscheinlichkeit in Datenschutzbegriffen beurteilen

Wie kausale Ketten von Designentscheiden zu Exposition und Schaden nachvollzogen werden, mit Indikatoren und transparenten Unsicherheiten statt falscher numerischer Präzision

Behandlungslogik und Restrisikofreigaben

Wie Bewertungsergebnisse mit Behandlungsoptionen verknüpft, begründet und über klare Entscheidungsrechte, Eskalationswege und Konsultationsauslöser gesteuert werden

DSFA-Aktenset und Nachvollziehbarkeit

Wie ein schlankes DSFA-Aktenset gepflegt wird, das die Nachvollziehbarkeit von der Bewertung über Entscheidungen bis zu Umsetzungsnachweisen unterstützt

Technologie als Unterstützung

Wie Register, Workflows, Versionierung und KI-gestützte Zusammenfassungen genutzt werden, um Bewertungen aktuell zu halten und mit Änderungsanlässen zu verknüpfen, ohne menschliches Urteil zu ersetzen

Praxisworkshop

Anwendung der erlernten Konzepte, Methoden und Ansätze in einem realistischen Praxisfall

Enthaltene Unterlagen

Lernunterlagen

- Foliensatz
- Workbook für Teilnehmende

Vorlagen & Werkzeuge

- Entscheidungsbaum für DSFA-Auslösung und Triage
- Vorlage für DSFA und Bewertung von Datenschutzrisiken
- Arbeitsblatt für die Begründung von Auswirkungen
- Matrix zur Nachvollziehbarkeit von Risiken zu Behandlungen
- Checkliste für DSFA-Überprüfung und Änderungsanlässe
- KI-Prompt-Sammlung

Bestätigung

- Teilnahmebestätigung

Vorbereitungshinweise

Vorausgesetzter Hintergrund

Dieses Modul setzt bereits Folgendes voraus:

- Arbeitswissen zu den grundlegenden Datenschutzkonzepten (personenbezogene Daten, Verarbeitungszwecke, Empfänger, Aufbewahrung, rechtmässige Bearbeitung)
- Vertrautheit damit, wie die eigene Organisation Verarbeitungstätigkeiten und Änderungen dokumentiert (auch wenn noch nicht perfekt)
- Grundlegendes Verständnis von Managementsystemen (Rollen, dokumentierte Information, Steuerungsroutinen)

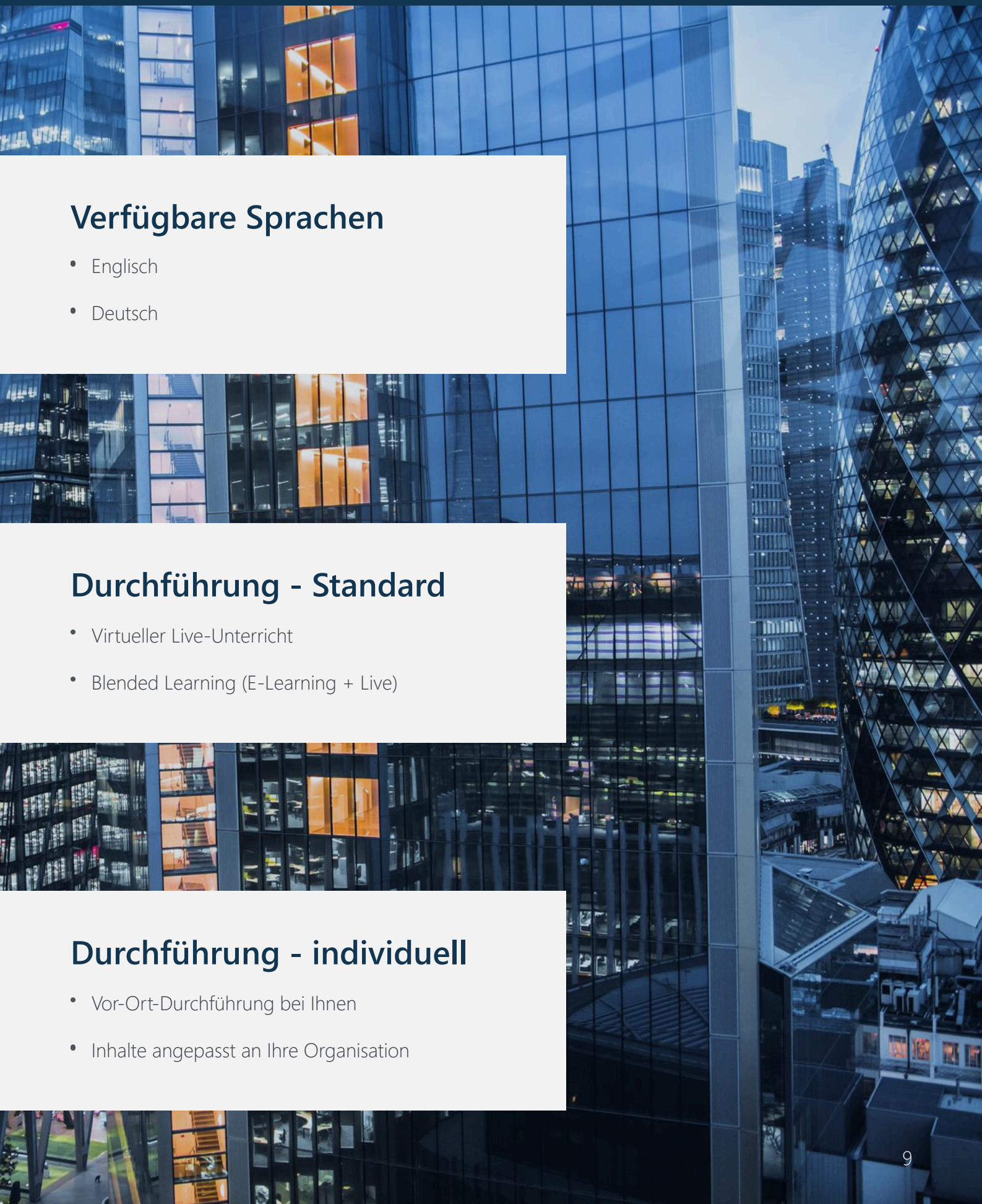
Vorbereitungsmodule

Grundlagen (je nach Vorwissen)

Hilfreich, wenn Sie mit den zugrunde liegenden Konzepten noch wenig vertraut sind

- Grundsätze des Datenschutzes
- Risikomanagement

Organisatorisches



Verfügbare Sprachen

- Englisch
- Deutsch

Durchführung - Standard

- Virtueller Live-Unterricht
- Blended Learning (E-Learning + Live)

Durchführung - individuell

- Vor-Ort-Durchführung bei Ihnen
- Inhalte angepasst an Ihre Organisation

Halderstone

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