WORKSHOP 07 / FACILITATOR GUIDE

Compliance trust and data boundaries

Make data flows, rules and open specialist reviews traceable

Create an evidenced data-flow map, permissions and rules matrix, data lifecycle and a decision and question register with owners.

Duration

Half day · 240 minutes including 20 minutes of breaks

Participants

3-6 representatives of privacy, information security, legal, IT and employee representation where relevant; include the process owner for the use case.

Outputs

• Data flow with purpose, data types, location, operator, recipient and retention at each step.

• Permissions matrix with technical enforcement and tests, beyond role descriptions.

• Coordinated drafts of AI disclosure, data lifecycle and rules catalogue.

• Vendor and contract review status, plus separate decisions, conditions and open legal questions.

Format and learning evidence

No legal advice. The session structures review of a specific deployment. Legal assessment, required participation and approvals belong to the responsible specialists. It is not blanket compliance certification.

Prerequisites

• Use case, users, selected or requested operating profile and affected systems are described.

• Current technical data flows and vendor documents exist for the specific deployment, or are explicitly marked missing.

• Privacy and information security can own unresolved assessments; legal questions are not resolved by majority vote.

Observable completion criteria

• Every processing statement has evidence or an open review item with an owner and date.

• Each role has bounded permissions; shared access is not treated as personal identity evidence.

• Every critical rule defines its trigger, permitted response, blocked action, handover and test.

• Unresolved required conditions prevent the affected live-data start. Decision status states scope and conditions explicitly.

Three parts of the kit

This guide contains the agenda, facilitation instructions, exercise debrief, sources and slide notes. Slides support the group session. Print the separate worksheets or use the editable HTML workbook.

Preparation

Before the session

• Beforehand, hold a 30-45 minute call with process ownership and privacy to confirm purpose, users, countries, data types, policies, employee agreements and specific review questions.

• Request current data-flow, vendor, security and contractual documents with version and date. Marketing claims do not confirm the chosen operating profile.

• Use sample data. Do not copy unnecessary personal data, credentials or confidential live data into participant material.

• Prepare worksheets 7.1-7.7; invite missing specialists to the relevant blocks or keep decisions open pending specialist review.

• Before each delivery, check source currency and current availability. The latest publicly available Overmind articles through 17 November 2026 are incorporated; illustrative scenarios are not feature commitments.

Materials and access

• Use-case brief, outputs from format 5 and current Scoping Workbook.

• Vendor documents, processing agreements where relevant, subprocessor list, technical and organisational measures, and customer policies.

• Slides, worksheets and a shared register with version and evidence references.

Agenda and materials

Time	Block	Sheet	Slides
00:00-00:10	Goal and review boundary (10 min)	7.7	1-3
00:10-00:50	Data flows and classes (40 min)	7.1	4-5
00:50-01:20	Roles and technical permissions (30 min)	7.2	6-7
01:20-01:30	Break (10 min)		
01:30-02:10	Information and data lifecycle (40 min)	7.3	8-9
02:10-02:45	Rules and precise status messages (35 min)	7.4	10-11
02:45-02:55	Break (10 min)		
02:55-03:30	Vendor and contract review (35 min)	7.5	12-13
03:30-04:00	Decision log and open questions (30 min)	7.6, 7.7	14-16

Times are elapsed from the start of each session and include scheduled breaks. A practice or testing phase between sessions is additional.

Facilitation script

01 Goal and review boundary / 10 min

Goal

Confirm review scope and responsibility.

Method

Read the use case and operating requirement. State No legal advice explicitly. Separate facts, assumptions and missing evidence; identify the specialist decision makers.

Facilitator prompt

Which specific decision should this session prepare?

Debrief

Who can make each assessment and approval?

Output

Bounded review assignment.

Materials: sheet 7.7; slides 1-3

02 Data flows and classes / 40 min

Goal

Identify all affected steps and recipients.

Method

Walk a normal path for 10 minutes, map data, purpose, location, operator, recipient and retention for 20, then classify data under the customer scheme and identify prohibited data for 10. Attach evidence or mark open status.

Facilitator prompt

Which data leave the original process, and where do they go next?

Debrief

Is any vendor, cache, export or recipient missing?

Output

Data flow with evidence status.

Materials: sheet 7.1; slides 4-5

03 Roles and technical permissions / 30 min

Goal

Constrain access throughout the workflow.

Method

Identify users, expert review, operations and support for 10 minutes. Allocate retrieval, content, reporting, settings, approval, action, export and deletion rights for 15. Define wrong-role and revoked-access tests for 5.

Facilitator prompt

Where is permission technically enforced, including caches and actions?

Debrief

Could a conversation instruction bypass the technical boundary?

Output

Permissions matrix with enforcement and test evidence.

Materials: sheet 7.2; slides 6-7

04 Break / 10 min

Goal

Rest.

Method

Pause work.

Facilitator prompt

We resume in ten minutes.

Debrief

Disclosures and data lifecycle follow.

Output

Break taken.

Materials: sheet ; slides

05 Information and data lifecycle / 40 min

Goal

Own wording and data flows through deletion.

Method

Draft AI disclosure and the location of full information for 10 minutes. Identify legal basis, participation, audio and transcript review questions for 10. Map purpose, retention, access, deletion, recipients and backups for 20.

Facilitator prompt

What remains after the conversation in each system, and why?

Debrief

Which wording is draft, and which has specialist approval?

Output

Draft wording and owned data lifecycle.

Materials: sheet 7.3; slides 8-9

06 Rules and precise status messages / 35 min

Goal

Translate boundaries into testable rules.

Method

Collect critical situations for 10 minutes. Define confirm, block or handover rules with exact responses for 15. Walk through wrong-role, third-party data and unknown-action-status cases for 10. Distinguish understood, prepared, sent, accepted and completed.

Facilitator prompt

Which statement would imply a processing status that has not been reached?

Debrief

Is the rule technically enforced and testable with a negative case?

Output

Rules catalogue with status and negative tests.

Materials: sheet 7.4; slides 10-11

07 Break / 10 min

Goal

Rest.

Method

Pause work.

Facilitator prompt

We resume in ten minutes.

Debrief

Vendors and decisions follow.

Output

Break taken.

Materials: sheet ; slides

08 Vendor and contract review / 35 min

Goal

Assign documents and open specialist assessments.

Method

Confirm parties' roles for 5 minutes. Compare vendors by processing step, subprocessors, locations, purposes, retention, support access and contracts for 20. Assign missing documents and questions about required assessments and participation for 10.

Facilitator prompt

Which specific document supports this commitment for this deployment?

Debrief

Which assessment still requires the responsible specialist?

Output

Review status with versions and open specialist questions.

Materials: sheet 7.5; slides 12-13

09 Decision log and open questions / 30 min

Goal

Assign every condition and record launch boundaries.

Method

Record decisions separately from open questions for 15 minutes. Assign evidence, responsible specialist and dates for 10. Read required live-data conditions, stop and fallback rules for 5.

Facilitator prompt

Which unresolved item blocks which specific use?

Debrief

Can each approval be traced to scope, version, person and evidence?

Output

Decision log and question list with no unassigned tasks.

Materials: sheet 7.6, 7.7; slides 14-16

Close and follow-up

Next steps

• Capture assigned open tasks on the day. Within five working days, provide the outcome document with evidence, versions, decisions and the No legal advice notice.

• To format 5: technical authorisation, confirmation, logging and handovers. To format 4: source permissions and rule tests. To format 8: approved wording and links.

• Record specialist decisions and retest technical implementation. Reopen affected checks after vendor, data-flow or scope changes.

Pitfalls

• The labels EU cloud or local do not replace evidence for each actual processing step.

• Deletion in one system does not delete copies already transferred to recipients.

• A friendly disclosure does not replace a required technical access control.

• Knowledge approval, design version, internal launch and guest access are distinct decisions; a test does not publish anything.

Terms

Data lifecycle

Collecting, processing, storing, sharing, retaining, exporting and deleting data with owners for each system.

Decision status

Draft, specialist review open, conditional decision or approved for an explicitly bounded scope.

Worksheet debrief

7.1 Data flow with evidence status

Use one sheet per step or recipient. Review source device, audio, recognition, KSE, response, output, logs and connected systems.

Illustrative example

Fictional example: a conversation note should reach a ticketing system. Evidence from the specific connection establishes which text and sources are actually transferred.

Review criterion

No processing step is described solely by a general profile name.

7.2 Roles permissions and technical tests

Use one card per role and function. Distinguish shared access from personal authentication.

Illustrative example

Fictional example: a team role can read approved instructions but not confidential personnel data. The negative test attempts the prohibited retrieval.

Review criterion

A role label without technical enforcement and a negative test is insufficient.

7.3 Information and data lifecycle

Use one card per data type or text. Review audio, transcript, evidence, operational data, notes and recipient copies separately.

Illustrative example

Fictional example: disclosure identifies AI support and the responsible organisation. Specialists still assess the full text and processing.

Review criterion

No blanket retention period for data types with different purposes and recipients.

7.4 Rules catalogue and status review

Use one card per critical situation; include third-party data, missing permission, missing evidence and unknown action status.

Illustrative example

Fictional example: report sent, acceptance still open. The voice states that status and does not claim completion.

Review criterion

Every rule is testable through its trigger, technical behaviour, response and evidence.

7.5 Vendor and contract review status

Use one card per vendor or review item. Identify assessments by privacy, security and legal specialists.

Illustrative example

Fictional example: vendor known, specific endpoint and processing location unconfirmed. Status remains open.

Review criterion

A requested contract is not yet a reviewed or executed contract.

7.6 Open legal and specialist questions

Record questions only; use 7.7 for decisions already made.

Illustrative example

Fictional example: may a particular external role view conversation content? Privacy assesses purpose and basis; IT provides the technical permission design.

Review criterion

Each open question has a responsible specialist, date and visible impact.

7.7 Decision log and launch conditions

Use the first three fields for shared context, evidence and stop conditions. Review earlier entries there. Then record one decision each for the internal trial, design and guests. Fictional design N2: E1 permits internal testing with sample data only. E2 documents bilateral confirmation of the fixed N2 design. E3 records a request for guest access with live data; there is no approval for that use. All three records are dated 5 March 2027.

Illustrative example

E1: internal use limited to N2 and sample data. Stop if live data is proposed. E2: design N2 fixed. E3: guest use with live data on hold; access team to obtain the specific decision. A change to N3 requires fresh evidence for E1/E2; the guest hold continues.

Review criterion

Three separate entries state scope, status and evidence. A version change reopens the affected review.

Slide facilitation notes

01 Compliance trust and data boundaries

State No legal advice explicitly.

02 Outputs and decision boundary

No blanket compliance certification.

03 Facts assumptions open questions

Link to the current Scoping review logic.

04 Data flow step by step

Include normal processing and onward transfers.

05 Data classes and boundaries

Do not collect sensitive live data in the workshop.

06 Roles and bounded permissions

Add backup roles and access revocation.

07 Technical enforcement

Require evidence from the actual system.

08 Information before use

Distinguish draft wording from specialist approval.

09 Data lifecycle by system

Local deletion does not recall recipient copies.

10 Confirm Block Hand over

A blocked action should not create a silent dead end.

11 State status precisely

A sent report is not a completed task.

12 Vendors by processing step

Use confirmed documents as evidence.

13 Assign specialist questions

Assign review of required participation and assessments.

14 Separate approvals

Confirm E1 and E2 only within their stated N2 scopes. E3 carries no guest approval. N3 requires a new review of the affected scope. Ask the learner to read back all three entries.

Activity

On sheet 7.7 record a status and evidence item for each scope. What changes for N3?

15 Go or Hold for the bounded scope

Scoping prepares the decision; it does not replace specialist approval.

16 Next steps

Read open launch conditions aloud and confirm them.

Sources and revision status

Materials for 2027, reviewed on 17 November 2026. Exercises and proposed criteria are newly authored facilitation materials. They do not establish technical availability or client approval.

Voice Operating Layer

https://overmind.one/en/voice-operating-layer

VOP components, ownership and separate approvals

The 4Cs of Voice Intelligence

https://overmind.one/en/the-4cs-of-voice-intelligence-effective-profitable-workflows

The four Cs as an integrated workflow to review rather than isolated technology components

Project scoping workbook

https://overmind.one/wp-content/uploads/2026/10/Scoping_EN.html

Task, workplace testing, roles, stop/fallback, integration register and Go/Hold review

Give Your Voice Hands

https://overmind.one/en/give-your-voice-hands

Processing states, target-system evidence, duplicate prevention and observation versus diagnosis

Local baseline

The inventory review used the October 2026 catalogues and kits 1 to 10. Current materials are in DE and EN. Product lists and interface terminology differ between the former catalogues, strategy and scoping. The review records these differences; the updated catalogue guides selection by task.

Before a client session

The facilitator checks current access, confirmed scope, language, sources, roles and approvals. Test demo limits and interfaces in the actual setting. Exact pricing and outcome commitments follow the approved quotation.