Workshop: KPIs & Maturity Model

Governance by Design: From Maturity to Risk to Action

Björn Möller · Daniela Will · Lukas Bootz

caralegal

Agenda

1 **Introduction** — 10 min
What is the benefit? · What are we working on?

2 **Workshop** — 65 min
3 stations · 3 rounds · 3 questions — teams rotate and build on each other's results

3 **Plenary & next steps** — 10 min
Compare results with the model · what we take away

caralegal

1.

Introduction



Benefits



Speak management language

Risk scores turn "we should" into prioritised, budgetable decisions.

Prove instead of feel

Objective KPIs support accountability (Art. 5(2) GDPR) towards management, auditors and authorities.

Benchmark

Compare business units, companies and markets on one common scale.

Shape the standard

Your input flows into the model and the guide — plus access to templates and KPIs.

What are we working on?

1

IDW PH 9.860.1 as the basis

67 test questions in 12 chapters — recognised, complete and audit-proof.

2

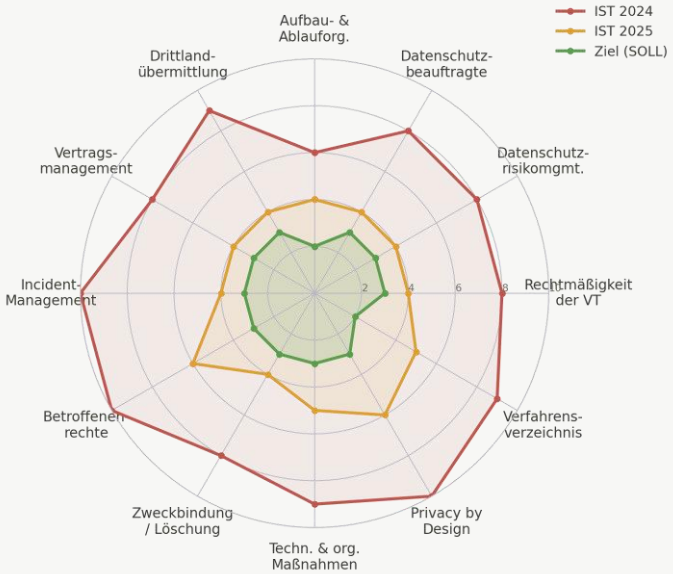
5 maturity levels + risk score

Each test question gets levels I–V and a risk score from 1 to from 1 to 10 per level.

3

KPIs make the level objective

Measurable indicators instead of gut feeling and self-self-assessments.



One picture for all topics: current → progress → target

Where we stand — and why we need you

ALREADY IN PLACE

- Maturity descriptions (I–V) for all 67 test questions (model V8.4)
- A risk score for every maturity level
- First "translations" and KPI drafts for selected test questions, e.g. incident management

TODAY'S WORK

- Objective KPIs defined for all levels
- Risk scores need a reality check across sectors
- Day-to-day translations so far reflect only a few organisations

Who we are



Daniela Will

Head of Data Protection Unit

HEALTHCARE

Highly sensitive data (Art. 9), close supervision — every request counts. counts.



Lukas Bootz, LL.M.

Manager Corporate Data Protection

GLOBAL LOGISTICS

Many countries and entities, broad processes — quantity counts.



Björn Möller

CEO & Co-Founder

DATA RESPONSIBILITY PLATFORM

The DPMS is where KPI data is generated — and where benchmarking becomes possible.

Three sectors, one model: different target maturity levels are normal — the method stays the same.

caralegal

2.

Workshop

3 stations · 3 rounds · 3 questions



How the workshop works

3 stations

Each station covers one test question from the maturity model — with a host who stays there.

3 rounds

Every round brings a new question: Maturity Level → Risk → KPIs.

Build on each other

Teams rotate and continue on the poster the previous team left behind.

	Round 1 Maturity Level	Round 2 Risk	Round 3 KPIs
Team A	Station 1	Station 2	Station 3
Team B	Station 2	Station 3	Station 1
Team C	Station 3	Station 1	Station 2

After three rounds, every station poster carries all three answers — each from a different team.

Workshop

The three stations

1 STATION 1

Chapter 5 · Record of processing activities activities

Maintaining the RoPA

Art. 30 GDPR

The backbone of every DPMS

2 STATION 2

Chapter 9 · Data subject rights

Handling access requests

Art. 15 GDPR

Deadline-driven, highly visible, a frequent frequent trigger of complaints

3 STATION 3

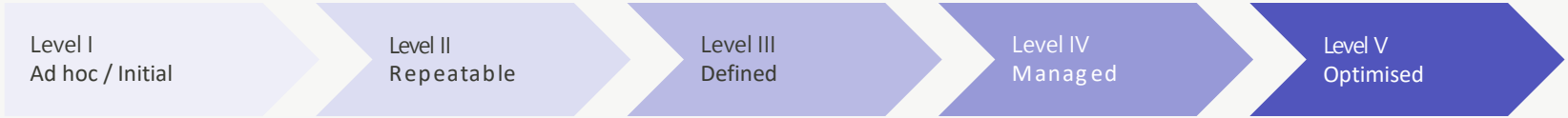
Chapter 10 · Incident management

Incident management process

Art. 33, 34 GDPR

72-hour clock and many interfaces (InfoSec, legal, comms

The five maturity levels



Level I	Level II	Level III	Level IV	Level V
Processes are informal, incomplete and applied inconsistently. Success depends on individual people.	Processes exist, but are not fully implemented or documented and may not cover all relevant aspects.	Suitable processes are fully fully implemented and documented, cover all relevant aspects and are reviewed regularly.	Implemented with above-average effort; the effectiveness of controls is reviewed and measured where sensible.	Regular reviews and feedback drive continuous improvement of the whole DPMS (PDCA cycle).

Levels build on each other: a level counts as reached only if the requirements of all lower levels are met as well. Not every topic has to has to reach level V — the target maturity depends on sector and risk appetite.

Question 1

ROUND 2 · 20 MIN

Translate the maturity levels into into your day-to-day work. What What does this mean / require in require in your organisation?

THINK ABOUT

- What would an auditor actually see at this level in your organisation?
- Which roles, tools, documents and routines are involved?
- What does it take to move up one level
- Corporate vs. local: what do expect as local translation of the corporate framework?

ON YOUR POSTER

1–3 concrete markers per level: “At level 2 I expect the DPMS to be accessible for all employees”

Workshop · Round 2

Question 2

ROUND 1 · 20 MIN

Assign a risk to each maturity level.

THINK ABOUT

- What happens if we stay at this level?
- Supervisory focus, fines, case law, media
- Impact on data subjects, hard deadlines

USE THE RISK SCORE SCALE

10	Immediate action	Clear GDPR violation, existential sanctions possible
8–9	Short-term action	Hardly defensible, high sanctions
6–7	Medium-term action	Borderline, investigation likely
4–5	Watch list	Minimal implementation, operational gaps gaps
1–3	No action needed	Largely met —controls prove it

ON YOUR POSTER One risk score (1–10) per level I–V, each with a one-one-line reason.

Workshop · Round 3

Question 3

ROUND 3 · 20 MIN

Define one or more KPIs for the different maturity levels.

THINK ABOUT

- Measurable: a number, a percentage or a time — no self-assessment
- Data source exists: DPM tool, ticket system, CRM/HR systems
- Threshold per level: which value separates III from IV?
- Cumulative: higher levels include the lower ones

ON YOUR POSTER

At least one KPI per level, with data source and threshold.

5.38 Maintaining the record of processing activities (RoPA)

Art. 30 GDPR · The company keeps a RoPA under Art. 30 GDPR that covers all processing of personal data, contains all mandatory particulars and is kept electronically.

	Level I	Level II	Level III	Level IV	Level V
What the model says says	No RoPA is kept — neither as controller nor, where applicable, as processor.	A rudimentary RoPA exists, but without uniform processes and reviews it may be incomplete, outdated or wrong and miss mandatory particulars.	RoPA covers all processing with with all particulars. Processes, Processes, roles and responsibilities are defined; processing may start only once once formal requirements are are met. Reviewed regularly.	Regular and ad-hoc effectiveness checks: risk-based based samples of RoPA entries entries are reviewed technically, technically, organisationally and and legally; findings are implemented.	Feedback from process owners owners drives continuous improvement; interfaces to other systems (e.g. ERM, IT asset management) are reviewed and optimised.
Q1 · Day-to-day					
Q2 · Risk score					
Q3 · KPI(s)					

9.55 Handling access requests

Art. 15 GDPR · Processes ensure that information is given only to the properly identified data subject, meets Art. 15(1) GDPR in content, respects the deadlines of Art. 12(3) deadlines of Art. 12(3) and allows a copy of the data (Art. 15(3)).

	Level I	Level II	Level III	Level IV	Level V
What the model says says	No dedicated processes; requests are answered sporadically, inconsistently and and possibly outside legal form form or deadlines.	Some processes exist but are not uniformly implemented or documented; requests via unexpected channels (e.g. social media) may be missed; no identity check.	Documented processes ensure ensure compliant answers in form, time and content to identified data subjects; all channels are monitored; staff staff have clear communication communication rules.	Regular effectiveness checks checks with business units ensure all relevant data about about the person is found and and included, and form, timing timing and content are met.	Continuous improvement from from feedback; wording tested tested for clarity; presentation presentation optimised, e.g. via via self-service access portals portals (user dashboards).
Q1 · Day-to-day					
Q2 · Risk score					
Q3 · KPI(s)					

10.62 Incident management process

Art. 33(1), 34(1) GDPR · A documented process, reviewed at least annually, defines responsibilities (incl. deputies), reporting lines and DPO involvement — from detection — from detection and risk assessment to notification (< 72 h) and post-incident review.

	Level I	Level II	Level III	Level IV	Level V
What the model says says	No dedicated process; incidents incidents are handled ad hoc hoc and inconsistently, possibly possibly outside the content and and time requirements of Art. Art. 33 GDPR.	Some processes exist but are not uniformly implemented or documented; timely notification of authority or data subjects is not ensured.	Documented processes: shared shared understanding of roles, roles, defined notification chains, uniform risk assessment, assessment, prepared incident incident plans, traceable notification decisions.	Effectiveness reviewed with business units, legal and communications to avoid wrong wrong or undocumented decisions; incident plans trained trained in simulations.	Continuous improvement: plans plans checked for clarity, checklists and incident logbooks, logbooks, contacts kept current, current, fallback channels if e.g. e.g. MS Teams is affected.
Q1 · Day-to-day					
Q2 · Risk score					
Q3 · KPI(s)					

Plenary · 10 min

What did we learn?

Risk

Where did teams' scores differ most — from each other and from the model? Why?

Day-to-day

Which level is a realistic target for for your organisation — and what what does it take to get there?

KPIs

Which KPI could you measure tomorrow? Which one would convince your management?

Next steps

We invite you

Guide to data protection maturity



caralegal blog article on maturity models

1. Understand

Practice test & insights

- Access to templates and KPIs
- Use experience from pilot projects
- Test the KPIs in your daily work

2. Try it out

Shape it actively

- Bring in feedback and ideas
- Co-create best practices
- Strengthen network and exchange

3. Get involved

Thank you!

Questions, feedback, KPI ideas? Talk to Daniela, Björn and Lukas — we will share the consolidated results with all participants.

caralegal