A. Checkliste für Mockup / DSGVO u. Datenschutz by Design

Arbeitsgrundlage für die MockUperin, damit der digitale Mockup datenschutzrechtlich korrekt gerahmt, nicht pflichtenauslösend, aber DSGVO-anschlussfähig gestaltet wird.

Adressat: Legal / Compliance / Revision (Trianel)

Kontext: AI Case Sprint – nicht produktiv, keine Echtdaten, keine Systemanbindung

I. Grundannahmen (müssen zwingend sichtbar sein im Mockup)

- Kein Einsatz personenbezogener Daten
- Keine Verarbeitung i.S.d. Art. 4 Nr. 2 DSGVO
- Keine Echtdaten, nur Platzhalter / Dummy-Daten
- Keine automatisierte Entscheidung mit Rechtswirkung (Art. 22 DSGVO)
- Kein Zugriff auf Trianel-Systeme

Hinweis im Mockup (Footer / Info-Box): „Dieser Mockup verarbeitet keine personenbezogenen Daten und entfaltet keine rechtliche oder operative Wirkung."

II. DSGVO-Bezug als Design-Rahmen (nicht als Pflicht)

Der Mockup soll zeigen, wie ein späterer Use Case DSGVO-konform denkbar wäre – ohne Pflichten auszulösen.

1. Rollenlogik (Art. 4 Nr. 7, 8 DSGVO – konzeptionell)

- Klare Visualisierung: Mensch (Legal/Compliance) = Entscheider, KI = unterstützendes Werkzeug
- Keine Darstellung: automatisierter Freigaben, automatisierter Bewertungen von Personen

Ziel: keine Nähe zu Art. 22 DSGVO

2. Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO)

- Mockup enthält: klar benannten fachlichen Zweck (z. B. Strukturierung, Vorprüfung, Dokumentation), keine offenen oder generischen Zwecke („Optimierung", „Analyse aller Daten")
- Zweck ist: eng, überprüfbar, rechtlich plausibel für Legal/Compliance.

3. Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO)

- Mockup zeigt nur die Datenkategorien, die zwingend erforderlich wären (hypothetisch)
  Beispiele (nur als Platzhalter):
  - Dokumententyp
  - Vorgangskategorie
  - Risikoklasse

- Keine Darstellung:
    - vollständiger Inhalte,
    - personenbezogener Attribute,
    - sensibler Daten (Art. 9 DSGVO).

4. Transparenz & Nachvollziehbarkeit (Art. 5 Abs. 1 lit. a, Art. 12 DSGVO)

- Mockup visualisiert:
    - Was die KI tut
    - Was sie nicht tut
    - Wo der Mensch entscheidet
- Empfohlen:
    - Info-Layer „So arbeitet das System“
    - einfache, nicht-technische Erläuterung

-> Transparenz als Governance-Element, nicht als Betroffeneninformation.

5. Zugriffs- und Rollenbeschränkung (Art. 32 DSGVO – konzeptionell)

- Mockup zeigt:
    - rollenbasierte Nutzung (z. B. Legal, Compliance, Revision)
    - keine „offenen“ oder anonymen Zugriffe
- Keine Darstellung:
    - externer Zugriffe,
    - Datenexporte,
    - Schnittstellen.

6. Protokollierung & Revisionsfähigkeit (Art. 5 Abs. 2 DSGVO – Accountability)

- Mockup enthält:
    - konzeptionelle Audit-Spur („wer hat was wann geprüft/freigegeben“)
    - keine Protokollierung realer Inhalte

Fokus: Rechenschaftsfähigkeit, nicht Überwachung.

III. Abgrenzung zu DSGVO-Pflichten (klar kommunizieren)

Der Mockup löst ausdrücklich nicht aus:

- Rechtsgrundlagenprüfung (Art. 6 DSGVO)
- Informationspflichten (Art. 13/14 DSGVO)
- DSFA (Art. 35 DSGVO)
- TOM-Implementierung (Art. 32 DSGVO)
- Auftragsverarbeitungsverträge (Art. 28 DSGVO)

Aber: Der Mockup soll sichtbar machen, wo diese Themen bei einer Umsetzung anzusetzen wären.

IV. Typische „No-Gos“ im Mockup (DSGVO-kritisch)

- Reale Namen, E-Mails, Vertragsinhalte
- „Automatische Risikobewertung von Personen“
- Scores, Rankings oder Ampeln mit Personenbezug
- Aussagen wie „KI entscheidet“, „automatisch freigegeben“
- Unklare Datenquellen („alle verfügbaren Daten“)

V. Kurzform für Melissa (1-Satz-Leitlinie)

„Der Mockup zeigt einen DSGVO-sensibel designten Zielprozess, ohne personenbezogene Daten zu verarbeiten oder Datenschutzpflichten auszulösen.“

B. Hintergrundmemo

I. Ausgangspunkt: Datenschutzrechtliche Relevanz des Mockups

1. Kein produktiver KI-Einsatz – keine Verarbeitung personenbezogener Daten

- Der im AI Case Sprint entwickelte digitale Mockup ist ausdrücklich:
  - nicht funktionsfähig,
  - nicht angebunden,
  - nicht entscheidend,
  - nicht datenverarbeitend,
  - Produktiv.

  Damit fehlt es tatbestandlich an einer „Verarbeitung personenbezogener Daten“ i.S.d. Art. 4 Nr. 2 DSGVO.

  Rechtsfolge: Für den Mockup selbst werden keine Datenschutzpflichten ausgelöst (keine Rechtsgrundlage, keine TOMs, keine Informationspflichten, keine DSFA).

  Gleichzeitig – und das ist für den Sprint entscheidend – dient der Mockup als antizipative Projektionsfläche für einen späteren KI-Use-Case, der typischerweise datenschutzrelevant wäre, insbesondere im Legal-/Compliance-Kontext (Dokumente, Vorgänge, Kommunikation, Prüfpfade).

2. DSGVO als strukturierender Referenzrahmen (nicht als Sperre)

Die Datenschutz-Grundverordnung ist – ähnlich wie die KI-VO – risikobasiert aufgebaut. Dies erlaubt es, Datenschutz frühzeitig als Design- und Governance-Thema mitzudenken, ohne operative Pflichten vorwegzunehmen.

Datenschutzrechtliche Grundspannung zwischen KI-Systemen und Datenschutzrecht:

- KI lebt von Datenumfang, Datenvielfalt, Wiederverwendung
- DSGVO basiert auf Zweckbindung, Datenminimierung, Transparenz (Art. 5 DSGVO)
- Diese Spannung wird ausdrücklich als Kernproblem moderner KI-Governance beschrieben

Konsequenz für den Sprint: Der Mockup muss nicht DSGVO-konform sein, sondern DSGVO-kompatibel denkbar.

3. Datenschutz by Design & by Default als Leitprinzip (Art. 25 DSGVO)

Funktion von Art. 25 DSGVO im Sprint-Kontext: Art. 25 DSGVO verpflichtet Verantwortliche, bereits bei der Konzeption geeignete technische und organisatorische Maßnahmen vorzusehen.

Für den Sprint bedeutet das:

- keine Umsetzungspflicht,
- aber Visualisierung von Datenschutz-Mechaniken im Mockup.

Der Mockup dient damit als didaktisches Instrument, um Management- und Fachentscheidungen vorzubereiten – exakt im Sinne des Sprints.

Typische Datenschutz-Design-Elemente im Mockup / Wiederkehrende Kernelemente, die bereits konzeptionell abgebildet werden können:

- Zweckklarheit (keine „Generallogik“)
- Rollenklärung (Mensch/KI)
- Datenkategorien (hypothetisch)
- Zugriffsbeschränkungen
- Protokollierung / Audit-Trails
- Abschalt- und Eskalationslogik

Diese Elemente werden ausdrücklich auch als Schnittstelle zwischen DSGVO und KI-VO beschrieben

4. Datenschutz & KI-VO: Keine Doppelregulierung, sondern Verzahnung

Parallele Risikologiken: DSGVO und KI-VO sind keine konkurrierenden, sondern komplementäre Regime.

DSGVO: Risiko für Rechte und Freiheiten natürlicher Personen

KI-VO: Risiko für Grundrechte, Sicherheit, gesellschaftliche Ordnung

Insbesondere wird hervorgehoben, dass DSFA (Art. 35 DSGVO) und Grundrechte-Folgenabschätzung (Art. 27 KI-VO) inhaltlich zusammen gedacht werden sollen.

Sprint-Mehrwert: Der Mockup kann zeigen, wo solche Assessments später andocken würden – ohne sie durchzuführen.

5. Spezifika des Legal-/Compliance-Use-Cases bei Trianel

5.1 Typische Datenschutzrisiken im Zielraum

Auch ohne Echtdaten ist klar, dass spätere KI-Use-Cases in Legal/Compliance typischerweise betreffen: interne Sachverhalte, Mitarbeiterdaten, Vertrags- und Kommunikationsdaten, ggf. sensible Konstellationen (Hinweise, Vorfälle, Prüfungen) Die Literatur betont, dass gerade indirekte Personenbezüge (Dokumente, Metadaten, Kontext) häufig unterschätzt werden.

5.2 KRITIS-Kontext als Verstärker, nicht als Sonderrecht

Für Trianel als KRITIS-Unternehmen gilt: DSGVO bleibt voll anwendbar, es treten keine Sonder-Datenschutzregeln, sondern erhöhte Erwartung an Governance. Datenschutz wird hier als Teil institutioneller Resilienz verstanden – nicht als Individualrechtsthema allein.

6. Abgrenzung: Mockup vs. späterer Einsatz (entscheidend)

6.1 Keine Datenschutzpflichten im Sprint

Solange:

- keine personenbezogenen Daten,
- keine reale Verarbeitung,
- keine operative Nutzung,

besteht keine Verantwortlichkeit i.S.d. DSGVO.

Das wird in der Literatur ausdrücklich unterstützt, sofern die Abgrenzung klar dokumentiert ist.

6.2 Dokumentationsfunktion des Hintergrundmemos

Das vorliegende Memo erfüllt selbst eine Schutzfunktion:

- Nachweis bewusster Nicht-Produktivität
- Nachweis frühzeitiger Datenschutzreflexion
- Abwehr von „Scope Creep“ (Schatten-IT)

7. Leitplanken für MockUperin (konkret)

Für diesen Punkt sollten im Mockup sichtbar, aber unverbindlich erscheinen:

- Keine Echtdaten (klar gekennzeichnet)
- Hypothetische Datenkategorien
- Visualisierte Zweckbindung
- Menschliche Freigabe vor jeder Wirkung
- Dokumentations- und Prüfpfade
- Hinweis: Datenschutz-Assessment erst bei Umsetzung

8. Zusammenfassung (Management-fähig)

- Der Mockup ist nicht DSGVO-pflichtig, aber DSGVO-sensibel konzipiert.
- Datenschutz by Design fungiert als Gestaltungsprinzip, nicht als regulatorische Last.
- DSGVO und KI-VO werden systematisch verzahnt, nicht vermischt.

Für Trianel als KRITIS-Akteur stärkt dies Entscheidungsqualität, Governance und Revisionssicherheit.