

GESAMT-RISIKOSTUFE ☐ Niedrig ☐ Moderat ☐ Kritisch

TREND GGÜ. VORQUARTAL ☐ besser ☐ stabil ☐ schlechter

MANAGEMENT-KURZFAZIT

1 Finanzen & Haftung

CFO · Legal

Drohen uns Bußgelder, persönliche Haftung oder ungedeckte Risiken in der Lieferkette?

RISIKOSTUFE ☐ niedrig ☐ moderat ☐ kritisch

TREND ☐ besser ☐ stabil ☐ schlechter

1.1 Einhaltung der gesetzlichen 72-Stunden-Meldefrist bei Datenpannen

% bei Vorfällen Ziel 100 %

Verspätete Meldungen lösen ein unmittelbares Bußgeld- und Haftungsrisiko gegenüber der Aufsichtsbehörde aus.

1.2 Abgesicherte und geprüfte kritische Lieferanten

% Vertrag % geprüft Ziel 100 % / ≥ 95 %

Bei einer Datenpanne eines ungesicherten Cloud-Anbieters haftet das Unternehmen voll im Außenverhältnis, ohne Regressschutz.

1.3 Prüfungsbereitschaft und Pflichtschulung der Mitarbeitenden

% Doku % geschult Ziel ≥ 95 %

Lücken führen bei Behördenprüfungen zur Beweislastumkehr und zum Vorwurf des Organisationsverschuldens.

2 Kunden & Umsatz

CEO · CRO

Gefährden Datenschutzlücken Enterprise-Abschlüsse, Kunden-Audits oder das Marktvertrauen?

RISIKOSTUFE ☐ niedrig ☐ moderat ☐ kritisch

TREND ☐ besser ☐ stabil ☐ schlechter

2.1 Konformität für Enterprise-Deals und Kunden-Audits

% konform Ziel ≥ 98 %

Fehlende Verträge mit Unterauftragnehmern oder veraltete Datenschutzhinweise blockieren Security- und Legal-Reviews im Vertrieb.

2.2 Fristgerechte Beantwortung von Kundenanfragen zu Auskunft und Löschung

% in ≤ 30 Tagen Ziel 100 %

Fristverspätungen bei Kunden- oder Ex-Mitarbeiteranfragen sind der häufigste Auslöser für Beschwerden bei Behörden.

2.3 Wiederholungsquote bei Datenschutzvorfällen

% wiederkehrend Ziel < 10 %

Wiederkehrende Vorfälle gleicher Ursache gefährden Bestandsverträge, zugesagte Service-Level und das Kundenvertrauen.

3 Produkt, KI & Technik

CTO · CISO

Sind Produkt-Releases blockiert oder bestehen kritische technische Risiken im Betrieb?

RISIKOSTUFE ☐ niedrig ☐ moderat ☐ kritisch

TREND ☐ besser ☐ stabil ☐ schlechter

3.1 Risikofreigabe für Hochrisiko-Produkte und KI vor dem Go-Live

% freigegeben Ziel 100 %

Launches ohne Freigabe riskieren einen Go-Live-Stopp, teuren Feature-Rückbau oder eine Betriebsuntersagung.

3.2 Überfällige kritische Schutzmaßnahmen

offen % Quote Ziel 0 überfällig

Bekannte hohe Risiken im Produktivbetrieb sind trotz abgelaufener Frist technisch noch nicht behoben.

3.3 Abdeckung der IT-Systeme und automatisierte Datenlöschung

% erfasst % Löschung Ziel ≥ 95 % / ≥ 90 %

Unbekannte Schatten-IT und ungelöschte Altbestände vervielfachen das Schadensausmaß bei einem Cyberangriff.

Erforderliche Entscheidungen der Geschäftsführung

Budgetfreigabe, Go-Live-Stopp oder bewusste Annahme eines Restrisikos

#	ENTSCHEIDUNGSVORLAGE / THEMA	RESSORT	KONSEQUENZ BEI NICHT-ENTSCHEIDUNG	ENTSCHEIDER	FRIST

Top-Geschäftsrisiken

im Klartext

#	RISIKO & GESCHÄFTLICHE AUSWIRKUNG	IMPACT: BUSSGELD / DEAL / PRODUKT-STOPP	VERANTWORTLICH & MASSNAHME

Behörden- & Kunden-Audit-Exposure

offene Verfahren und kritische Audits

#	VORGANG / ANFRAGE	AUFSICHTSBEHÖRDE / ENTERPRISE-KUNDE	TRAGWEITE & FRIST

Herleitung der Leit-Werte

Executive Brief (Seite 1) ← KPI-Dashboard (Seite 3)

BERICHTSZEITRAUM

STAND

ERSTELLT / DSB



DIMENSION	NR.	LEIT-WERT IM EXECUTIVE BRIEF	ZIEL	SPEISENDE KENNZAHLEN AUS DEM KPI-DASHBOARD (SEITE 3)
1 Finanzen & Haftung CFO · Legal	1.1	Einhaltung der gesetzlichen 72-Stunden-Meldefrist bei Datenpannen	100 %	5.1 72h-Meldequote Datenpannen
	1.2	Abgesicherte und geprüfte kritische Lieferanten	100 % / ≥ 95 %	3.1 AVV-Abdeckungsquote 3.2 Kritische Lieferanten-Prüfquote
	1.3	Prüfungsbereitschaft und Pflichtschulung der Mitarbeitenden	≥ 95 %	1.2 VVT-Vollständigkeitsquote 1.3 VVT-Aktualitätsquote 6.1 Pflichtschulungs- & Onboarding-Quote
2 Kunden & Umsatz CEO · CRO	2.1	Konformität für Enterprise-Deals und Kunden-Audits	≥ 98 %	1.4 Art. 13/14-Abdeckungsquote 3.1 AVV-Abdeckungsquote
	2.2	Fristgerechte Beantwortung von Kundenanfragen zu Auskunft und Löschung	100 %	4.1 DSAR-Fristeinhaltungsquote
	2.3	Wiederholungsquote bei Datenschutzvorfällen	< 10 %	5.2 Vorfalls-Wiederholungsquote
3 Produkt, KI & Technik CTO · CISO	3.1	Risikofreigabe für Hochrisiko-Produkte und KI vor dem Go-Live	100 %	2.2 DSFA-Abdeckungsquote
	3.2	Überfällige kritische Schutzmaßnahmen	0 überfällig	2.1 Überfällige Datenschutzrisiken 2.3 Überfällige DSFA-Maßnahmen
	3.3	Abdeckung der IT-Systeme und automatisierte Datenlöschung	≥ 95 % / ≥ 90 %	1.1 IT-Asset-VVT-Abdeckung 4.2 Umsetzungsgrad Löschkonzept

Wie die Risikostufe entsteht Nicht jede verfehlte Kennzahl ist ein Geschäftsrisiko – die 14 KPIs sind deshalb in zwei Gruppen geteilt

Kritisch – akutes Geschäftsrisiko

Die Risikostufe springt auf Kritisch, sobald einer dieser sieben Risiko-Treiber im roten Bereich liegt. Jeder davon hat eine unmittelbare rechtliche, vertragliche oder operative Folge.

- 2.1 Überfällige Datenschutzrisiken
- 2.2 DSFA-Abdeckungsquote
- 2.3 Überfällige DSFA-Maßnahmen
- 3.1 AVV-Abdeckungsquote
- 3.2 Kritische Lieferanten-Prüfquote
- 4.1 DSAR-Fristeinhaltungsquote
- 5.1 72h-Meldequote Datenpannen

Moderat – operativer Nachsteuerungsbedarf

Liegen nur diese Dokumentations-, Struktur- und Qualitätsindikatoren zurück, während alle Risiko-Treiber im Ziel sind, steht das Executive Brief maximal auf Moderat – nicht auf Kritisch.

- 1.1 IT-Asset-VVT-Abdeckung
- 1.2 VVT-Vollständigkeitsquote
- 1.3 VVT-Aktualitätsquote
- 1.4 Art. 13/14-Abdeckungsquote
- 4.2 Umsetzungsgrad Löschkonzept
- 5.2 Vorfalls-Wiederholungsquote
- 6.1 Pflichtschulungs- & Onboarding-Quote

Alle 14 Kennzahlen des Dashboards sind abgedeckt. KPI 3.1 speist zwei Leit-Werte, weil fehlende Verträge sowohl ein Haftungs- als auch ein Vertriebsrisiko auslösen.

Schwellenwerte und Berechnungsformeln je KPI auf Seite 3.

Datenschutz-KPI-Dashboard

Anlage zum Executive Brief · 6 MECE-Säulen · 14 Kennzahlen

BERICHTSZEITRAUM

STAND

ERSTELLT / DSB



SÄULE	NR.	KPI · DSGVO-BEZUG · BERECHNUNG	ZIEL	GRÜN	GELB	ROT	IST-WERT
1 Grundlagen & Transparenz VVT, White Spots & Informationspflichten	1.1	IT-Asset-VVT-Abdeckung Art. 30 Abs. 1 · Art. 5 Abs. 2 Aktive IT-Assets mit ≥ 1 VVT-Eintrag oder geprüfter „keine-pbD“-Bestätigung ÷ alle aktiven IT-Assets (CMDB / App-Katalog)	≥ 95 %	● ≥ 95 %	● 85-94 %	● < 85 %	
	1.2	VVT-Vollständigkeitsquote Art. 30 Abs. 1 lit. a-g · Art. 6 VVT-Einträge mit vollständigen Pflichtfeldern (inkl. valider Rechtsgrundlage & konkreter Löschfrist) ÷ alle aktiven Einträge	100 %	● 100 %	● 95-99 %	● < 95 %	
	1.3	VVT-Aktualitätsquote Art. 30 Abs. 1 · Art. 24 Abs. 1 VVT-Einträge mit dokumentiertem Review-Datum ≤ 12 Monate ÷ alle aktiven Einträge	≥ 95 %	● ≥ 95 %	● 85-94 %	● < 85 %	
	1.4	Art. 13/14-Abdeckungsquote Art. 12 Abs. 1 · Art. 13 · Art. 14 VVT-Einträge mit verknüpfter, aktueller Datenschutzinformation ÷ alle aktiven Einträge (exkl. dokumentierter Ausnahmen)	≥ 98 %	● ≥ 98 %	● 90-97 %	● < 90 %	
2 Risikomanagement & DSFA Risikoregister, Schwellenwertanalyse & TOM-Umsetzung	2.1	Überfällige Datenschutzrisiken Art. 24 Abs. 1 · Art. 32 Offene High/Critical-Risiken mit überschrittenem Zieldatum ÷ alle offenen High/Critical-Risiken · stets mit Absolutzahl ausweisen	0 %	● 0 %	● 1-5 %	● > 5 %	
	2.2	DSFA-Abdeckungsquote Art. 35 Abs. 1 Hochrisiko-Verarbeitungen mit abgeschlossener, freigegebener DSFA ÷ alle Verarbeitungen mit positivem Schwellenwert-Screening	100 %	● 100 %	● 90-99 %	● < 90 %	
	2.3	Überfällige DSFA-Maßnahmen Art. 35 Abs. 7 lit. d Aus DSFAs abgeleitete TOMs mit überschrittener Umsetzungsfrist ÷ alle offenen/fälligen Maßnahmen aktiver DSFAs	0 %	● 0 % · ≤ 2 % bei nachgel. Optimierungen	● 2-10 %	● > 10 %	
3 Drittparteien & Auftragsverarbeitung AVV, Drittlandtransfer & Lieferantenprüfung	3.1	AVV-Abdeckungsquote Art. 28 Abs. 3 · Art. 44-46 Aktive Auftragsverarbeiter mit beidseitig unterzeichnetem AVV (inkl. SCC/TIA) ÷ alle aktiven pbD-Dienstleister/SaaS-Assets	100 %	● 100 %	● 95-99 %	● < 95 %	
	3.2	Kritische Lieferanten-Prüfquote Art. 28 Abs. 1 & Abs. 3 lit. h Tier-1-Auftragsverarbeiter mit dokumentierter TOM-/Zertifikatsprüfung ≤ 12 Monate ÷ alle als kritisch eingestuften Auftragsverarbeiter	≥ 95 %	● ≥ 95 %	● 80-94 %	● < 80 %	
4 Betroffenenrechte & Löschung Operative Prozesse: DSAR-Fristen & Speicherbegrenzung	4.1	DSAR-Fristeinhaltsquote Art. 12 Abs. 3 i. V. m. Art. 15-22 Innerhalb der gesetzlichen Monatsfrist abgeschlossene DSARs ÷ alle im Berichtszeitraum fälligen/abgeschlossenen DSARs	100 %	● 100 %	● 98-99 %	● < 98 %	
	4.2	Umsetzungsgrad Löschkonzept Art. 5 Abs. 1 lit. e · Art. 17 · Art. 25 pbD-relevante IT-Assets mit aktiver automatischer oder protokollierter manueller Löschroutine ÷ alle pbD-relevanten IT-Assets	≥ 90 %	● ≥ 90 %	● 75-89 %	● < 75 %	
5 Datenschutzvorfälle Meldepflichten nach Art. 33 & Wirksamkeit der Abhilfe	5.1	72h-Meldequote Datenpannen Art. 33 Abs. 1 Meldepflichtige Vorfälle, binnen ≤ 72 h an die Aufsichtsbehörde gemeldet ÷ alle meldepflichtigen Vorfälle im Berichtszeitraum	100 %	● 100 %	● kein Gelb – Frist ist binär	● < 100 %	
	5.2	Vorfalls-Wiederholungsquote Art. 32 Abs. 1 · Art. 33 Abs. 3 lit. d Vorfälle, deren Root Cause im Vorquartal bereits ≥ 1x auftrat ÷ alle registrierten Datenschutzvorfälle (inkl. nicht-meldepflichtiger)	< 10 %	● < 10 %	● 10-20 %	● > 20 %	
6 Schulungen Sensibilisierung, Schulung & Onboarding	6.1	Pflichtschulungs- & Onboarding-Quote Art. 39 Abs. 1 lit. b · Art. 32 Abs. 4 Aktive Mitarbeitende mit gültigem Schulungszertifikat (Turnus ≤ 12/24 Mon.; Neueintritte ≤ 30 Tage) ÷ alle Schulungspflichtigen	≥ 95 %	● ≥ 95 %	● 85-94 %	● < 85 %	

● Grün Ziel erreicht | ● Gelb Nachsteuerung durch den Owner, Frist setzen | ● Rot Eskalation an die Geschäftsführung / Go-Live-Stopp | Steckbriefe mit Typ, Frequenz, Owner und Datenquelle separat

Wie berichtsfähig ist Ihr Datenschutz?

Readiness-Check für das 14-KPI-Reporting

ORGANISATION

STAND

AUSGEFÜLLT DURCH



#	KPI-BEZUG	FRAGE	3 PUNKTE	2 PUNKTE	1 PUNKT	0 PUNKTE
1	1.1 IT-Asset-VVT-Abdeckung	Können Sie sagen, für welchen Anteil Ihrer aktiven IT-Systeme mindestens eine Verarbeitung im VVT hinterlegt ist (oder eine „keine-pbD“-Bestätigung vorliegt)?	☐ sofort, systemisch verknüpft	☐ mit manuellem Listenabgleich	☐ nur für einzelne Systeme	☐ nein, kein Abgleich möglich
2	1.2 VVT-Vollständigkeit	Wissen Sie, bei welchem Anteil Ihrer VVT-Einträge alle Pflichtangaben – insbesondere Rechtsgrundlage und konkrete Löschfrist – vollständig gepflegt sind?	☐ sofort, automatisch prüfbar	☐ durch manuelle Durchsicht	☐ nur stichprobenartig	☐ unbekannt
3	1.3 VVT-Aktualität	Können Sie auswerten, welcher Anteil Ihres Verarbeitungsverzeichnisses in den letzten 12 Monaten nachweislich geprüft wurde?	☐ ja, über Prüfdatum im System	☐ in den meisten Bereichen	☐ nur in einzelnen Bereichen	☐ unbekannt
4	1.4 Art. 13/14-Abdeckung	Ist für jede Verarbeitung im VVT hinterlegt, über welche Datenschutzinformation (Art. 13/14) Betroffene informiert werden und ob diese aktuell ist?	☐ ja, direkt mit VVT verknüpft	☐ über separate Übersicht	☐ nur für Haupt-Touchpoints	☐ nein
5	2.1 Überfällige DS-Risiken	Haben Sie ein zentrales Datenschutz-Risikoregister und sehen sofort, bei welchem Anteil der hohen/kritischen Risiken die Behandlungsfrist überschritten ist?	☐ ja, zentral mit Fristen	☐ verteilt in Einzellisten	☐ nur auf Nachfrage	☐ kein zentrales Register
6	2.2 DSFA-Abdeckung	Wissen Sie genau, welche Ihrer Verarbeitungen eine DSFA benötigen (Schwellenwertanalyse) und für welchen Anteil diese abgeschlossen vorliegt?	☐ ja, vollständig erfasst	☐ für die meisten	☐ für einzelne	☐ nein
7	2.3 Überfällige DSFA-Maßnahmen	Werden Maßnahmen aus DSFAs mit Fristen nachverfolgt, sodass Sie jederzeit die Quote überfälliger Maßnahmen berichten können?	☐ ja, laufend im System/Ticket	☐ manuell in den Dokumenten	☐ nur auf Nachfrage	☐ kein Tracking nach DSFA
8	3.1 AVV-Abdeckung	Können Sie sagen, für welchen Anteil Ihrer relevanten Dienstleister und Cloud-Tools ein gültiger Vertrag nach Art. 28 (inkl. Drittland-Absicherung) vorliegt?	☐ ja, auf Knopfdruck	☐ mit etwas Suche	☐ grob geschätzt	☐ nein, Gesamtzahl unklar
9	3.2 Krit. Lieferanten-Prüfquote	Ist erfasst, welche Auftragsverarbeiter kritisch (High-Risk) sind und bei welchem Anteil in den letzten 12 Monaten TOMs oder Zertifikate geprüft wurden?	☐ ja, mit Prüfdatum erfasst	☐ Nachweise liegen verteilt vor	☐ nur beim Onboarding geprüft	☐ nein
10	4.1 DSAR-Fristeinhaltung	Messen Sie, welcher Anteil aller Betroffenenanfragen (Auskunft, Löschung etc.) innerhalb der gesetzlichen Frist von einem Monat abgeschlossen wurde?	☐ ja, laufend mit Zeitstempel	☐ einmal im Jahr / manuell	☐ auf Nachfrage	☐ nein
11	4.2 Umsetzung Löschkonzept	Wissen Sie, in welchem Anteil Ihrer relevanten IT-Systeme die definierten Löschfristen tatsächlich technisch oder protokolliert umgesetzt sind?	☐ ja, je System dokumentiert	☐ für Kernsysteme bekannt	☐ nur Konzept auf Papier	☐ unbekannt
12	5.1 72h-Meldequote	Ist bei jedem Datenschutzvorfall mit Zeitstempel dokumentiert, wann er bekannt wurde, ob er meldepflichtig war und ob die 72-Stunden-Frist gehalten wurde?	☐ ja, bei jedem mit Zeitstempel	☐ bei den meisten	☐ nur bei gemeldeten	☐ nein
13	5.2 Wiederholungsquote Vorfälle	Erfassen Sie bei Datenschutzvorfällen die Grundursache (Root Cause) strukturiert, sodass Sie den Anteil wiederkehrender Fehlerursachen auswerten können?	☐ ja, nach Kategorien auswertbar	☐ als Freitext nachlesbar	☐ nur gefühlt bekannt	☐ nein
14	6.1 Schulungs- & Onboarding-Quote	Kennen Sie die aktuelle Schulungsquote (inkl. Neueintritte binnen 30 Tagen) im Verhältnis zur Gesamtzahl aller aktiven Beschäftigten?	☐ ja, aktuell je Bereich	☐ für die Organisation gesamt	☐ nur Teilnehmerzahlen ohne Quote	☐ nein

Auswertung von maximal 42 Punkten · je Frage genau ein Feld ankreuzen

0–14 Punkte

Anlassbezogen (Blindflug)

Datenschutz wird sichtbar, wenn etwas passiert. Für Quoten fehlt meist der Nenner – die Gesamtzahl der IT-Systeme, Lieferanten oder Beschäftigten.

Erster Schritt: Grundgesamtheiten für die Fragen 1 (IT-Assets), 8 (AVVs), 10 (DSARs) und 12 (Vorfälle) einmal sauber erfassen – auch wenn die Werte anfangs rot sind.

15–28 Punkte

Im Aufbau (Insel-Daten)

Vieles ist vorhanden, liegt aber verteilt in Dokumenten, E-Mails und Abteilungslisten. Quoten lassen sich nur über manuelle Listenabgleiche berechnen.

Erster Schritt: Eindeutige Verknüpfungen (IDs) zwischen VVT, IT-Asset-Katalog und Vertragsliste herstellen und Fälligkeitsdaten als Pflichtfelder führen.

29–42 Punkte

Steuerbar (berichtsfähig)

Alle 6 Säulen sind belastbar berichtsfähig. Zähler und Nenner sind strukturiert verknüpft.

Nächster Schritt: Erhebungsaufwand weiter automatisieren und das Reporting nach Zielgruppen takten – Quartals-Board-Report gegenüber Monats-Operations-Check.

Geprüft wird je KPI, ob **Nenner** (Grundgesamtheit), **Zähler** und die **Systemverknüpfung** vorliegen – also ob sich die Kennzahl ohne tagelange Handarbeit valide erheben lässt.

Regnify · Datenschutz-KPI-Framework
Vorlage v1.6 · 22.10.2026 · Seite 4 von 4