QUALIFIZIERUNGSGUTACHTEN (MUSTER)

Fiktives Beispiel. Firma, Befunde und Nachweise sind frei erfunden und dienen ausschließlich der Demonstration der Methode.

Gutachten-Nr.: MZG-2026-014 (Beispiel)
Datum: 21.09.2026
Erstellt durch: Jan Richter, Qualifizierungsexperte für IT-Sicherheit (GxP-Methodik)
Auftraggeber: MUSTERWERK GROUP (fiktiv) – globaler Industriekonzern, EU-Tochtergesellschaften in DE/CZ, Umsatzklasse 500 Mio. EUR+

Geltungsbereich: EU-IT-Instanz der MUSTERWERK GROUP, 180 Mitarbeitende, Hosting Azure EU, 4 kritische Anwendungen, 11 Auftragsverarbeitungsverträge mit Auftragsverarbeitern.
Anforderungsquellen: DSGVO Art. 28, 32, 33; NIS2UmsuCG § 30, § 33, § 38, § 39; BSI-Grundschutz-Bausteine APP / CLA / ORP.
Methode: Qualifizierung in drei Stufen je Maßnahme:

- I – Installation: Ist die Maßnahme korrekt eingerichtet (Konfiguration, Policy, Rollen)?
- O – Betrieb: Läuft sie dauerhaft und nachweisbar (Logs, Reports, Wiederholprüfungen)?
- P – Leistung: Hält sie unter Druck stand (Test, Last, Angriffs-/Ausfallszenario)?

Evidenzklassen (Nachweismethode je Befund ausgewiesen):

- SELBST-ERHOBEN: Roh-Evidenz vom Auftraggeber über versionierte, checksummte Qualifizierungs-Protokolle selbst erhoben (Skript-Rohoutput, keine Bewertungen), vom Gutachter methodisch geprüft.
- LIVE-VERFOLGT: Leistungstest unter Aufsicht des Gutachters in gemeinsamer Sitzung ausgeführt.
- NICHT VERIFIZIERBAR: Evidenz nicht nachvollziehbar. Befund wird abgewertet, nicht übernommen.

---

1. Gesamturteil

Kennzahl	Wert
Geprüfte Maßnahmen	20
Bestanden (I+O+P)	6
Teilbestanden (I ok, O oder P fehlend)	9
Nicht bestanden	5
Nachweisreife gegenüber Aufsicht	eingeschränkt gegeben

Kernaussage: Die Organisation hat eine gute Papierlage. 15 von 20 Maßnahmen sind dokumentiert. Nur 6 von 20 lassen sich heute mit Ausführungsnachweis gegen eine Prüfung verteidigen. Genau diese Lücke zwischen dokumentierter und gelebter Maßnahme ist der Sanktionstatbestand der vergangenen Verfahren (CNIL/France Travail 01/2026: im DPIA identifizierte, aber nicht wirksam umgesetzte Maßnahmen, 5 Mio. EUR; ANSPDCP/Renault 03/2026: angemessene Maßnahmen und Auftragnehmersteuerung nicht nachgewiesen; UODO/Polen 2025: erkanntes Risiko ohne Umsetzung der Gegenmaßnahme).

---

2. exemplarische Befunde (Auszug, 5 von 20)

B1 – MFA auf Verwaltungs- und Fernzugängen

• Quelle: DSGVO Art. 32 Abs. 1 lit. b; NIS2UmsuCG § 30 (Zugriffskontrolle)

• I – Installation: RICHTIG. MFA-Richtlinie vorhanden, Azure Conditional Access konfiguriert.

• O – Betrieb: FEHLERHAFT. Nachweisbare Durchsetzung nur für VPN und Mail. Admin-Konsolen und HR-System greifen über Legacy-Authentifizierung ohne MFA (Export der Login-Logs, 30 Tage, 1.214 MFA-freie Admin-Logins).

• P – Leistung: NICHT GEPRÜFT. Kein Test, ob die Richtlinie bei Ausschluss des zweiten Faktors wirklich sperrt.

• Bewertung: Teilbestanden. Auf dem Papier steht MFA überall, die Ausführung sagt: nicht bei privilegierten Konten. Das ist das exakte Muster der CNIL- und EDPB-kritisierten "Partial MFA"-Fälle.

• Nachweis für Prüfung heute möglich: Nein.

B2 – Backup und Wiederanlauffähigkeit

• Quelle: DSGVO Art. 32 Abs. 1 lit. c (Wiederherstellbarkeit); NIS2UmsuCG § 30 (Wiederherstellung)

• I: RICHTIG. Immutable Backups konfiguriert, Zeitplan dokumentiert.

• O: BESTANDEN. Tägliche Job-Reports vorhanden und archiviert.

• P: NICHT BESTANDEN. Letzter dokumentierter Restore-Test: vor 19 Monaten, eine Anwendung von vieren.

• Bewertung: Teilbestanden. Art. 32 verlangt die Fähigkeit zur Wiederherstellung, nicht den Backup-Job. Ungetestete Backups werden in Verfahren als mangelhaft gewertet (EDPB-Breach-Beispiele, UODO-Rechtsprechung: Sicherheit muss im Versagensszenario funktionieren).

• Nachweis heute möglich: Teilweise (Installation/Betrieb), nicht für Leistung.

B3 – Auftragsverarbeiter-Steuerung (Art. 28)

• Quelle: DSGVO Art. 28 Abs. 1; NIS2UmsuCG § 30 (Lieferantensteuerung)

• I: RICHTIG. 11 AVV vorhanden, Kontrollklauseln enthalten.

• O: NICHT BESTANDEN. Kein Nachweis einer einzigen Ausübung der Audit-Rechte in 3 Jahren (Art. 28 Abs. 3 lit. h). Risikobewertung der AV nur bei Vertragsschluss, keine Periodik.

• P: NICHT BESTANDEN. Keine guarantees-Prüfung (Subprocessor-Listen, Logzugriff, Leak-Tests) bei 8 von 11 AV.

• Bewertung: Nicht bestanden. Kontinuierliche Prüfungspflicht: jahrelange Zusammenarbeit ohne Prüfung gilt als keine hinreichende Garantie (UODO 2025, EDPB ETL 07/2020 Rn. 99).

• Nachweis heute möglich: Nein.

B4 – Registrierung und BSI-Pflichten

• Quelle: NIS2UmsuCG § 33, § 38, § 39

• I: RICHTIG. Registrierung im BSI-Portal erfolgt (Nachweis: Portalbestätigung).

• O: FEHLERHAFT. Prozess zur Aktualisierung geänderter Angaben (2 Wochen, § 33 Abs. 5) existiert nicht. IP-Bereichsänderung vom Juni wurde nach 31 Tagen aktualisiert.

• P: OFFEN. Schulungsnachweis Geschäftsleitung vorhanden, aber kein Überwachungsbericht der Umsetzung (Meldeprozess nie geprobt; 24h/72h/1-Monat-Fristen nie durchgespielt).

• Bewertung: Teilbestanden. Ab 2028 Nachweispflicht § 39; der jetzige Zustand besteht einen anlasslosen Check der Leitungspflichten (Art. 34 RL, § 38) nicht.

• Nachweis heute möglich: Für Registrierung ja, für Leitungsüberwachung nein.

B5 – Verschlüsselung mobiler Geräte

- Quelle: DSGVO Art. 25, 32 Abs. 1 lit. a
- I: RICHTIG. Intune-Richtlinie BitLocker, Ausnahmegruppe "Feldtechnik" (9 Geräte).
- O: NICHT BESTANDEN. Ausnahme ohne Ausgleich: kein technischer Ersatz, keine Kompensation, keine befristete Auslaufliste, keine Quartalsprüfung.
- P: – (wegen O-Fehler nicht erreicht)
- Bewertung: Nicht bestanden. Risiko erkannt, Maßnahme auf Papier, Umsetzung mit Dauerlücke: Das ist der Anlastungshebel, der in Verfahren grobe Fahrlässigkeit begründet, weil Kenntnis des Risikos belegt ist (UODO 2025: "Erkenntnis des Risikos ohne angemessene Entlastung wiegt schwerer als das Fehlen einer Analyse").
- Nachweis heute möglich: Nein.

---

3. Priorisierter Nacharbeiten-Plan (Auszug)

Prio	Maßnahme	Aufwand	Nachweisziel
1	MFA auf allen Privileged-Systemen, Legacy-Auth ab	2–3 Wochen	O+P: 30-Tage-Log + Sperrtest
1	Restore-Test aller 4 Anwendungen, quartalsweise	1 Woche je Zyklus	O+P: Restore-Report + Sign-off
2	AV-Auditzyklus: 11 AVV, risikobasiert, Start mit Zahlungsverkehr	Audit-Slot je AVV	O: Audit-Berichte, Subprocessor-Nachweise
2	Feldtechnik: Intune-Ausnahme auflösen (Exchange On-Prem Client), Auslaufliste	2 Wochen	I+O: Konfig-Export, Quartalsevidenz
3	Meldeprozess-Probe (24h/72h) mit Leitung	1 Tag	O+P: Übungsnachweis § 32/§ 38

4. Übergabe und Gültigkeit

Dieses Gutachten übergibt 20 Einzelbewertungen, 5 fertige Nachweispakete und den Maßnahmenplan. Gültigkeit: 12 Monate oder bis zum ersten Revalidierungs-Auslöser (neuer Cloud-Provider, neue kritische Systeme, Sicherheitsvorfall, wesentliche Änderung der AV-Landschaft). Nach Ablauf oder Auslöser entscheidet der Auftraggeber neu, ohne Bindung, ohne Mindestlaufzeit.

Rechtlicher Hinweis: Fachliche Qualifizierung durch einen unabhängigen Experten. Keine Zertifizierung, keine behördliche Auditierung, keine Rechtsberatung.
