URTEILSBESPRECHUNG · DATENSCHUTZRECHT · AŞHOFF.LEGAL

DPIA zu Google Cloud Platform: Niederländisches Justizministerium identifiziert 11 Datenschutzrisiken — und warnt vor US-Risiken

Analyse der öffentlichen DPIA des SLM Rijk vom 11. Juni 2026 (Version 1.3)

Auftraggeber	Ersteller	Datum	Kategorie
Niederl. Justizministerium (SLM Rijk)	Privacy Company (Nas/Terra)	11. Juni 2026, V1.3	DPIA — Cloud-Datenschutz

Auf einen Blick: 11 niedrige Datenschutzrisiken bei GCP — formal ein gutes Ergebnis. Im Detail: Google handelt in 3 Konstellationen als unzulässiger eigenständiger Verantwortlicher, Diagnostic Data sind kaum kontrollierbar, und die DPIA warnt ausdrücklich vor geopolitischen US-Risiken für die Datenverfügbarkeit. Originaldokument: open.overheid.nl/details/3ef89ab7-ccaf-4753-8335-9f226eaa9c24

Die fünf Datenkategorien — und wo Google die Kontrolle verliert

Die DPIA unterscheidet 5 Kategorien, die Google mit nur 2 anerkennt (Customer / Service Data). Die Prüfer halten diese Zweiteilung für unzureichend und intransparent:

→ Content Data: vom Kunden hochgeladene Inhalte

→ Account Data: Daten des Admin-Accounts

→ Diagnostic Data: Telemetry, Server Logs, Sicherheitslogs

→ Support Data: bei Support-Anfragen

→ Website Data: Cloud Console und Dokumentationswebsite

Google als unzulässiger eigenständiger Verantwortlicher

In drei Konstellationen handelt Google als eigenständiger Datenverantwortlicher — der AVV greift nicht, Weisungsrechte entfallen:

→ Account Data außerhalb des GCP-Kontexts (fließen in Googles allgemeines System)

→ Website Data der Admin Console (console.cloud.google.com)

→ Daten von öffentlichen GCP-Seiten, die Admins zwingend besuchen

> Praxisrelevanz: Das Unternehmen/die Behörde kann Betroffene über diese Verarbeitungen nicht informieren und sie nicht kontrollieren — obwohl es als Verantwortlicher gegenüber den Betroffenen haftet.

Die 11 Risiken — die wichtigsten im Überblick

Risiko 1 — Telemetry Data: Diagnosedaten vom Admin-Gerät werden übertragen. Empfehlung: pseudonyme Admin-Accounts.

Risiko 2 — Betroffenenrechte: Auskunft nur über Support-Ticket möglich, nicht direkt.

Risiko 7 — Drittlandübermittlung Account/Diagnostic/Website Data: Keine wirksamen Schutzmaßnahmen möglich. Google hat keine Maßnahmen angekündigt. [CONFIDENTIAL]

Risiko 9 — Feedback-Funktion: Kann Content Data enthalten. Google bietet keine zentrale Deaktivierung an.

Die geopolitische Warnung: US-Risiken für Datenverfügbarkeit

> Zitat aus der DPIA (Summary, S. 9): "Government organisations also have to take the risk into account of sudden unavailability of personal data due to US American policy measures that may force Google to stop providing the services. Government organisations are advised to have back-ups available outside of the tested GCP services for critical processes for which unavailability is unacceptable."

Diese Warnung ist keine akademische Übung — sie ist eine direkte Aufforderung zur Business-Continuity-Planung außerhalb von GCP.

EU-US Data Privacy Framework: Stabil — aber vorbereitet sein

Aktuell trägt das DPF die Datentransfers zu Google. Für den Fall einer Annullierung (wie bei Privacy Shield 2020):

→ DTIA (Data Transfer Impact Assessment) durchführen — inkl. Weitertransfers aus den USA

→ Verschlüsselung mit eigenen Schlüsseln (Cloud EKM) für Content Data — möglich und empfohlen

→ Account/Diagnostic/Website Data: keine wirksamen Verschlüsselungsmaßnahmen möglich

→ SCC können dann nicht mehr als Auffangregelung dienen

Was bedeutet das für deutsche Unternehmen?

→ AVV allein reicht nicht: Google-Eigenverantwortlichkeit korrekt in Datenschutzerklärung und Verarbeitungsverzeichnis abbilden

→ Diagnostic Data adressieren: pseudonyme Admin-Accounts als pragmatischste Maßnahme

→ DPF-Risiko einpreisen: Cloud EKM für Content Data als Standard einführen

→ Business-Continuity: kritische Prozesse müssen Backup außerhalb GCP haben

Das Originaldokument (142 Seiten, englisch) ist abrufbar unter:
open.overheid.nl/details/3ef89ab7-ccaf-4753-8335-9f226eaa9c24