CPQI Security-Konzept

Cisco Partner Quality Index – Datenschutz, Sicherheitsarchitektur & Fraud-Detection

Stand: 2026-02-14 | Dr. Ralf Korell

Management Summary

Das CPQI-System erhebt qualitative Bewertungen von Cisco-Vertriebspartnern durch interne Mitarbeiter. Die Erhebung ist **anonym** – es werden weder Namen noch E-Mail-Adressen erfasst. Dieses Dokument beschreibt die technischen und organisatorischen Maßnahmen (TOM) zum Schutz der Teilnehmerdaten sowie die methodischen Grundlagen der Qualitätssicherung.

Kernprinzipien:

Prinzip	Umsetzung
Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO)	Keine Namen, keine E-Mail-Adressen, keine Cookies. IP-Adressen werden ausschließlich als Hash gespeichert.
Privacy by Design (Art. 25 DSGVO)	IP-Hashing mit SHA-256 und Salt, Anonymisierung der Apache-Logs, DB-Credentials außerhalb des Webroots.
Sicherheit der Verarbeitung (Art. 32 DSGVO)	HTTPS-Verschlüsselung, CSRF-Schutz, Session-basierte Authentifizierung, Security-Headers.
Fraud-Detection	Mehrstufige Qualitätssicherung: IP-Duplikate, Straightlining-Erkennung, Severity-Klassifikation.

Risikobewertung: Das Gesamtrisiko wird als **gering** eingestuft. Die erhobenen Daten (anonyme Bewertungen auf einer 1-5-Skala) haben keinen direkten Personenbezug. Die IP-Adresse als einziges potenziell personenbezogenes Datum wird durch SHA-256-Hashing mit Salt wirksam pseudonymisiert. Eine Reidentifizierung einzelner Teilnehmer ist für den Betreiber praktisch nicht möglich.

---

1. Rechtsrahmen

1.1 Anwendbare Vorschriften

Das CPQI-System unterliegt als Webanwendung mit potenzieller Verarbeitung personenbezogener Daten der **Datenschutz-Grundverordnung (DSGVO)**. Relevante Normen:

Norm	Inhalt	Relevanz für CPQI
Art. 5 Abs. 1 lit. c	Datenminimierung	Nur die für die IPA-Analyse zwingend erforderlichen Daten erheben [1]
Art. 25	Privacy by Design und by Default	Datenschutz bereits in der Systemarchitektur verankern [2]
Art. 32	Sicherheit der Verarbeitung	Technische und organisatorische Maßnahmen nach Stand der Technik [3]
Erwägungsgrund 26	Anonyme Daten	DSGVO gilt nicht für wirksam anonymisierte Daten [4]

Die **EDPB Guidelines 4/2019** zu Art. 25 konkretisieren: Data Protection by Design gilt für alle Verantwortlichen unabhängig von der Organisationsgröße und muss sowohl vor als auch während der Verarbeitung implementiert werden [5].

1.2 Personenbezug von IP-Adressen

Dynamische IP-Adressen können personenbezogene Daten darstellen. Der **EuGH** hat in der Rechtssache **Breyer (C-582/14)** entschieden, dass der „relative Ansatz" gilt: Maßgeblich sind die konkreten Mittel des Verantwortlichen zur Reidentifizierung, nicht die abstrakte Möglichkeit [6].

Das **EuG** hat in der Rechtssache **SRB (T-557/20)** bestätigt: Pseudonymisierte Daten, bei denen der Empfänger nicht über die Zusatzinformationen zur Reidentifizierung verfügt, sind für diesen **anonyme Daten** [7].

Einordnung für CPQI: Der CPQI-Betreiber speichert keine Klartext-IPs und verfügt über keine Zuordnungstabelle Hash → IP. Der Salt liegt außerhalb der Anwendung. Eine Reidentifizierung wäre nur über den Internetzugangsanbieter möglich – ein Weg, der dem Betreiber nicht zur Verfügung steht. Das **BfDI-Positionspapier zur Anonymisierung** bestätigt: Absolute Anonymisierung ist nicht erforderlich; es genügt, dass die Reidentifizierung „praktisch nicht durchführbar" ist [8].

1.3 Cookie-freie Architektur

Das CPQI setzt im öffentlichen Bereich (Erhebungs-Wizard) **keine Cookies**. Die **DSK-Orientierungshilfe Telemedien** (Version 1.1, 2022) stellt klar: Automatisch übermittelte Daten (IP-Adresse, User-Agent) fallen nicht unter § 25 TTDSG (kein Zugriff auf das Endgerät), unterliegen aber der DSGVO-Verarbeitungspflicht [9]. Da die IP-Adresse sofort gehasht und der Klartext verworfen wird, ist diese Pflicht erfüllt.

---

2. Technische Sicherheitsmaßnahmen

Die Sicherheitsarchitektur folgt dem Prinzip **Defense in Depth**: Mehrere unabhängige Schutzschichten, sodass der Ausfall einer einzelnen Maßnahme nicht zu einem vollständigen Schutzversagen führt.

2.1 IP-Anonymisierung (Anwendungsebene)

Aspekt	Umsetzung
Verfahren	SHA-256 Hash mit Salt
Speicherung	`participants.ip_hash` (VARCHAR 64)
Salt-Speicherort	Konfigurationsdatei außerhalb des Webroots
Zweck	Duplikat-Erkennung ohne Rückverfolgbarkeit

Ablauf:

```
hash('sha256', IP_HASH_SALT . $_SERVER['REMOTE_ADDR'])
```

SHA-256 ist nach **BSI TR-02102-1** (Version 2026-01) ein empfohlenes Hash-Verfahren [10]. Der Salt verhindert Rainbow-Table-Angriffe. Da der IPv4-Adressraum endlich ist (~4,3 Mrd. Adressen), wäre ohne Salt ein vollständiger Brute-Force-Angriff theoretisch möglich. Mit Salt wird dieser Angriff auf den Besitz des Salt-Wertes konditioniert.

Der DB-Index `idx_participants_ip_hash` ermöglicht effiziente Duplikat-Suchen innerhalb einer Survey.

2.2 IP-Anonymisierung (Infrastrukturebene)

Apache-Access-Logs werden über **Piped Logging** anonymisiert:

Maßnahme	Konfiguration
Verfahren	Letztes Oktett wird auf 0 gesetzt
Beispiel	`203.0.113.47` → `203.0.113.0`
Script	Piped-Logging-Script (außerhalb des Webroots)
Log-Retention	7 Tage (via logrotate)

Damit ist auch auf Infrastrukturebene keine vollständige IP-Adresse persistent gespeichert.

Hinweis: Das BSI empfiehlt in **OPS.1.1.5** (Protokollierung) grundsätzlich die Erfassung sicherheitsrelevanter Ereignisse [11]. Die Anonymisierung des letzten Oktetts stellt einen bewussten Kompromiss zwischen Protokollierungspflicht und Datenschutz dar: Netzwerk-Segment-Analysen bleiben möglich, individuelle Zuordnung nicht.

2.3 Server-Härtung

Maßnahme	Umsetzung
HTTPS	TLS-Verschlüsselung für externen Zugriff (Let's Encrypt)
Security-Headers	`X-Frame-Options: DENY`, `X-Content-Type-Options: nosniff`
.htaccess	Blockiert Zugriff auf `.git`, `*.sql`, `README.md`, Konfigurationsdateien
DB-Credentials	Außerhalb des Webroots (`/etc/partneranalyse/db_connect.php`)
PHP-Fehler	`display_errors = Off` in Produktion

Die TLS-Konfiguration folgt den Empfehlungen der **BSI TR-02102-2** [10]. Die `.htaccess`-Regeln adressieren die OWASP-Risikokategorie **A05:2021 Security Misconfiguration** [12].

2.4 Authentifizierung & Session-Management

Der Analyse-Bereich (`score_analyse.html`, `survey_admin.html`) ist passwortgeschützt:

Aspekt	Umsetzung

Aspekt	Umsetzung
Login	Session-basiert gegen `admin_users`-Tabelle
Passwort-Speicherung	`password_hash()` mit `PASSWORD_DEFAULT` (bcrypt)
Session-Cookies	`HttpOnly`, `SameSite=Lax`
Steuerung	Globaler Schalter `USE_LOGIN` in `php/common.php`

Das **OWASP Session Management Cheat Sheet** empfiehlt `HttpOnly` als Pflicht-Attribut gegen XSS-basierte Session-Übernahme und `SameSite` gegen Cross-Origin-Informationsabfluss [13].

2.5 CSRF-Schutz

Der Survey-Wizard ist durch **CSRF-Tokens** gegen Cross-Site Request Forgery geschützt:

Aspekt	Umsetzung
Verfahren	Synchronizer Token Pattern (OWASP-Empfehlung [14])
Generierung	Beim Laden der Seite (serverseitig, `protect.php`)
Validierung	Bei jedem Submit in `save_data.php`
Token-Rotation	Bewusst **keine** Erneuerung nach Submit (siehe unten)

Design-Entscheidung – keine Token-Rotation nach Submit:

Das CSRF-Token wird nach einem erfolgreichen Submit nicht erneuert. Begründung:

- **Schutzziel CSRF:** Schutz gegen *externe Dritte*, die im Namen des Nutzers Requests absenden. Dieses Ziel ist mit dem bestehenden Token vollständig erfüllt.
- **Mehrfach-Abstimmung:** Wird bewusst toleriert (Erkennung via IP-Hash, keine Verhinderung). Eine Token-Erneuerung würde bei bewusster Zweitabgabe zu einem verwirrenden 403-Fehler führen.
- **Fazit:** Token-Rotation brächte keinen Sicherheitsgewinn, verschlechterte aber die Nutzererfahrung.

Dies adressiert die OWASP-Risikokategorie **A01:2021 Broken Access Control** [12].

2.6 Übersicht der Schutzschichten

Schicht	Daten	Maßnahme	Referenz
Datenbank	IP-Adresse	SHA-256 Hash mit Salt	BSI TR-02102-1 [10]
Apache Logs	IP-Adresse	Letztes Oktett anonymisiert	BSI OPS.1.1.5 [11]
Dateisystem	Salt, DB-Credentials	Außerhalb des Webroots	BSI APP.3.1 [15]
Dateisystem	Log-Retention	Max. 7 Tage, komprimiert	DSK OH Telemedien [9]
Transport	Alle Daten	HTTPS/TLS	BSI TR-02102-2 [10]
Anwendung	Session	HttpOnly, SameSite	OWASP [13]
Anwendung	Formulare	CSRF-Token	OWASP [14]
Webserver	Systemdateien	.htaccess-Blockade	BSI APP.3.1 [15]

---

3. Survey-Fraud-Detection

3.1 Methodische Grundlagen

Die Qualitätssicherung von Online-Erhebungen ist ein aktives Forschungsfeld. **Krosnick (1991)** führte das Konzept des **Satisficing** ein: Teilnehmer wählen statt der optimalen Antwort eine „ausreichend gute", wobei kognitive Schritte übersprungen werden [16]. Prädiktoren für Satisficing sind geringe Motivation, hohe Aufgabenschwierigkeit und geringe kognitive Fähigkeit.

Leiner (2019) identifiziert drei nicht-reaktive Indikatorkategorien für bedeutungslose Daten [17]:

Indikator	Beschreibung	Messmethode
Too Fast	Unrealistisch kurze Bearbeitungszeit	Relativer Speed-Index
Too Straight	Identische Antworten in Batterie-Fragen (Straightlining)	Standardabweichung, Longest String
Too Weird	Multivariate Ausreißer	Mahalanobis-Distanz

Leiners Schlussfolgerung: Bearbeitungszeit ist der zuverlässigste Einzelindikator. Die Kombination mehrerer Indikatoren erhöht die Erkennungsrate erheblich.

Meade & Craig (2012) beziffern den Anteil von Careless Responding auf ca. **10-12%** der Teilnehmer bei längeren Befragungen und empfehlen die Kombination von Consistency-Indices und Outlier-Analyse [18].

Storozuk et al. (2024) analysieren 31 Fraud-Detection-Strategien und schlussfolgern: **Keine Einzelstrategie reicht allein** – ein mehrstufiger Ansatz (vor, während, nach Datenerhebung) ist zwingend erforderlich. Klassische Methoden (CAPTCHA, Duplicate-IP, Geolocation) werden durch KI-gestützte Fraud zunehmend unwirksamer [19].

3.2 CPQI-Qualitätsindikatoren

Basierend auf der Forschungslage implementiert das CPQI-System folgende Indikatoren:

Indikator	Severity	Methode	Grundlage
IP-Duplikate	3 (hoch)	SHA-256-Hash-Vergleich innerhalb Survey	Teitcher et al. (2015) [20], Storozuk et al. (2024) [19]
Straightlining (Häufung identischer Bewertungen)	2 (mittel)	Standardabweichung = 0 über alle Kriterien	Leiner (2019) [17], Kim et al. (2019) [21]
Extreme Scores (Score 1 oder 5 durchgängig)	1 (niedrig)	Mittelwert-Prüfung über alle Bewertungen	Krosnick (1991) [16]

Severity-Stufen

Severity	Bedeutung	Typisches Muster
3	Starke Indikation für Manipulation	Mehrfache Abgabe von derselben IP-Adresse
2	Verdacht auf Satisficing	Alle Kriterien identisch bewertet (z.B. alles 5)
1	Hinweis, prüfenswert	Extremwerte ohne weitere Auffälligkeiten

3.3 IP-Clustering

IP-Duplikate werden im Analyse-Dashboard als **Cluster** dargestellt: Mehrere Bewertungen von derselben IP erscheinen als eine einzige Zeile mit Indikation. Dies folgt dem **REAL-Framework** (Lawlor et al., 2021): Reflect → Expect → **Analyze** → Label [22].

Bewusste Einschränkung: Das System trifft keine Aussage darüber, ob es sich um eine Person mit mehreren Abgaben oder mehrere Personen hinter einem NAT-Gateway handelt. Diese Einschätzung obliegt dem Analysten.

3.4 Bewusst tolerierte Mehrfach-Abstimmung

Teilnehmer können technisch mehrfach abstimmen. Dies ist eine bewusste Design-Entscheidung:

Aspekt	Begründung
Keine technische Sperre	Bei einer anonymen Erhebung wären Sperrmechanismen (Cookies, Browser-Fingerprinting) entweder invasiv oder leicht umgehbar
Erkennung statt Verhinderung	IP-Hash-Duplikate machen Mehrfach-Abgaben im Analyse-Dashboard sichtbar
Analysten-Entscheidung	Der Admin kann verdächtige Bewertungen selektiv aus der Analyse ausschließen

Ethische Dimension: Teitcher et al. (2015) betonen die Abwägung zwischen Datenqualität und Teilnehmerrechten: Ein automatischer Ausschluss birgt das Risiko, legitime Teilnehmer (z.B. hinter Corporate-NAT) fälschlich auszuschließen [20]. Das CPQI löst dies durch transparente Indikation mit manueller Entscheidung.

---

4. Datenschutz-Bewertung

4.1 Erhobene Daten

Datenkategorie	Personenbezug	Speicherung
Abteilung (Hierarchie)	Indirekt (bei kleinen Abteilungen)	Klartext
Manager-Status (ja/nein)	Indirekt (bei kleinen Abteilungen)	Klartext

Datenkategorie	Personenbezug	Speicherung
Bewertungen (1-5 Skala)	Kein	Klartext
Kommentare (Freitext)	Potenziell (Inhalt)	Klartext
IP-Adresse	Ja (EuGH C-582/14)	SHA-256 Hash
Name, E-Mail	Nicht erhoben	–

4.2 Risikobewertung

Risiko	Eintrittswahrscheinlichkeit	Auswirkung	Mitigierung
Reidentifizierung über IP-Hash	Sehr gering	Mittel	Salt außerhalb Webroot, keine Zuordnungstabelle
Reidentifizierung über Abteilung + Rolle	Gering (bei kleinen Teams)	Gering	Aggregierte Darstellung, Mindest-Stichprobe im Dashboard
SQL-Injection	Sehr gering	Hoch	PDO Prepared Statements durchgängig
XSS	Gering	Mittel	Input-Validierung, Security-Headers
CSRF (Formular-Flooding)	Gering	Mittel	Token-Validierung in save_data.php
Unbefugter Zugriff auf Analyse	Gering	Mittel	Session-basierter Login, USE_LOGIN Flag

4.3 Ergebnis

Die Verarbeitung personenbezogener Daten ist auf das **absolute Minimum** reduziert (Art. 5 Abs. 1 lit. c DSGVO [1]). Die IP-Adresse wird sofort nach Empfang gehasht; der Klartext wird nicht persistiert. Die Sicherheitsmaßnahmen entsprechen dem **Stand der Technik** im Sinne von Art. 32 DSGVO [3], konkretisiert durch BSI TR-02102-1 [10] und BSI APP.3.1 [15].

Eine formale **Datenschutz-Folgenabschätzung** (DSFA) nach Art. 35 DSGVO ist nicht erforderlich, da die Verarbeitung kein „hohes Risiko" für die Rechte und Freiheiten der Betroffenen darstellt: Die Erhebung ist anonym, die Bewertungen betreffen Firmen (nicht Personen), und die einzige potenziell personenbezogene Information (IP-Hash) ist praktisch nicht rückführbar.

Quellenverzeichnis

#	Quelle
[1]	**Art. 5 DSGVO** – Grundsätze der Datenverarbeitung. dejure.org, dsgvo-gesetz.de
[2]	**Art. 25 DSGVO** – Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen. dejure.org, dsgvo-gesetz.de
[3]	**Art. 32 DSGVO** – Sicherheit der Verarbeitung. dejure.org, dsgvo-gesetz.de
[4]	**Erwägungsgrund 26 DSGVO** – Anonyme Daten. dsgvo-gesetz.de
[5]	**EDPB Guidelines 4/2019** zu Art. 25, Version 2.0, 20.10.2020. PDF (EN), PDF (DE)
[6]	**EuGH C-582/14** (Breyer), Urteil vom 19.10.2016 – Dynamische IP-Adressen als personenbezogene Daten. CURIA, EUR-Lex
[7]	**EuG T-557/20** (SRB), Urteil vom 26.04.2023 – Relativer Personenbezug bei Pseudonymisierung. dejure.org
[8]	**BfDI Positionspapier** zur Anonymisierung unter der DSGVO, 29.06.2020. PDF
[9]	**DSK Orientierungshilfe Telemedien**, Version 1.1, 2022. PDF
[10]	**BSI TR-02102-1** – Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 2026-01. BSI. **BSI TR-02102-2** – TLS-Empfehlungen. BSI
[11]	**BSI OPS.1.1.5** – Protokollierung, IT-Grundschutz-Kompendium Edition 2023. PDF
[12]	**OWASP Top 10:2021** – A01 Broken Access Control, A05 Security Misconfiguration. owasp.org
[13]	**OWASP Session Management Cheat Sheet**. cheatsheetseries.owasp.org
[14]	**OWASP CSRF Prevention Cheat Sheet**. cheatsheetseries.owasp.org

#	Quelle

[15] **BSI APP.3.1** – Webanwendungen und Webservices, IT-Grundschutz-Kompendium Edition 2023. PDF

[16] **Krosnick, J.A. (1991):** Response strategies for coping with the cognitive demands of attitude measures in surveys. *Applied Cognitive Psychology*, 5(3), 213-236. Wiley

[17] **Leiner, D.J. (2019):** Too Fast, too Straight, too Weird: Non-Reactive Indicators for Meaningless Data in Internet Surveys. *Survey Research Methods*, 13(3), 229-248. Volltext

[18] **Meade, A.W. & Craig, S.B. (2012):** Identifying careless responses in survey data. *Psychological Methods*, 17(3), 437-455. PubMed

[19] **Storozuk, A. et al. (2024):** AI-powered fraud and the erosion of online survey integrity. *Frontiers in Research Metrics and Analytics*, 9, 1432774. Frontiers

[20] **Teitcher, J.E.F. et al. (2015):** Detecting, Preventing, and Responding to "Fraudsters" in Internet Research. *Journal of Law, Medicine & Ethics*, 43(1), 116-133.

[21] **Kim, Y. et al. (2019):** Straightlining: Overview of Measurement, Comparison of Indicators, and Effects. *Social Science Computer Review*, 37(2), 214-233. SAGE

[22] **Lawlor, J. et al. (2021):** Suspicious and fraudulent online survey participation: Introducing the REAL framework. *Methodological Innovations*, 14(3). SAGE

Ergänzende Quellen (nicht direkt zitiert, aber für die Konzeptentwicklung herangezogen):

- **BSI CON.10** – Entwicklung von Webanwendungen, IT-Grundschutz Edition 2023. PDF
- **Krosnick, J.A. & Presser, S. (2010):** Question and Questionnaire Design. In: Handbook of Survey Research, 2nd Ed. PDF
- **Martilla, J.A. & James, J.C. (1977):** Importance-Performance Analysis. *Journal of Marketing*, 41(1), 77-79. SAGE
- **Kanzlei Herfurtner (2024):** Hash-Funktionen und Datenschutz. kanzlei-herfurtner.de

---