

Technisches Konzept: Datenschutzkonforme Verarbeitung von Kundendaten

1. Projekttitle und Zweck

- **Projekttitle:** System zur datenschutzkonformen Verarbeitung von Kundendaten
- **Zweck:** Gewährleistung der sicheren und DSGVO-konformen Verarbeitung von Kundendaten durch Trennung personenbezogener Daten von Problembeschreibungen bei Eingang über E-Mail und weitere Kommunikationskanäle.

2. Ausgangssituation und Problemstellung

Kunden übermitteln Anfragen und Daten häufig via E-Mail oder alternative Kommunikationswege. Diese enthalten personenbezogene Informationen sowie technische Problembeschreibungen. Die Herausforderung liegt darin, die datenschutzrechtlich relevanten Informationen separat und sicher zu verarbeiten, insbesondere wenn externe Dienstleister zur Problemlösung eingebunden werden. Eine vollständige Trennung personenbezogener Daten von Problembeschreibungen ist technisch und organisatorisch umzusetzen.

3. Lösungsansatz

Implementierung einer lokalen KI-basierten Lösung zur automatisierten Erkennung, Extraktion und Trennung personenbezogener Daten von der Problembeschreibung. Die Lösung nutzt ein strukturiertes Ausgabeformat zur differenzierten Speicherung beider Datenkategorien. Die personenbezogenen Daten werden mit einer Verschlüsselungsmethode bis zu 512 Bit Tiefe gesichert. Die Problembeschreibung kann isoliert extern verarbeitet und später in einem Workflow sicher mit den Originaldaten zusammengeführt werden.

4. Technische Umsetzung

4.1 Komponenten

- **Lokale KI-Extraktionsmodul:** Analyse eingehender Daten zur Identifikation personenbezogener Daten und Problembeschreibung.
- **Verschlüsselungsmodul:** Starke Verschlüsselung (bis 512 Bit) der personenbezogenen Daten.
- **Strukturiertes Datenformat:** Ausgabe getrennt nach *personenbezogenen Daten* und *Problembeschreibung* mit klar definierten Variablen.
- **Workflow-Management:** Synchronisation und Zusammenführung der extern verarbeiteten Problembeschreibung mit den verschlüsselten Kundendaten.

- **Schnittstellen:** API zur Datenübergabe an externe Dienstleister und zur Integration der Ergebnisdaten zurück in den Workflow.

4.2 Datenfluss und Prozessschritte

1. Empfang der Kundendaten (E-Mail oder alternative Kanäle).
2. Lokale KI analysiert und trennt personenbezogene Daten von der Problembeschreibung.
3. Verschlüsselung der personenbezogenen Daten mit bis zu 512-Bit-Verschlüsselung.
4. Ausgabe eines strukturierten Formats mit separaten Variablen für beides.
5. Weiterleitung der unveränderten Problembeschreibung an externe Systeme/Dienstleister.
6. Rückaufnahme und Zusammenführung der externen Antworten mit den verschlüsselten personenbezogenen Daten im internen Workflow.

4.3 Beispiel für das strukturierte Ausgabeformat

```
{
  "personenbezogeneDaten": {
    "name": "[verschlüsselt]",
    "email": "[verschlüsselt]",
    "telefon": "[verschlüsselt]",
    "weitereldentifikatoren": "[verschlüsselt]"
  },
  "problembeschreibung": "Klartextbeschreibung des technischen Problems"
}
```

5. Datenschutz und Sicherheitskonzept

- **Datentrennung:** Logische und physische Trennung personenbezogener Daten von Problembeschreibungen.
- **Verschlüsselung:** Einsatz starker symmetrischer oder asymmetrischer Verschlüsselungsverfahren (bis 512-Bit-Sicherheit) zur Sicherung personenbezogener Daten.
- **Lokale Verarbeitung:** Alle datenschutzrelevanten Extraktionen und Verschlüsselungen erfolgen lokal, um Datenlecks zu vermeiden.
- **Zugriffskontrollen:** Rollenbasierte Berechtigungen zur Verwaltung des Zugriffs auf verschlüsselte Daten und Workflows.
- **Auditierung:** Protokollierung aller Zugriffe und Datenoperationen zur Nachvollziehbarkeit.

6. Implementierungsplan

1. Entwicklung und Training der lokalen KI zur zuverlässigen Datenextraktion.
2. Implementierung des Verschlüsselungsmoduls mit auswählbarer 512-Bit-Stärke.
3. Definition und Realisierung des strukturierten Ausgabeformats.
4. Einrichtung der Schnittstellen für externe Dienstleister und interne Workflows.
5. Testphase mit realen und synthetischen Daten inklusive Sicherheitsüberprüfung.

6. Rollout und Schulung der Anwender.
7. Kontinuierliche Überwachung und Verbesserung des Modells und Security-Systems.

7. Betrieb und Wartung

- Regelmäßige Aktualisierung und Nachtrainierung der KI-Modelle zur Erhöhung der Extraktionsqualität.
- Kontinuierliche Überprüfung der Verschlüsselungsstandards und Sicherheitsinfrastruktur.
- Monitoring des Workflows und Datenflusses, inklusive Fehlererkennung und -behebung.
- Periodische Sicherheitsaudits und Penetrationstests.
- Backup und Wiederherstellungsmaßnahmen für gespeicherte Daten.