Was hat die Stunde Datenschutz mit diesem Herbert zu tun?

* Alle nun folgenden Namen und die gesamte Handlung sind natürlich VOLLKOMMEN frei erfunden und würden einem Kärntner Unternehmen so NIEMALS widerfahren….

Wer ist Herbert eigentlich?

- EPU
- Experte für Personaldienstleistung und Recruiting

- Hat eine Mitarbeiterin (Angela*) für:
  - Telefonie
  - Termine
  - Taskmanagement
  - Protokolle

*Name frei erfunden.

Herbert, Angela und die DSGVO

- Ein Musterschüler-Betrieb aus Sicht der DSGVO:
  - Vollständige Datenschutzerklärung (Artikel 13+14 DSGVO)
  - Betroffenenrechte (Artikel 15ff DSGVO)
  - Auftragsverarbeitungs-Verträge (Artikel 28 DSGVO)
  - Verarbeitungsverzeichnis (wegen Artikel 9+10 DSGVO)
  - Dokumentation der TOM (Artikel 30 DSGVO)

- Was nicht gemacht wurde:
  - Risikoabschätzung der Verarbeitungstätigkeiten
    - Datenschutzfolgeabschätzung erforderlich?
  - Prüfung/Adaptierung der VdV / TOM

Herbert bekommt ein Problem!

- Angela verlässt nach der Pandemie das Unternehmen.
- Anfangs funktioniert es für Herbert ohne Angela noch recht gut.
- Es bleiben nur immer wieder Backoffice-Tätigkeiten liegen...

- …aber genau diese werden zum unübersehbaren Problem

Herbert hat die Lösung! (?)

- Er liest ja überall, dass KI die Arbeiten des Backoffice erledigen kann
- Nun aktiviert er den Quick & Dirty Modus
- Aktiviert Accounts bei chatGPT, N8N, etc…
- Er baut sich per Drag&Drop seine Backoffice-Unterstützung zusammen
- Nach etwa einer Woche ist er happy und alles funktioniert wie gewünscht!

Der Impact kurz vor dem Urlaub

- Die DSB nimmt Kontakt auf, es liegt eine Beschwerde vor

- Herbert bekommt eine Menge Aufgaben
  - Dokumentation TOMs
  - Verarbeitungsverzeichnis
  - Meldung von Datenschutzverletzungen binnen 72 Stunden
  - Unverzügliche Meldung an die Betroffenen darüber

Bei Nichteinhaltung => Strafandrohung

Der zweite Impact kurz danach

- Herbert arbeitet gerade alles für die DSB ab
- Da flattert ein Brief eines Anwalts seines Hauptkunden ins Haus

- Herbert bekommt eine fristlose Vertragskündigung
  - NDA verletzt
  - Vertrauliche Daten veröffentlicht
  - Vertrauen in professionelle Zusammenarbeit verloren
  - Schadenersatzforderung…

Was ist denn passiert?

- Es kam zu einem Verlust vertraulicher Daten in Herberts Prozess
- Vertrauliche Projektdaten wurden veröffentlicht
- Weitere Schadensersatzklagen sind nicht ausgeschlossen
- Es greift die Geschäftsführerhaftung

Wie kann das sein?

- Herbert forscht nach
- In seinem Workflow kam es zu einem Datenleak bei einem verwendeten Dienstleister
- Die Daten, inklusive Herberts, sind zum Kauf verfügbar

- Aus welchen Daten besteht der Datensatz?
  - Einschränkungen & chronische Erkrankungen
  - Religiöse Überzeugung und Weltanschauung
  - Gewerkschaftszugehörigkeit
  - Ethnische Herkunft
  - Polizeiliches Führungszeugnis

Betrifft DSGVO Art. 9,10

Was sagt die DSB?

- Verarbeitung personenbezogener Daten in unsicherem Drittland
- Keine Prüfung der TOMs => Schutzniveau
- Keine Dokumentation eigener TOMs
- Keine Evaluierung der TOMs seit 2018
- Keine Risikoeinschätzung der im Einsatz befindlichen Software-Dienstleister
- Keine Datenschutzfolgeabschätzung jener Verarbeitungstätigkeiten (Hohes Risiko)

Strafbescheid der DSB in der Höhe von 2 / 4 % des letztjährigen Jahresumsatz?

+ Schadensersatzforderungen des Hauptkunden!

Worauf hätte Herbert achten müssen?

- Rechtsgrundlage der Verarbeitung
- Nachvollziehbarkeit der Verarbeitungstätigkeiten
  (Er muss wissen wie es funktioniert)
- Dokumentation JEDER Verarbeitungstätigkeit
- Sicherstellung der techn. Sicherheit der Verarbeitung

Daher am besten zuerst prüfen:

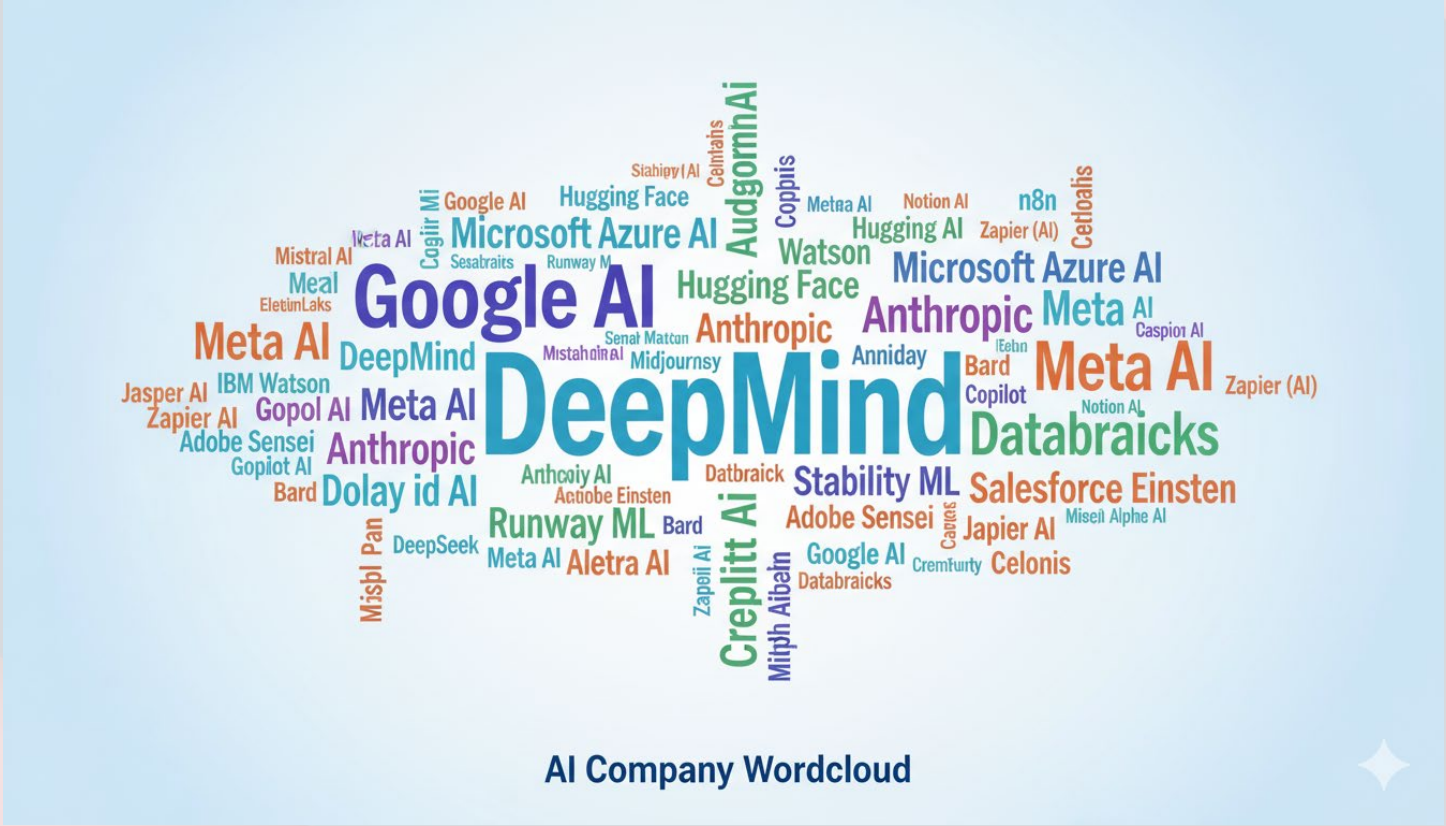
- ***Gibt es dies schon so zu kaufen (inkl. Haftungsübernahme des Lieferanten?)***

Wie identifiziert Herbert vertrauenswürdige Partner?

- Aufrechtes Gewerbe vorhanden?
  - Gibt es einen Geschäftsführer?
  - Prüfen über Wirtschaftskammer und Firmen A-Z
- Ist eine aktuelle Auftragsverarbeitungsvereinbarung vorhanden?
- Sind aktuelle TOMs vorhanden und entsprechen sie der Realität?

- Es muss Herbert klar sein, wo von wem welche Daten verarbeitet werden!
  - Gibt es Unterauftragsnehmer?
  - Wenn ja, gibt es für das Land, in dem sich der Firmensitz befindet, ein angemessenes Datenschutzniveau?

Das ist doch leicht für Herbert…



KI-generierte „Wordcloud“
Fehler sind Programm

Was wäre der richtige Weg für Herbert?

1) Arbeitskreis Datenschutz der Wirtschaftskammer Kärnten kontaktieren
2) Datenschutzkonforme Lösungen evaluieren…

stackfield

fonio.ai

stream diver

Die Auswahl ist zufällig für Herbert und keine Werbung.
Welche Lösung perfekt zu einem Unternehmen passt, entscheidet eine fundierte Evaluierung!

Was ist bei einer Lösung wichtig?

- Wenn möglich, EU-Lösungen bevorzugen
- Privacy by Design
- Einhaltung aktueller Gesetzesbestimmungen
- Nachweisbares Wissen über die tatsächliche Verarbeitungen
- Kein Vendor Lock-In (Data Act)
- EU AI ACT (Anbieter/Betreiber, Risikokategorisierung, KI-Kompetenz nachweisbar)

Wie finde ich Anbieter?

Die nachfolgenden Links bieten mögliche Alternativen.
Jede Lösung muss auf ihre individuelle Verwendbarkeit und Legalität geprüft werden.

- EU-Alternativen für digitale Produkte: https://european-alternatives.eu/de
- AI-Landscape Austria: https://www.ai-landscape.at/

SCAN ME

Ing. Walter Wratschko
+43 699 150 43 860

datenschutz-sued
sicherheit . orientierung . vielfalt

Christian Kollegger
+43 676 844 180 180

stream diver

SCAN ME