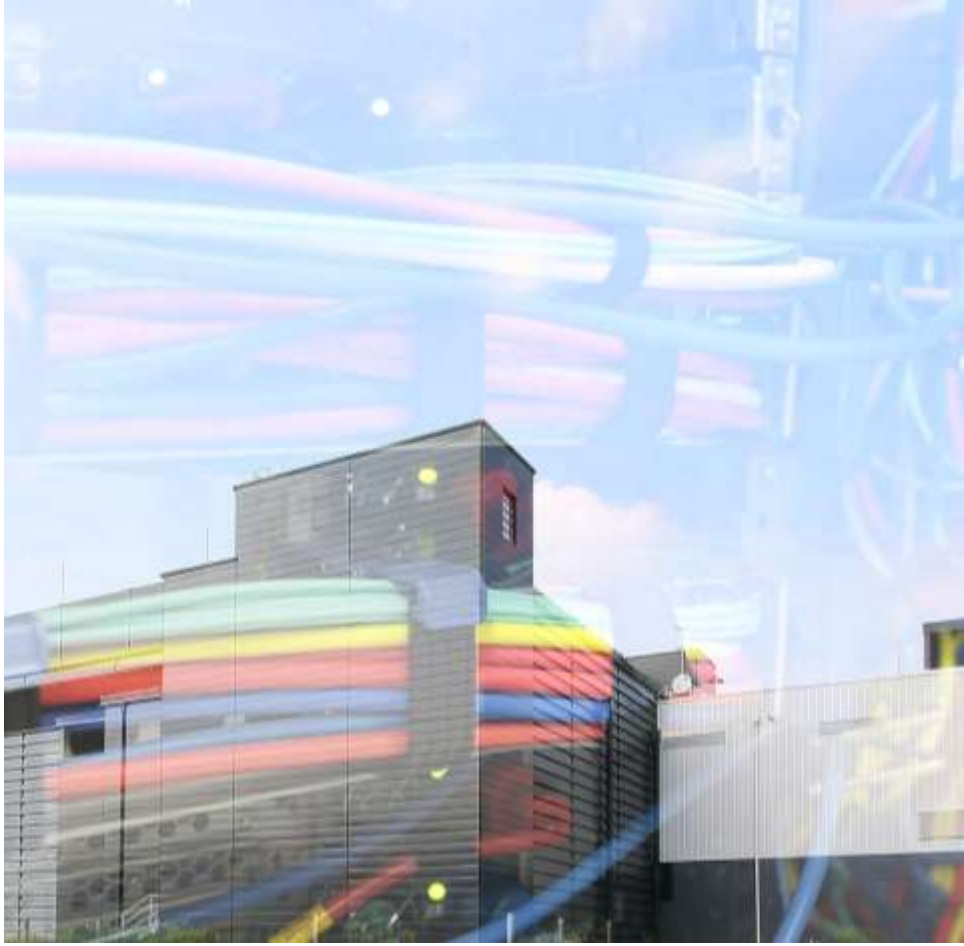


DSGVO-Umsetzung aus der Sicht eines Praktikers – Auszug Präsentation

G.Moser – März 2018

14.03.2018

RAIFFEISEN INFORMATIK

Fragen nach 10 Monaten Projekt

- Haben wir wirklich Rechtssicherheit?
- Wie schaffen wir noch den Rest?
- Kann die SW das wirklich sauber?
- Haben wir den richtigen Weg zwischen Aufwand und Restrisiko gewählt?
- Könnten wir vielleicht nicht noch mehr löschen - Vergleich der Risiken des zu wenig versus zu viel Löschen?
- Wie schaffen wir die laufenden Aufgaben?

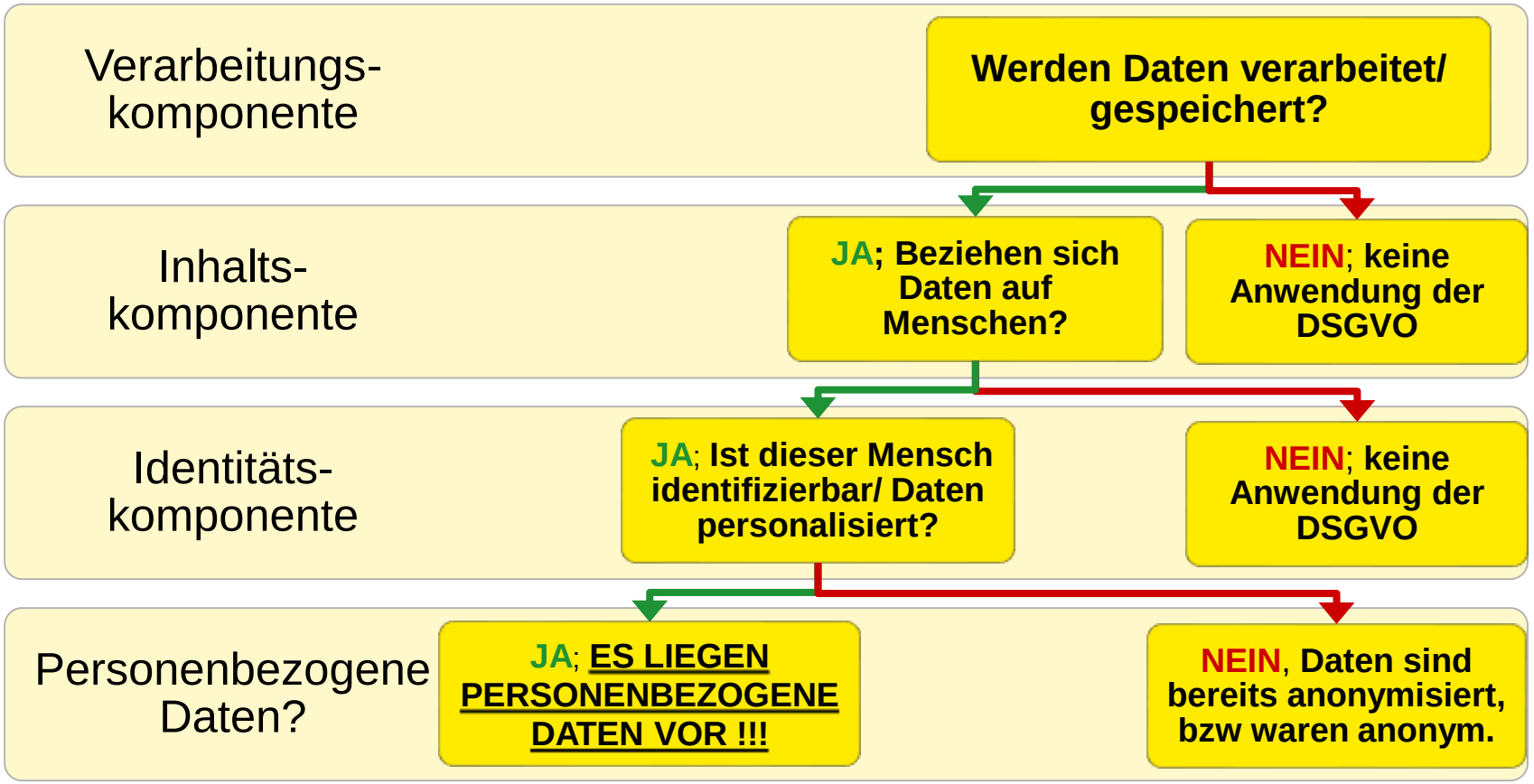
Case for action

- Per 25.5.2018 müssen die Voraussetzungen welche die DSGVO (Datenschutzgrundverordnung) an Unternehmen stellt erfüllt sein. Bei Nichtumsetzung drohen Verwaltungsstrafen von bis zu 20 Mio EUR oder 4% des Konzern-Gesamtumsatzes.
- Zusätzliche Auswirkungen (auf Dienstleister):
  - neue Dienstleisterpflichten/ solidarische Haftung im Außenverhältnis
  - Haftung für ideelle Schäden des Betroffenen möglich
  - neue Data Breach Notification (Informationspflicht binnen drei Tagen)

Datenschutzgrundverordnung

- Wesentliche Neuerungen:
  - Dokumentationspflichten
    - Unternehmensinternes VvV für Fälle in denen Unternehmen Verantwortlicher ist
    - VvV für Fälle in denen Unternehmen Auftragsverarbeiter ist
  - Datenschutz- Folgenabschätzung
  - Datenschutz by design and default
  - Betrieblicher Datenschutzbeauftragter
  - Recht auf Datenübertragbarkeit
  - Sanktionen (Verwaltungsstrafen)
  - Sonstige wesentliche Neuerungen
- **Grundsätze der DSGVO :**
  - Datensparsamkeit (Einschränkung auf sachliche Erforderlichkeit)
  - Zweckbindung (Löschung nach Zweckerfüllung)
  - Transparenz (gegenüber den Betroffenen)

Prüfschema personenbezogene Daten



Datenschutz Management System (DMS)

Risikoanalyse

- Anforderungen erörtern
- betroffene Systeme erheben
- Prozesse durchleuchten
- DS- Folge-abschätzungen

Maßnahmen

- DS-Beauftragter
- E-Learning
- Dienstanweisung
- Security- Policy
- Verträge/ AGB anpassen
- Servicierung d. betroffenen Stellen
- Datenminimierung
- ITSM- Workflow (DVZ erstellen)

Information/ Kommunikation

- Helpdesk
- DS-Manual
- Bericht an GF
- Newsletter
- Intranet
- Schulungen
- Info d. Betroffenen (u.a. Data Breach)

Überwachung/ Kontrolle

- Workflow-Genehmigung
- DVZ überprüfen
- Zertifizierungen (ISO 27001)
- Einsichtsrecht des DSB
- Kontrolle im IKS implementieren

Just Do It

Analyse durchführen – welche Tools, Prozesse etc. sind betroffen?

Wer ist für welche Datenverarbeitung zuständig?

DVZ erstellen

Dienstleistervereinbarungen neu aufsetzen

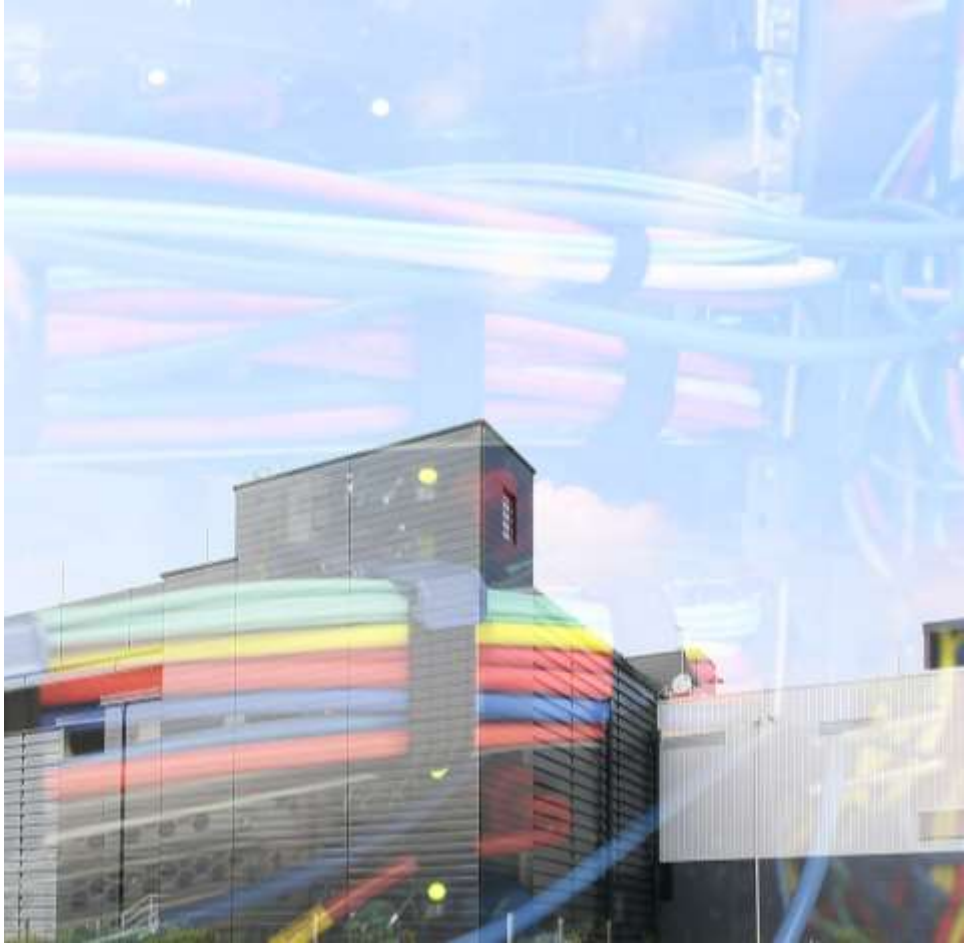
Einwilligungserklärungen neu aufsetzen

Information Security Maßnahmen implementieren

Löschfristen festlegen und implementieren

Prozesse für Auskunftsersuchen implementieren

Notfallsplan für Data Breach entwickeln



Raiffeisen Informatik GmbH
Lilienbrunngasse 7-9
1020 Wien

T +43 1 99 3 99 0
E info@r-it.at
W www.r-it.at

RAIFFEISEN INFORMATIK