TEMET
end-to-end IT security

# Vom Auftragsdatenverarbeiter zur Risikofolgenabschätzung

## Ausgewählte Aspekte der DSGVO und ihre Bedeutung für die IT in der Schweiz

Stephan Töndury

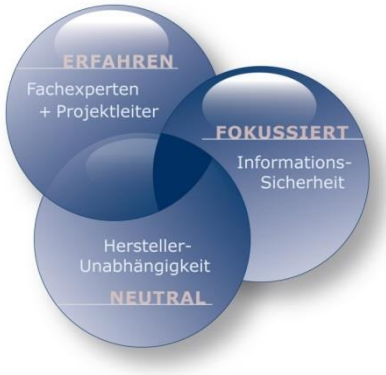
27. Juni 2017

TEMET
end-to-end IT security

# Agenda

- Über die TEMET AG
- Einleitung
- Risiken
- Technologien
- Empfehlungen

# Über die TEMET AG




- Gründung: März 2010
- Inhabergeführte Aktiengesellschaft
- Sitz am Basteiplatz 5, im Herzen von Zürich
- Aktuell 12 Information Security Consultants
- Aktuell 76 Kunden aus Finanz, Verwaltung und Gesundheitswesen

Die TEMET AG positioniert sich im Markt als herstellerneutrale und auf Informationssicherheit fokussierte Firma, deren Berater fachliche Expertise mit Projektmanagement-Kompetenz verbinden.

# Die Eckpunkte der DSGVO

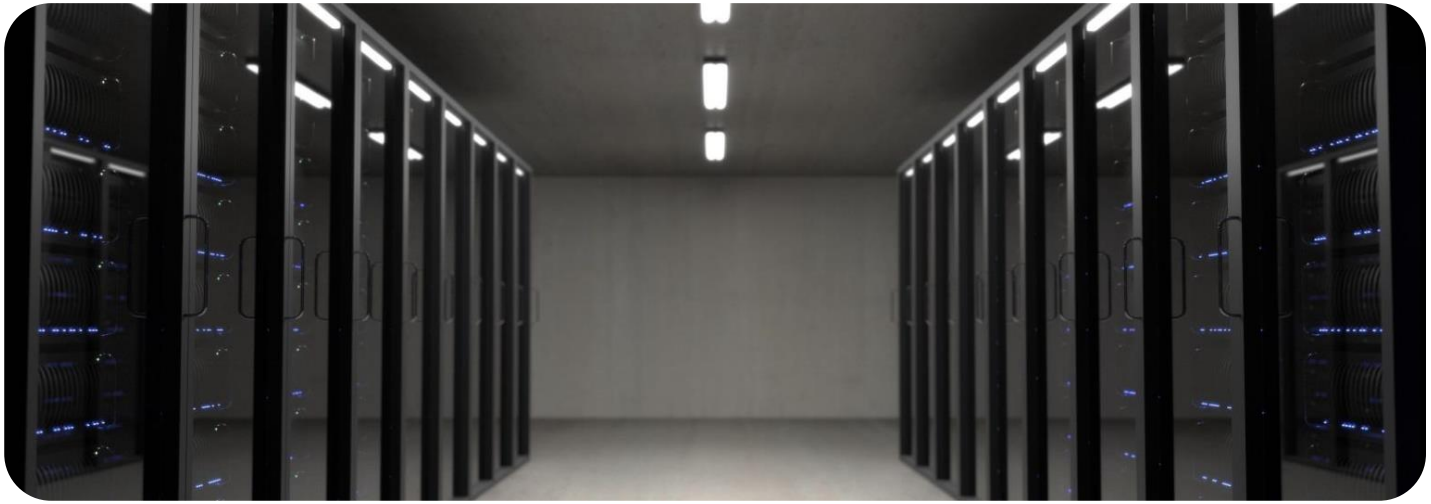
- Ziel der neuen DSGVO
- Übernommene Datenschutz-Grundsätze
  - Insbesondere Datenschutz-Ziele wie etwa die Zweckbindung, die Berechtigten (Betroffenen) und die Verpflichteten
- Neue Grundsätze (Auszug)
  - Anwendbarkeit der DSGVO
  - Datenschutzfolgenabschätzung („Vorabkontrolle“)
  - Datenportabilität und Recht auf Vergessen
  - Stellung und Pflichten der Auftragsdatenbearbeiter
  - Betrieblicher Datenschutzbeauftragter
  - Privacy by Design und by Default
  - Erweiterte Rechte betroffener Personen
  - Melde- und Informationspflichten
- Neue Sanktionen

# Die Eckpunkte der DSGVO

- Ziel der neuen DSGVO
- Übernommene Datenschutz-Grundsätze
  - Insbesondere Datenschutz-Ziele wie etwa die Zweckbindung, die Berechtigten (Betroffenen) und die Verpflichteten
- Neue Grundsätze (Auszug)
  - Anwendbarkeit der DSGVO
  - Datenschutzfolgenabschätzung („Vorabkontrolle“)
  - Datenportabilität und Recht auf Vergessen
  - Stellung und Pflichten der Auftragsdatenbearbeiter
  - Betrieblicher Datenschutzbeauftragter
  - Privacy by Design und by Default
  - Erweiterte Rechte betroffener Personen
  - Melde- und Informationspflichten
- Neue Sanktionen

# „Die IT“ als Datenbearbeiter

- Datenherrschaft
- Datenbearbeitung im Auftrag
- Rechtliche Stellung/Verantwortlichkeit von Auftraggeber und -nehmer
- Risiken für die IT i.e.S.
- Konsequenzen betreffend Technik, Recht und Organisation



# Risiken für die IT aus der DSGVO

- Risiko als Wert
- Risikobestandteile
  - Bedrohungen
  - Schwachstellen
  - Schadenszenarien
  - Eintretenswahrscheinlichkeit
  - Schadensausmass
- Die DSGVO als Bedrohung
- Die Datenbearbeitung als Schwachstelle
- Neue Schadenszenarien?
- Die Sanktionen als Schaden (auch für beauftragte Datenbearbeiter)

- Was ist daran neu?

# Risikobehandlung

- (Corporate) Governance und Compliance
  - Unternehmerische Risiken
  - Operationelle Risiken
  - …
  - Risiken der Informationssicherheit
- Risikobehandlung nach gesetzlichen und internen Vorgaben
- Wo gehören die Datenschutzrisiken hin?
  - Das Management der Informationssicherheit umfasst regelmässig die Umsetzung der gesetzlichen Datenschutzvorgaben, nennt diese aber nicht, da lokal geregelt.
- Eigene RM-Disziplin?
  - Indiz: Zertifizierungsfähigkeit inkl. Managementsystem; Eigene ISO/IEC-Reihe 291xx (Privacy [architecture] framework, Guidelines for privacy impact assessment, CoP for PII protection etc.) sowie andere wie ISO/IEC27018 CoP for PII in public clouds etc.

# Privacy Enhancing Technologies

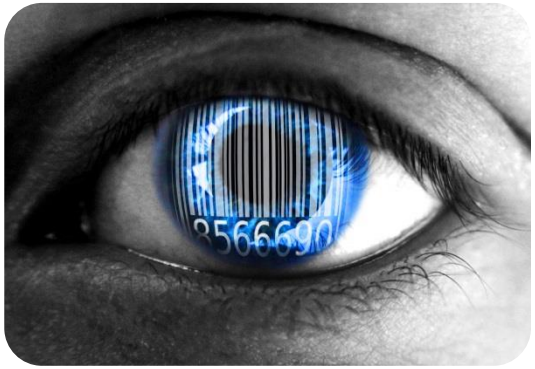
- Datenvermeidung und –sparsamkeit durch Technologie und Prozesse
  - So wenig Bearbeitung von Personendaten wie möglich, insb. durch Anonymisierung oder Pseudonymisierung, etwa bei Authentisierungsprozessen durch Attribute based Credentials statt Personendaten i.S. des Gesetzes
- Transparenz
  - Soll die informierte Entscheidung ermöglichen, ob und falls ja, wie viele Daten wie und unter welchen Bedingungen bearbeitet werden sollen
  - Z.B. durch automatisierte Hinweise über Datenschutzrisiken vor der Übermittlung von Daten über ungeschützte Kommunikationskanäle
  - Z.B. im ePD: Patientendossier mit Verwendung nach Entscheid der betroffenen Person
  - Opt-in vs. Opt-out
- PET zur Anonymisierung bzw. Pseudonymisierung bei
  - Kommunikation: Verschlüsselung
  - Aufbewahrung (und Löschung)
  - Verarbeitung
  - Bekanntgabe

# Verschlüsselung

- Datenverluste
  - „Last year, the UK suffered more data breaches than any previous year. In 2016, 54,468,603 records were compromised – a 475% increase over the 9,478,730 compromised in 2015“ (Quelle: J. Pindar, Gemalto.com)
- Die DSGVO nennt ausdrücklich Verschlüsselung zur Anonymisierung als taugliche Sicherungsmassnahme
- Verschlüsselung auf Dateiebene schützt nicht nur nach innen, sondern macht gestohlene/verlorene Daten wertlos
- Praktikabel? Gesteuerte Pseudonymisierung als Alternative?
- Schlüsselmanagement und Codeverwaltung: Schlüsselmaterial als höchst sensitive Unternehmensdaten muss angemessen geschützt werden
- Identitäts- und Access Management als Grundlage
- Bewährte Massnahme etwa 2FA / MFA
- Zudem Kommunikationsverschlüsselung und –anonymisierung

# Anonymisierung & Pseudonymisierung

- Wie sehen Ihre Geschäftsprozesse und Ihr Datenmodell aus, wenn Löschansprüche berücksichtigt werden müssen?
- Privacy by Design und referentielle Integrität in Datenbanken
- Anonymisierung durch irreversible De-Personifizierung
- Anonymisierung durch vollständige Verschlüsselung
- Wo kann anonymisiert werden, wo pseudonymisiert?



- Was hält Ihr Softwarelieferant davon?
- Und welche sind die Standardeinstellungen Ihres Kernsystems?

# Melde- & Informationspflichten

- Zeitnahe Reaktion ist gefordert
- Setzt Aufzeichnungen / Überwachung und Auswertungen voraus
- (Rekursionsproblem: Datenschutz beim Überwachen und Auswerten )
- Die neuen Pflichten sind geeignet, Reputationsschäden zu erhöhen
- SIEM als Mittel zur konformen Berichterstattung

# Handlungsempfehlungen

- Management-Attention schaffen
- Organisatorische Massnahmen
  - Datenschutzkompetenz aufbauen und installieren, inkl. Regulativ und Prozessen für berechtigte Ansprüche
  - Übersicht gewinnen: Inventarisierung und Klassifizierung der Daten und ihren Bearbeitungsprozessen (inkl. Archivierung, Bekanntgabe etc.)
  - Neue Melde- und Informationsprozesse etablieren
  - Einwilligungen und Rechtsgrundlagen der Datenbearbeitung prüfen
  - Datenschutzhinweise anpassen
  - Alles dokumentieren
  - Mitarbeitende ausbilden

  - Workaround: Anwendbarkeit wo möglich ausschliessen (~ Datensparsamkeit und Privacy by Design)

# Handlungsempfehlungen

- Technische Massnahmen
  - Whitelisting in der Datenbearbeitung zur Datensparsamkeit bzw. -vermeidung
  - Systeme prüfen auf Umsetzbarkeit von Löschansprüchen und Herausgabeansprüchen (in maschinenlesbarer Form) unter Wahrung der referentiellen Integrität
  - Storage prüfen auf end-to-end Belastbarkeit/Resilienz  sowie Manipulationssicherheit, insbesondere bei nachweisrelevanten Daten
  - Prozess zur Risikofolgenabschätzung erarbeiten, in Projektmethodik integrieren und wo nötig durchführen
  - Disaster Recovery Pläne prüfen
  - Aufzeichnung der Datenbearbeitung konzipieren und einführen
  - SIEM in irgend einer (genügenden) Form sicherstellen, um Melde- und Informationspflichten erfüllen zu können

# Vorgehensempfehlung

- Compliance Projekt
- Status erheben und Delta ableiten
- Priorisierung (Sofortmassnahmen wo nötig)
- Organisatorische Massnahmen
- Technische Massnahmen
- Verbesserungsprozess etablieren
- Dokumentieren, dokumentieren, dokumentieren

# Ausgewählte Aspekte der DSGVO

# Ausgewählte Aspekte der DSGVO

Besten Dank
für Ihre Aufmerksamkeit!

**TEMET AG**
Basteiplatz 5
8001 Zürich
044 302 24 42
info@temet.ch
www.temet.ch