DPIA Smart Meter

DPIA
Praktische Umsetzung in der Salzburg AG

Manfred Farthofer
Salzburg AG

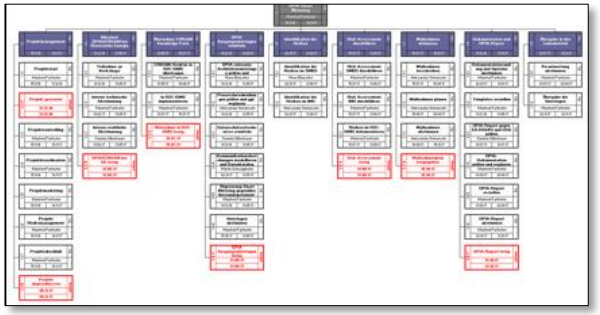
Informations-Klassifizierung: öffentlich

Agenda

- Projektrahmendaten
- Projektumwelten
- Bezug zu ISMS und Risikomanagement
- DPIA-Modellierung
- Datenflussanalyse
- Anwendung der Content Library
- Toolfrage
- Zusammenfassung und Ausblick

Projektrahmendaten Projekt DPIA Smart Meter in der Salzburg AG

- Projektorganisation
  - Projektleiter Manfred Farthofer
  - Projekt ist im Programm Smart Metering aufgehängt
  - Projektauftraggeber sind der Programmleiter Smart Metering und der Leiter der IT
- Projektteammitglieder
  - Projektteammitglieder aus dem Projekt Smart Metering, Datenschutz und Informationssicherheit, im speziellen auch aus der IT
- Projektzeitplan
  - Projektlaufzeit von Jänner 2017 bis März 2018
- Projektmanagement lt. Standard der Salzburg AG

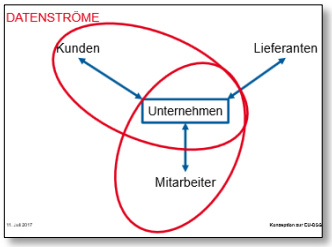


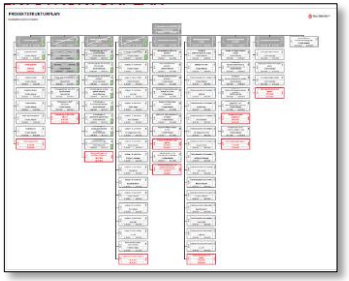
Projektziele / -inhalte

- Mitarbeit im DPIA/CRISAM-Projekt bei Österreichs Energie
- Übernahme des bei OE entwickelten CRISAM-DPIA-Knowledge Packs in das Tool R2C-ISMS
- Abgrenzung DPIA Smart Metering gegenüber den Bestandsprozessen / -systemen
- Durchführen des DPIA für die konkrete Smart Metering Infrastruktur
- Ermittlung und Abstimmung allenfalls noch zu setzender Datenschutz-Maßnahmen im Programm Smart Metering
- Erstellung des DPIA-Reports für Smart Metering und Übergabe in die Linienverantwortung

Projektumwelten Konzeptionsprojekt EU-DSGVO und IS-Risikomanagement

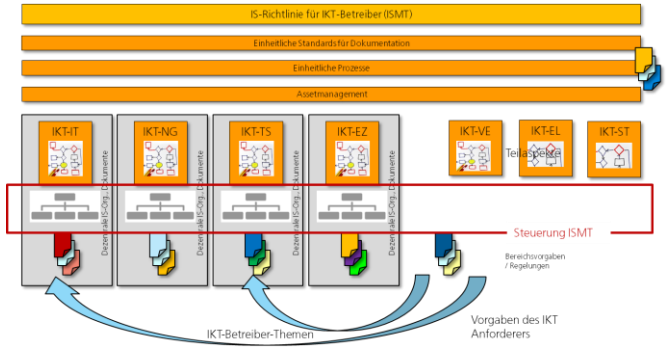
- Vorgehensweise ist mit dem in der Salzburg AG laufenden Projekt Konzeption EU-DSGVO abzustimmen.
- Unternehmensweit harmonisierte Vorgehensweise hinsichtlich der anderen Datenschutzthemen.
- Berücksichtigung des rechtlichen Rahmens.
- Harmonisierung der Verzeichnisse der Verarbeitungstätigkeiten.
- Entwicklung und Vorgabe der Datenschutzprozesse
- Gemeinsame Risikosicht und Berücksichtigung des Informationssicherheits-Risikomanagement aus dem ISMS.





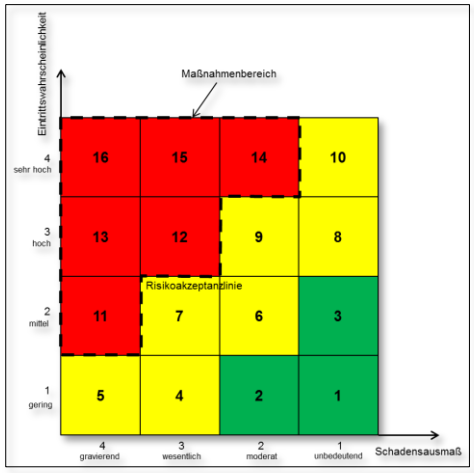
Bezug zu ISMS und IS-Risikomanagement

- Es gibt in der Salzburg AG ein Informationssicherheitsmanagement nach ISO 27001 bzw. daran ausgerichtet.
- Die IT der Salzburg AG ist seit 2014 nach ISO 27001 zertifiziert
- Sowohl auf Unternehmensebene als auch in der IT ist IS-Risikomanagement etabliert.
- Regelmäßige strukturierte Betrachtung der Risiken.
- Datenprozesse bauen auf IKT-infrastruktur auf
- Wesentlicher Bezug zur Informationssicherheit
- Bekannte Liste der wesentlichen IT-Risiken als Basis für die Betrachtung



ISMS-Risiken versus Datenschutz-Risiken

- ISMS
  - **Bewertung aus Unternehmenssicht**
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit

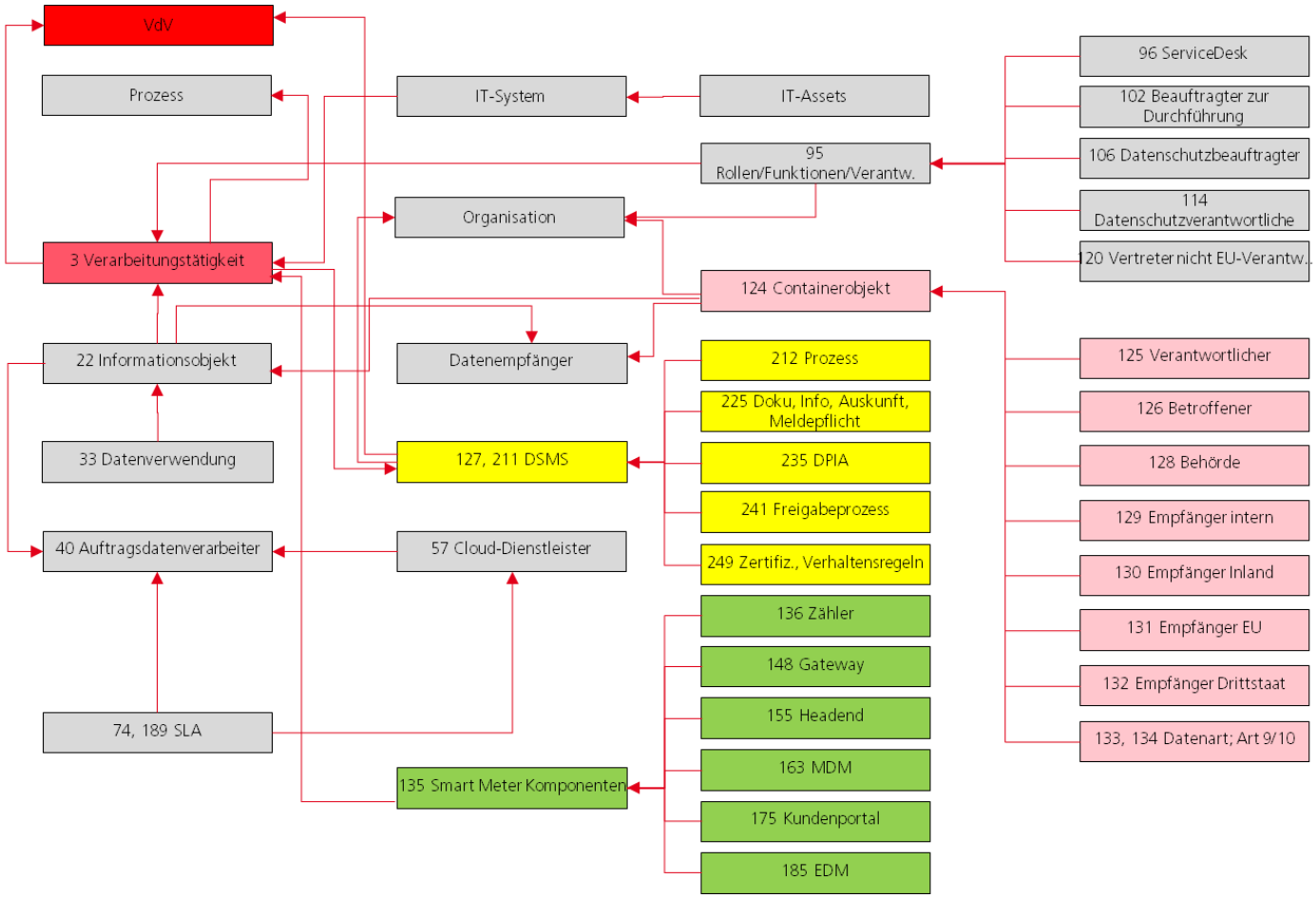


- Datenschutz
  - **Bewertung aus Sicht der Betroffenen**
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit
  - Nichtverkettbarkeit
  - Transparenz
  - Intervenierbarkeit

Bedrohungen/Schwachstellen → Gefährdungsbeurteilungen → Risiken

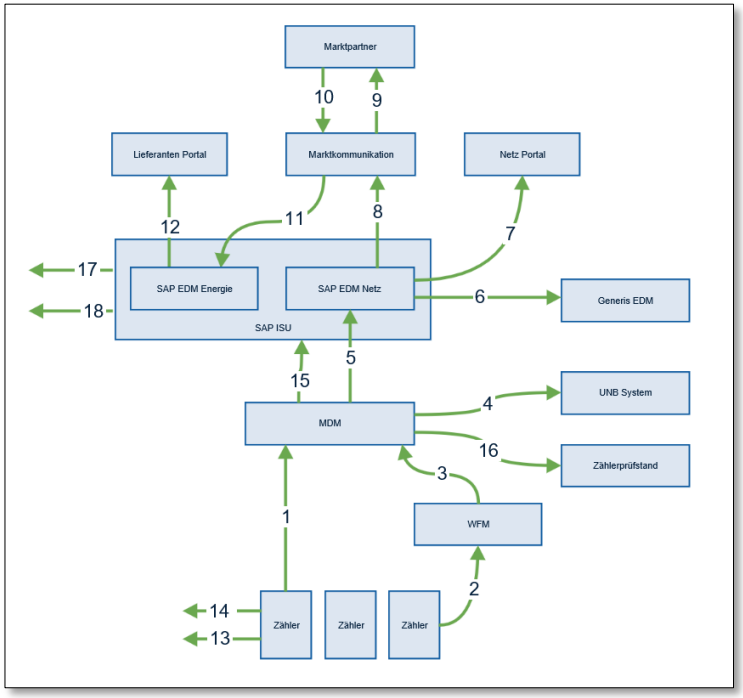
Bewertung der Risiken entsprechend
Eintrittswahrscheinlichkeit und Schadensausmaß.

DPIA-Modell


VdV
Prozess
IT-System
IT-Assets
96 ServiceDesk
102 Beauftragter zur Durchführung
106 Datenschutzbeauftragter
95 Rollen/Funktionen/Verantw.
114 Datenschutzverantwortliche
Organisation
3 Verarbeitungstätigkeit
20 Vertreter nicht EU-Verantw.
124 Containerobjekt
22 Informationsobjekt
Datenempfänger
212 Prozess
125 Verantwortlicher
225 Doku, Info, Auskunft, Meldepflicht
126 Betroffener
33 Datenverwendung
127, 211 DSMS
235 DPIA
128 Behörde
241 Freigabeprozess
129 Empfänger intern
40 Auftragsdatenverarbeiter
57 Cloud-Dienstleister
249 Zertifiz., Verhaltensregeln
130 Empfänger Inland
136 Zähler
131 Empfänger EU
148 Gateway
132 Empfänger Drittstaat
74, 189 SLA
155 Headend
133, 134 Datenart; Art 9/10
163 MDM
135 Smart Meter Komponenten
175 Kundenportal
185 EDM

Datenflussanalyse

- Darstellung der wesentlichen Datenflüsse als Basis für die Datenschutzfolgenabschätzung
- Ermittlung der wesentlichen (kritischen) Datenarten
- Berücksichtigung der konkreten IKT-Infrastruktur
- Erhebung der getroffenen Sicherheitsmaßnahmen
- Dokumentation der Rollen mit Datenzugriff je Datenfluss



Beispiel Datenflüsse Verbrauchsdaten

Konkrete Anwendung der Content Library

- Die Content-Library wird bei der Beurteilung der konkreten Prozesse und der konkreten Infrastruktur angewendet auf
  - Zähler, Gateway, MDMS, Kundenportal, EDM
  - weitere IT-Systeme sinngemäß
  - auf die generellen organisatorischen Datenschutzfragen entsprechend der zutreffenden Objekte und jeweiligen Kontrollziele
- Die Beurteilung des Umsetzungsstandes ist das Ausgangs-Niveau für die Ableitung von Maßnahmen.
- Wird nicht mindestens die Einstufung „B“ (Stand der Technik) erreicht, so sind Maßnahmen zu definieren, die sicherstellen, dass die Einstufung „B“ erreicht wird.

Nutzen der Projektergebnisse von OE

- „Blaupause“ für die konkrete Datenschutzfolgenabschätzung
- Templates für das Verzeichnis der Verarbeitungstätigkeiten
- Template für den DPIA-Bericht
- Bewertungs-Excel für die Beurteilung der wesentlichen zu betrachtenden Objekte im Smart Metering.
- Bewertung der Gefährdungen (PIA).
- Rahmen für die Einordung in den Stand der Technik und damit Basis für die Ermittlung allenfalls noch zu setzenden Maßnahmen.
- Content Library ist im EXCEL für Unternehmen ohne Tool auch direkt anwendbar und bewertbar.

Toolfrage

- Auf Sicht ist bei größeren Unternehmen jedenfalls ein Datenschutzmanagementsystem (DSMS) integriert mit einem ISMS zu empfehlen.

- Grundlegende Anforderungen:
  - Verbindung der ISMS-Gesichtspunkte mit den Datenschutzgesichtspunkten
  - Abdeckung Risikomanagement und einheitliche Abläufe für ISMS und DSMS
  - Abdeckung der Dokumentationsanforderungen wie z.B. Führung des Verzeichnis der Verarbeitungstätigkeiten, Datenschutzfolgenabschätzungen
  - Einheitliche Datenbasis (z.B. Assets) und damit Vermeidung von Doppelführungen
  - Sicht als Verantwortlicher und als Auftragsdatenverarbeiter
  - Historisierung
  - Mandanten und Mehrbenutzerfähig
  - Automatische Generierung der gesetzlich erforderlichen Berichte

Zusammenfassung und Ausblick

- Datenschutzfolgeabschätzung muss für Smart Meter durchgeführt werden.
- Bei OE erarbeitete Dokumente bilden eine sehr gute Grundlage.
- Die Dokumente müssen auf die jeweilige konkrete Smart Meter Umsetzung angewendet werden.
- Für die konkrete Durchführung ist ein „kleines“ Projekt mit den erforderlichen Fachexperten zu empfehlen.
- Eine Verantwortungszuordnung und Überführung in die Linientätigkeit ist erforderlich.
- Im Frühjahr 2018 erfolgt eine Überarbeitung auf Basis der Erfahrungen und Aktualisierung