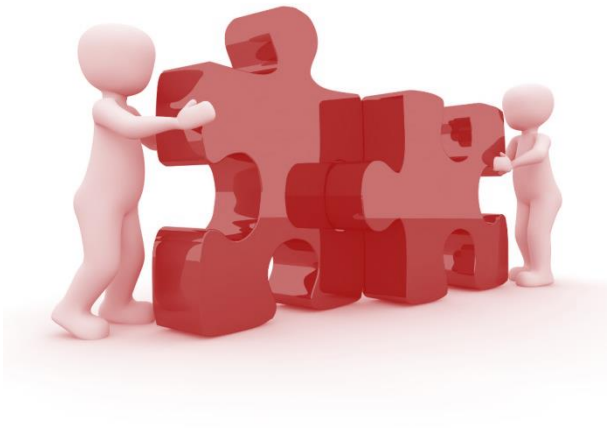
oesterreichs energie.

Smart Metering DPIA

Risiko- und Folgeabschätzung Durchführung und Nutzen

Martin Jagerhofer
Energie Graz GmbH & Co KG

Vorgehensweise der Branche



- Identifikation der Betroffenen
- Bewerten der Bedrohungslage der Betroffenen (PIA)
- Erstellen des Verzeichnisses der Verarbeitungstätigkeiten
- Identifizieren der erforderlichen Services, Anwendungen und IT -Assets
- Feststellen der Risiken der Betroffenen (DPIA)

Arbeitsunterlagen

- **DSMS Katalog Smart Metering (DPIA)**
- **ISMS Katalog Smart Metering (Basis IT-Services)**
- **DPIA Standardbericht**
- **Musterprojekt (CRISAM®)**
- **DPIA „White Paper“**
- **Verhaltensregeln**
  für Netzbetreiber bei der Verwendung von mit intelligenten Messgeräten erhobenen personenbezogenen Daten
- **Interne Arbeitshilfe** für Netzbetreiber bei der Anwendung der Verhaltensregeln
- **Smart Grid Task Force**

DPIA Content Library

ca.240 Kontrollfragen

Objekt	Kontroll-ziel ID	Kontrollziel	Beschreibung	Impact							Priorität	KO	Optimal möglich
				Gesamt	Verfügbarkeit	Vertraulichkeit	Integrität	Nichtverkettbarkeit	Transparenz	Intervenierbarkeit	[1 .. 4]	Y/N	Y/N
Meter Data Management (MDM)_Datenschutz	10	Wie ist sichergestellt, dass der Zugang zu den im Meter Data Management gespeicherten Verbrauchsdaten nur durch berechtigte bzw. autorisierte Personen erfolgt?				x							y
	20	Wie ist der Fernwartungszugang, sofern vorhanden, vor unberechtigtem bzw. unautorisiertem Zugang gesichert?				x							Y
	30	Wie können auf Kundenwunsch Daten aus dem Meter Data Management System gelöscht werden?							x				N
	40	Wie ist sichergestellt, dass bei Einsatz eines Meter Data Management Systems für mehrere Unternehmen eine Trennung der Daten erfolgt?				x		x					N
	50	Wie kann der Missbrauch von Berechtigungen im Meter Data Management System erkannt werden?				x	x						y
	60	Wie kann ein unberechtigter Datenabfluss (z.B. über Schnittstellen oder Datenbank-Mitteln) erkannt werden?				x	x						y
	70	Wie ist sichergestellt, dass Fernabschaltungen nur durch authorisierte Personen erfolgt?				x							Y

DPIA Content Library

Antwortmöglichkeiten A-F

A	B	C	D
Berechtigungs- Rollenkonzept, Berechtigungen nach Whitelisting-Prinzip, Minimal-Prinzip (Admin und User), Anforderungsprozess User, Logging	Berechtigungs- Rollenkonzept, Berechtigungen nach Whitelisting-Prinzip, Minimal-Prinzip (User), Anforderungsprozess User, Logging	Berechtigungs- Rollenkonzept, Minimal-Prinzip (User), Logging	Berechtigungs- Rollenkonzept, Logging
Jump Host, FW-Regeln (Whitelisting), Protokollierung, Freischaltung, 2FA auf Jump Host	Jump Host, FW-Regeln (Whitelisting), Protokollierung, Freischaltung	direkte VPN-Wartungszugänge, Freischaltung	VPN-Wartungszugänge
Rechtskonforme Löschung der Daten aus der Applikation	Löschung der Daten aus der Applikation	Keine Löschfunktion in der Applikation, lediglich Löschung der Daten auf Datenbankebene	
Daten werden je Mandant in einer separaten Instanz gehalten, das Management erfolgt über ein MDMS-System.	Daten aller Mandanten wird in einer einzigen Instanz gehalten, der Zugriff ist durch eine systemtechnisch implementierte Mandantentrennung und Berechtigungskonzept gewährleistet.		
Logging und Protokollierung von Benutzeraktivitäten, Alarmfunktion bei Anomalien	Logging und Protokollierung von kritischen / sicherheitsrelevanten Benutzeraktivitäten, Anbindung an SIEM System	Logging und Protokollierung von kritischen / sicherheitsrelevanten Benutzeraktivitäten	
Logging und Protokollierung von Benutzeraktivitäten, Alarmfunktion bei Anomalien, Data Loss Prevention Maßnahmen (4-Augen-Prinzip)	Logging und Protokollierung von kritischen / sicherheitsrelevanten Benutzeraktivitäten, Anbindung an SIEM System	Logging und Protokollierung von kritischen / sicherheitsrelevanten Benutzeraktivitäten	
Einschränkung des Zugriffs auf diese Funktion über Berechtigungen, 4-Augenprinzip zur Durchführung der Abschaltung, Aktivität wird protokolliert	Einschränkung des Zugriffs auf diese Funktion über Berechtigungen, zur Durchführung wird nur 1 Person benötigt - die Freigabe erfolgt durch einen zusätzlichen 2-Faktor, Aktivität wird protokolliert	Einschränkung des Zugriffs auf diese Funktion über Berechtigungen, Aktivität wird protokolliert	Einschränkung des Zugriffs auf diese Funktion über Berechtigungen
PW-Policy, AD-Koppelung, 2FA, keine Speicherung von Passwörtern im Klartext, Trennung der Berechtigungsvergabe (Secu-Officer, Admin)	PW-Policy, keine Speicherung von Passwörtern im Klartext, Trennung der Berechtigungsvergabe (Secu-Officer, Admin)	PW-Policy, keine Speicherung von Passwörtern im Klartext	keine Speicherung von Passwörtern im Klartext
Es existiert eine Mehrsystem-Landschaft, in welcher Updates getestet werden können. Der Testkatalog enthält auch datenschutzrelevante Testfälle. Die Durchführung der datenschutzrelevanten Testfälle erfolgt automatisch.	Es existiert eine Mehrsystem-Landschaft, in welcher Updates getestet werden können. Der Testkatalog enthält auch datenschutzrelevante Testfälle. Die Tests erfolgen manuell	Es existiert eine Mehrsystem-Landschaft, in welcher Updates getestet werden können. Der Testkatalog enthält keine datenschutzrelevanten Testfälle.	Es existiert eine Mehrsystem-Landschaft, in welcher Updates getestet werden können. Es erfolgen nur ad-hoc Tests

DPIA Content Library

Eine Datenschutz Folgeabschätzung sollte ab einem **Gefährungsgrad MITTEL** des Betroffenen oder bei oder Art. 9 / Art. 10 Daten durchgeführt werden.

Kontrollziel-Nr.	Kontrollziel	Erfüllung	Soll-Erfüllung
10	Wie ist sichergestellt, dass die Verarbeitung der personenbezogenen Daten zulässig und berechtigt ist?		F
20	Wie werden die Grundlagen der Verarbeitung bei Minderjährigen sichergestellt?		F
30	Wie ist die Zweckbindung der Verarbeitung über die Dauer der Verarbeitung sichergestellt?		C
40	Wie wird die Einhaltung des Grundsatzes der Datenminimierung sichergestellt?		C
50	Wie erfolgt bei einem V		F
60	Wie erfolgt die Abschä		F
70	Wie erfolgt die Behand		C
80	In welcher Form wird d		C
90	Wie erfolgt eine durch	n?	C
100	Wie wird dem Recht au		C
110	Welche Möglichkeit wir	r...	F

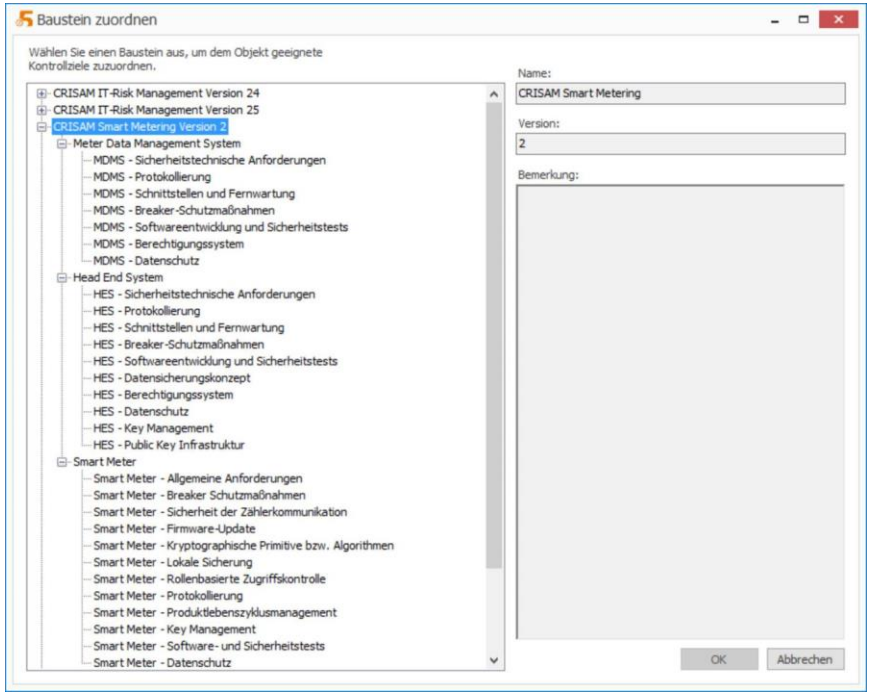
Erfüllung für Kontrollziel

- ○ A — Vom Betroffenen ist eine explizite und konkludente Einwilligung für die Verarbeitung seiner personenbezogenen Daten mit genauer Zweckbeschreibung vorhanden und/oder es besteht eine eindeutige Rechtsgrundlage für die Verarbeitung zum definierten Zweck.
- ○ B — Vom Betroffenen ist eine konkludente Einwilligung für die Verarbeitung seiner personenbezogenen Daten zum Zweck der Verarbeitung vorhanden und/oder es besteht eine Rechtsgrundlage für die Verarbeitung zum definierten Zweck.
- ○ C — Vom Betroffenen ist eine implizite Zustimmung für die Verarbeitung seiner personenbezogenen Daten zum Zweck der Verarbeitung vorhanden und/oder es besteht eine anwendbare Rechtsgrundlage für die Verarbeitung zum definierten Zweck.
- ○ D — Vom Betroffenen wird implizit über Anerkennung von AGBs der Verarbeitung seiner personenbezogenen Daten zugestimmt.
- ○ E — Der Betroffene hat der Verarbeitung seiner personenbezogenen Daten nicht widersprochen.
- ○ F — Es besteht weder eine Einwilligung, noch eine gültige Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten.
- ○ nr — nicht relevant

ISMS Katalog (Smart Metering)

Informationssicherheit der IT- und Smart Meter Infrastrukturen
(ca.200 Kontrollzielfragen als Excel-Tabelle und CRISAM® Content Libraries)

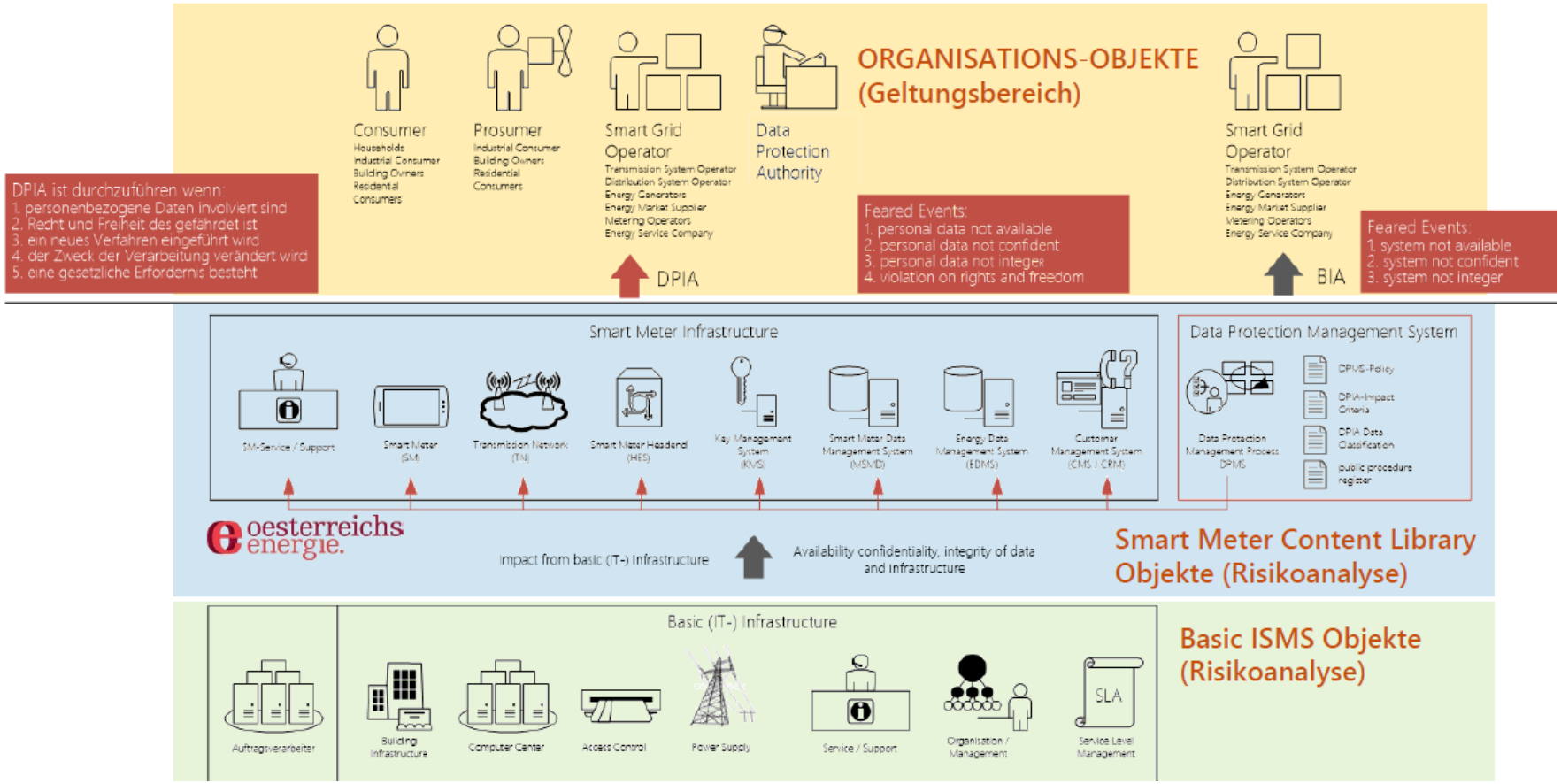
Grundlage „Anforderungskatalog Ende – zu –Ende Sicherheit Smart Metering“



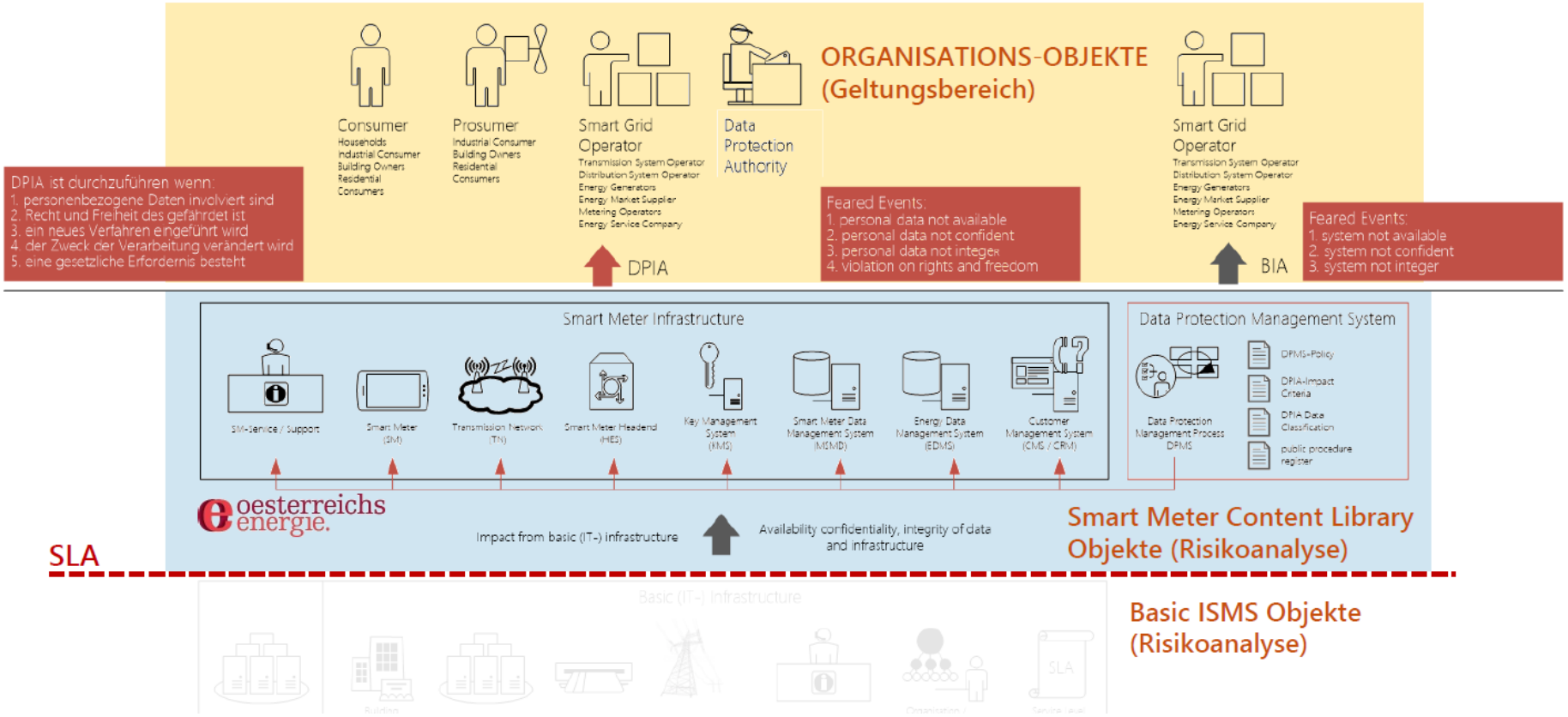
Folgende Module sind enthalten:

1. Meta Data Management System
2. Head End System
3. Smart Meter

Mögliche Implementierungsszenarien



Mögliche Implementierungsszenarien



Mögliche Implementierungsszenarien

SLA Objekt: 21 Kontrollzielfragen

Kontrollziel-Nr.	Kontrollziel	Erfüllung	Soll-Erfüllung
10	Wie sind die Anforderungen für Verfügbarkeit des Dienstleisters auf interne Erforde…	B	B
20	Wie sind die Anforderungen für Vertraulichkeit des Dienstleisters auf interne Erford…	B	B
30	Wie sind die Anforderungen für Integrität des Dienstleisters auf interne Erfordernis…	B	B
40	Wie wird die Einhaltung der SLAs sichergestellt?	B	B
50	Wie wird die Einhaltung der SLAs überprüft?	B	B
60	Wie wird die Leistungsfähigkeit des Dienstleisters plausibilisiert?	B	B
70	Wie wird die Veränderung des Stands der Technik abgedeckt?	A	A
80	Sind Servicezeiten festgelegt?	B	B
90	Sind Wartungsfenster festgelegt?	B	B
100	Wie sind Rechte und Pflichten bei der Vertragserfüllung definiert?	B	B
105	Existiert ein Betriebskonzept, das auch die Sicherheitsaspekte berücksichtigt?	B	B

Erfüllung für Kontrollziel

- ○ A
- ◉ B Anforderungen werden periodisch nachjustiert.
- ○ C Anforderungen wurden einmalig festgelegt.
- ○ D
- ○ E Anforderungen wurden vom Dienstleister festgelegt.
- ○ F Es sind keine Anforderungen definiert.
- ○ nr

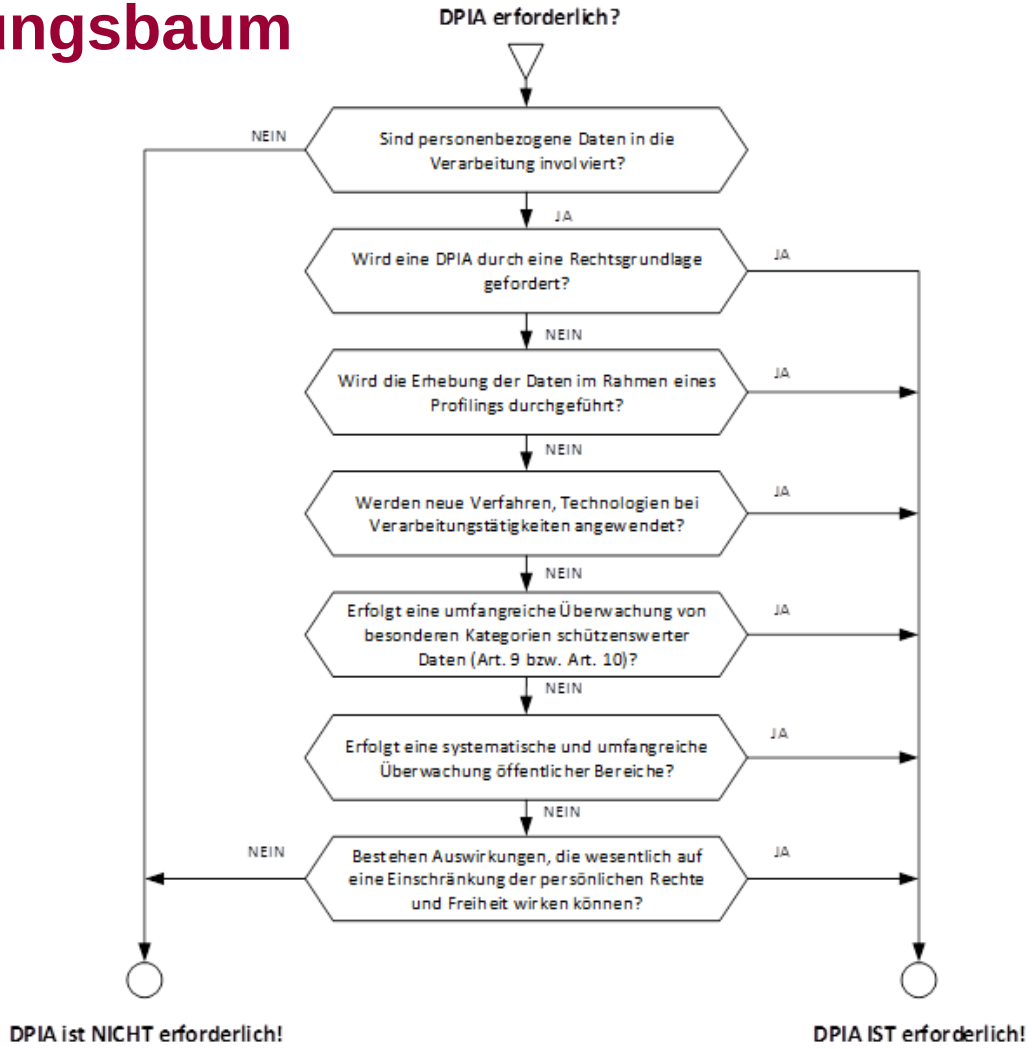
DPIA White Paper

- Beschreibung des DPIA Verfahrens
- Entscheidungsbaum DPIA
- Branchen Privacy Impact Assessment (PIA)

Musterprojekt

- Beschreibt die Anwendung der DPIA Content Library
- Verknüpfen von DSMS und ISMS

Entscheidungsbaum

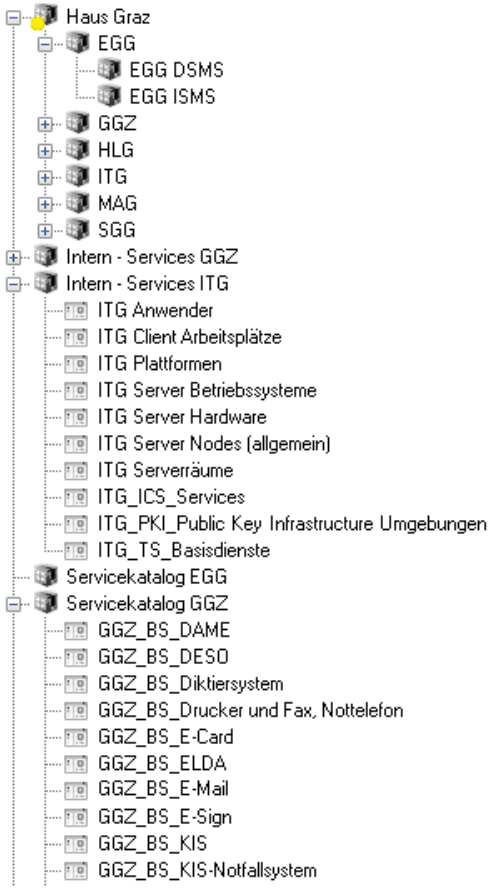


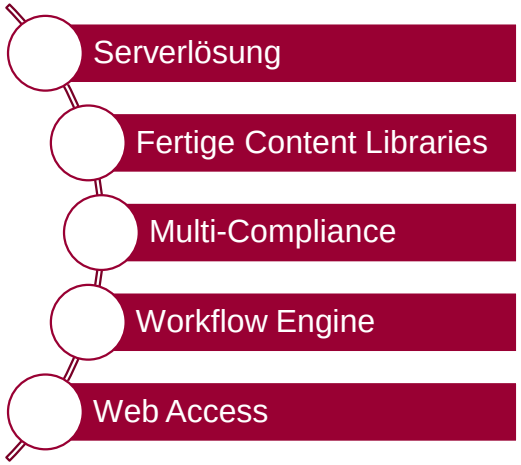
Verhaltensregeln / Interne Arbeitshilfe für Netzbetreiber

- „Spezifische“ Begriffsbestimmungen (neben Begriffen des DSGVO);
- Datenschutzrechtliche Rollenverteilung: Auftraggeber, Dienstleister – Übermittlungsempfänger, Betroffener (=„Datensubjekt“);
- Darlegung der gesetzlichen Rahmenbedingungen und Grundlagen für die Datenverwendung:
- Arten und Wege zulässiger Datenerhebung;
- Zulässigkeit der Verwendung bestimmter Arten oder Kategorien von Daten als Auftraggeber für bestimmte Zwecke;
- Organisatorische Datensicherheitsaspekte;
- Betroffenenrechte (Auskunft, Löschung, Widerspruch)

Vorgehen in der ENERGIE GRAZ

- Datenschutz-Informationssicherheitsprojekt
- Koordination Haus Graz
- Gemeinsame IT Serviceliste
- Ein System Datenschutz Informationssicherheit





crisam DECISION ENGINEERING

Nutzen

- Einheitliches Verfahren für DPIA
- Bereitstellung von Arbeitsunterlagen
- Abdeckung der gesetzlichen Anforderungen
- Grundgerüst für DSMS / ISMS in den Organisationen