



Einsatzmöglichkeiten von ADONIS und ADOIT im Kontext der Europäische Datenschutzgrundverordnung

Inhalt

1. DSGVO?
2. Unterstützung durch ADOIT und ADONIS
3. Detailbetrachtung: Verzeichnis von Verarbeitungstätigkeiten
 - I. Grundsätzlicher Aufbau, Struktur und Inhalt
 - II. Granularität und Detailgrad
 - III. Verarbeitungstätigkeiten unterschiedlicher Verantwortlicher
4. Verzeichnis von Verarbeitungstätigkeiten: Umsetzung in ADOIT und ADONIS
 - I. Verwendete Assets und Attribute
 - II. Reporting und Sichten



Inhalt

1. Theoretische Grundlagen

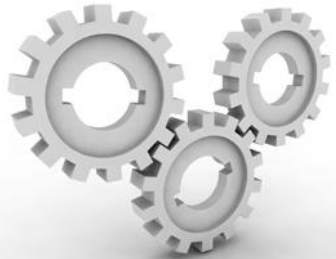
2. Unterstützung durch ADOIT und ADONIS

3. Detailbetrachtung: Verzeichnis von Verarbeitungstätigkeiten

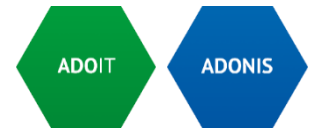
- I. Grundsätzlicher Aufbau, Struktur und Inhalt
- II. Granularität und Detailgrad
- III. Verarbeitungstätigkeiten unterschiedlicher Verantwortlicher

4. Verzeichnis von Verarbeitungstätigkeiten: Umsetzung in ADOIT und ADONIS

- I. Verwendete Assets und Attribute
- II. Reporting und Sichten



EU-DSGVO: Theoretische Grundlagen



GDPR (General Data Protection Regulation) – EU Datenschutz Grundverordnung

▶ **Historie**

- ▶ Beschluss im Europäischen Parlament 24. Mai 2016
- ▶ Umsetzungsfrist 2 Jahre → Inkrafttreten der Verordnung am 25. Mai 2018

▶ **Geltungsbereich**

- ▶ Gilt direkt und muss nicht im Parlament in nationales Recht umgesetzt werden
- ▶ Direkte Anwendung der Datenschutzgrundverordnung in allen EU Staaten
- ▶ Gültig für alle in der EU tätigen Unternehmen (auch wenn HQ nicht in EU)

▶ **ABER...**

- ▶ Einige Interpretationsspielräume in der Anwendung der DSGVO, z.B. Dokumentationstiefe

Warum auch in der CH betroffen?

what are other
words for
extraterritorial?



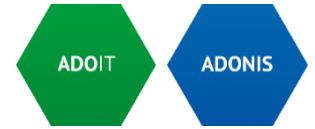
extraterritorial, outdoor, outer,
external, extraterrestrial,
foreign, peripheral, over,
surface, extraneous



Thesaurus.plus

- ▶ Ausserdem: Überarbeitung des DSG
 - ▶ Der Bundesrat will den Datenschutz an das Internet-Zeitalter anpassen und die Stellung der Bürgerinnen und Bürger stärken. Parallel dazu gleicht er das Schweizer Recht an die Entwicklung in der EU und im Europarat an [...] Der Bundesrat hat an seiner Sitzung vom 15. September 2017 eine entsprechende Botschaft verabschiedet. [Medienmitteilung](#)
 - ▶ Angleichung des schweizerischen Datenschutzrechts an die europäischen und völkerrechtlichen Entwicklung zur Sicherstellung eines reibungslosen und funktionierenden grenzüberschreitenden Datenaustauschs.

EU-DSGVO: Theoretische Grundlagen



GDPR (General Data Protection Regulation) – EU Datenschutz Grundverordnung

▶ **Wesentliche Änderungen**

- ▶ Deutlich erhöhter Strafraumen: Bis zu 4 % des weltweiten Jahresumsatzes
- ▶ Erhöhte Dokumentationspflichten
- ▶ Recht auf Herausgabe der Daten: Jeder der Daten „hergibt“, muss diese auch wieder einfordern können
- ▶ Recht auf Vergessenwerden
- ▶ Verpflichtender Datenschutzbeauftragter
- ▶ Data Breach Notification: Betroffene (aktuell auch) & Behörde (aktuell nicht)

GDPR (General Data Protection Regulation) – EU Datenschutz Grundverordnung

- ▶ **Betroffene:**
ist eine natürliche oder juristische Personen oder Personengemeinschaften, deren Daten von einem Auftraggeber verwendet werden.
- ▶ **Verantwortlicher** (früher: Auftraggeber):
ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.
- ▶ **Auftragsverarbeiter** (früher: Dienstleister):
ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen bearbeitet.



EU-DSGVO: Herausforderungen für Unternehmen

GDPR – General Data Protection Regulation

- Grundsätze der Datenübermittlung
 - Sicherheit der Datenverarbeitung (technische und organisatorische Maßnahmen)
- Grundsätze für die Verarbeitung
- Datenschutz-Folgenabschätzung
- Informationspflicht
- Garantien zur Datenübermittlung
- Verzeichnis von Verarbeitungstätigkeiten
- Rechte der betroffenen Personen (Recht auf Auskunft, Löschung, Berichtigung, ...)
- Empfänger der Datenübermittlung
- Zertifizierungen
- Rechtmäßigkeit der Verarbeitung



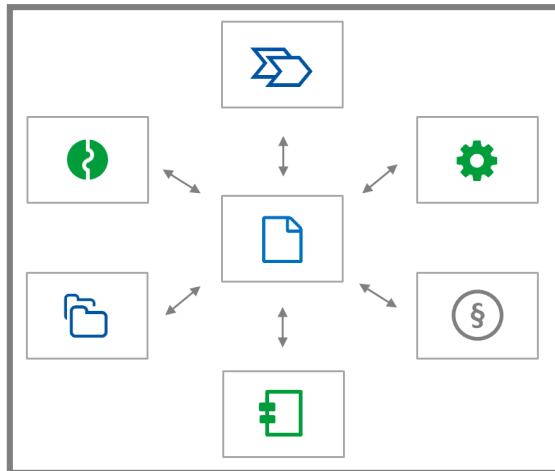
Inhalt

1. Theoretische Grundlagen
2. Unterstützung durch **ADOIT** und **ADONIS**
3. Detailbetrachtung: Verzeichnis von Verarbeitungstätigkeiten
 - I. Grundsätzlicher Aufbau, Struktur und Inhalt
 - II. Granularität und Detailgrad
 - III. Verarbeitungstätigkeiten unterschiedlicher Verantwortlicher
4. Verzeichnis von Verarbeitungstätigkeiten: Umsetzung in ADOIT und ADONIS
 - I. Verwendete Assets und Attribute
 - II. Reporting und Sichten



Datenschutzaspekte im Kontext der Unternehmensarchitektur

Unterstützung durch das BOC Management Office

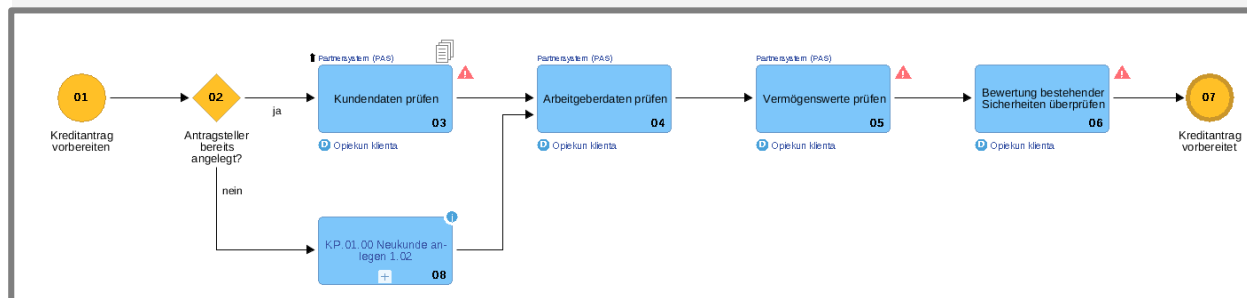


✓ Handlungsbedarfe (Risiken) identifizieren

✓ Maßnahmen bewerten

	Controls against malware	Information backup	Key management	Management of privileged access rights	Removal or adjustment of access rights	Technical compliance review	User registration and de-registration
Accounts and Payments System (GIR)	Yellow circle with arrow		Green circle with arrow	Green circle with arrow	Yellow circle with arrow		Yellow circle with arrow
Business Partner	Green circle with arrow	Green circle with arrow		Red circle with arrow	Yellow circle with arrow		
Credit Manager (CMA)	Yellow circle with arrow		Yellow circle with arrow			Green circle with arrow	
Partner System (PAS)	Yellow circle with arrow	Green circle with arrow	Yellow circle with arrow	Red circle with arrow	Yellow circle with arrow	Red circle with arrow	Green circle with arrow
Working Capital Analytics System (WAC)	Red circle with arrow	Red circle with arrow	Green circle with arrow			Green circle with arrow	

✓ Technische & organisatorische Maßnahmen definieren & implementieren



Inhalt

1. Theoretische Grundlagen
2. Unterstützung durch ADOIT und ADONIS
3. **Detailbetrachtung: Verzeichnis von Verarbeitungstätigkeiten**
 - I. Grundsätzlicher Aufbau, Struktur und Inhalt
 - II. Granularität und Detailgrad
 - III. Verarbeitungstätigkeiten unterschiedlicher Verantwortlicher
4. Verzeichnis von Verarbeitungstätigkeiten: Umsetzung in ADOIT und ADONIS
 - I. Verwendete Assets und Attribute
 - II. Reporting und Sichten



Art. 30 der DSGVO – Verzeichnis von Verarbeitungstätigkeiten

Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben:

- ▶ den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten.
- ▶ Die Zwecke der Verarbeitung
- ▶ eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten
- ▶ die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen
- ▶ gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien.
- ▶ wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien
- ▶ wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 32 Absatz 1)

EU-DSGVO: Verzeichnis von Verarbeitungstätigkeiten



Verzeichnis aller Verarbeitungstätigkeiten: Aufbau, Struktur und Inhalt

Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen							
Unternehmen	Firma XY Straße XY Stadt XY	Geschäftsführung	Name XY Anschrift XY Kontaktdaten XY	Verantwortlicher	Name XY Kontaktdaten XY	Datenschutzbeauftragter	Name XY Kontaktdaten XY
Bezeichnung der Verarbeitungstätigkeit	Zwecke der Verarbeitung	Kategorien personenbez. Daten	Kategorien betroffener Personen	Kategorien von Empfängern	IT-Anwendung / -Tool	Risiken	Techn. und org. Maßnahmen
Antrag Haushaltversicherung bearbeiten	Antrag Haushaltsversicherung bearbeiten	Adressdaten Geburtsdaten	Kunden	Cloud Provider	Versicherungssystem XY	Unbefugter Zugriff	Passwortschutz
Antrag Lebensversicherung bearbeiten	Antrag Lebensversicherung bearbeiten	Adressdaten Geburtsdaten Gesundheitsdaten	Kunden	Cloud Provider Gesundheitsamt	Versicherungssystem XY	Unbefugter Zugriff	Passwortschutz
Bewerbungsverfahren	Bewerber vorauswählen Bewerbungen sichten Bewerbungsgespräch führen	Adressdaten Geburtsdaten	Bewerber	IT Abteilung	Notes Mail Client	Unbefugter Zugriff	Passwortschutz
Lohnabrechnung	Lohnabrechnung	Adressdaten Bankverbindung Sozialversicherungsdaten	Mitarbeiter	Finanzamt	SAP HR Finanz Online	Unbefugter Zugriff	Passwortschutz
FATCA Meldung	Gesetzliche Meldepflicht	Steuererhebliche Daten	Kunde	US Steuerbehörde	FATCA Online	Unbefugter Zugriff	Passwortschutz

Europäische Datenschutzgrundverordnung

Verzeichnis von Verarbeitungstätigkeiten



Verzeichnis aller Verarbeitungstätigkeiten: Granularität und Detailgrad

Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen

Unternehmen	Firma XY Straße XY Stadt XY	Geschäftsführung	Name XY Anschrift XY Kontaktdaten XY	Verantwortlicher	Name XY Kontaktdaten XY	Datenschutzbeauftragter	Name XY Kontaktdaten XY
--------------------	-----------------------------------	-------------------------	--	-------------------------	----------------------------	--------------------------------	----------------------------

Bezeichnung der Verarbeitungstätigkeit	Zwecke der Verarbeitung	Kategorien personenbez. Daten	Kategorien betroffener Personen	Kategorien von Empfängern	IT-Anwendung / -Tool	Risiken	Techn. und org. Maßnahmen
Antrag Haushaltversicherung bearbeiten	Antrag Haushaltsversicherung bearbeiten	Adressdaten Geburtsdaten	Kunden	Cloud Provider	Versicherungssystem XY	Unbefugter Zugriff	Passwortschutz
Antrag Lebensversicherung bearbeiten	Antrag Lebensversicherung bearbeiten	Adressdaten Geburtsdaten Gesundheitsdaten	Kunden	Cloud Provider Gesundheitsamt	Versicherungssystem XY	Unbefugter Zugriff	Passwortschutz

Unterscheidung von „Verarbeitungstätigkeit“ und „Zweck der Verarbeitung“ im Zuge der Detaillierung

Europäische Datenschutzgrundverordnung

Verzeichnis von Verarbeitungstätigkeiten



Verzeichnis aller Verarbeitungstätigkeiten: Unterschiedliche Verantwortliche

**Unterschiedliche
Verantwortliche**

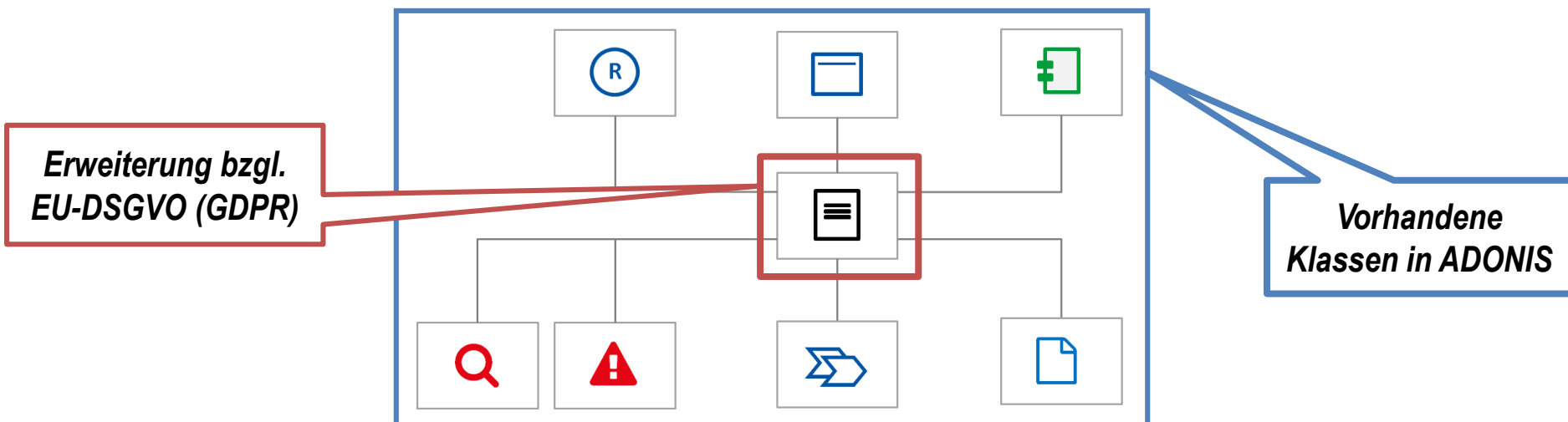
Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen							
Unternehmen	Firma XY Straße XY Stadt XY	Geschäftsführung	Name XY Anschrift XY Kontaktdaten XY	Verantwortlicher	Name XY Kontaktdaten XY	Datenschutzbeauftragter	Name XY Kontaktdaten XY
Bezeichnung der Verarbeitungstätigkeit	Zwecke der Verarbeitung	Kategorien personenbez. Daten	Kategorien betroffener Personen	Kategorien von Empfängern	IT-Anwendung / -Tool	Risiken	Techn. und org. Maßnahmen
Antrag Haushaltversicherung bearbeiten	Antrag Haushaltversicherung bearbeiten	Adressdaten Geburtsdaten	Kunden	Cloud Provider	Versicherungssystem XY	Unbefugter Zugriff	Passwortschutz
Antrag Lebensversicherung bearbeiten	Antrag Lebensversicherung bearbeiten	Adressdaten Geburtsdaten Gesundheitsdaten	Kunden	Cloud Provider Gesundheitsamt	Versicherungssystem XY	Unbefugter Zugriff	Passwortschutz

Verzeichnis aller Verarbeitungstätigkeiten

Aufbau, Struktur und Inhalt

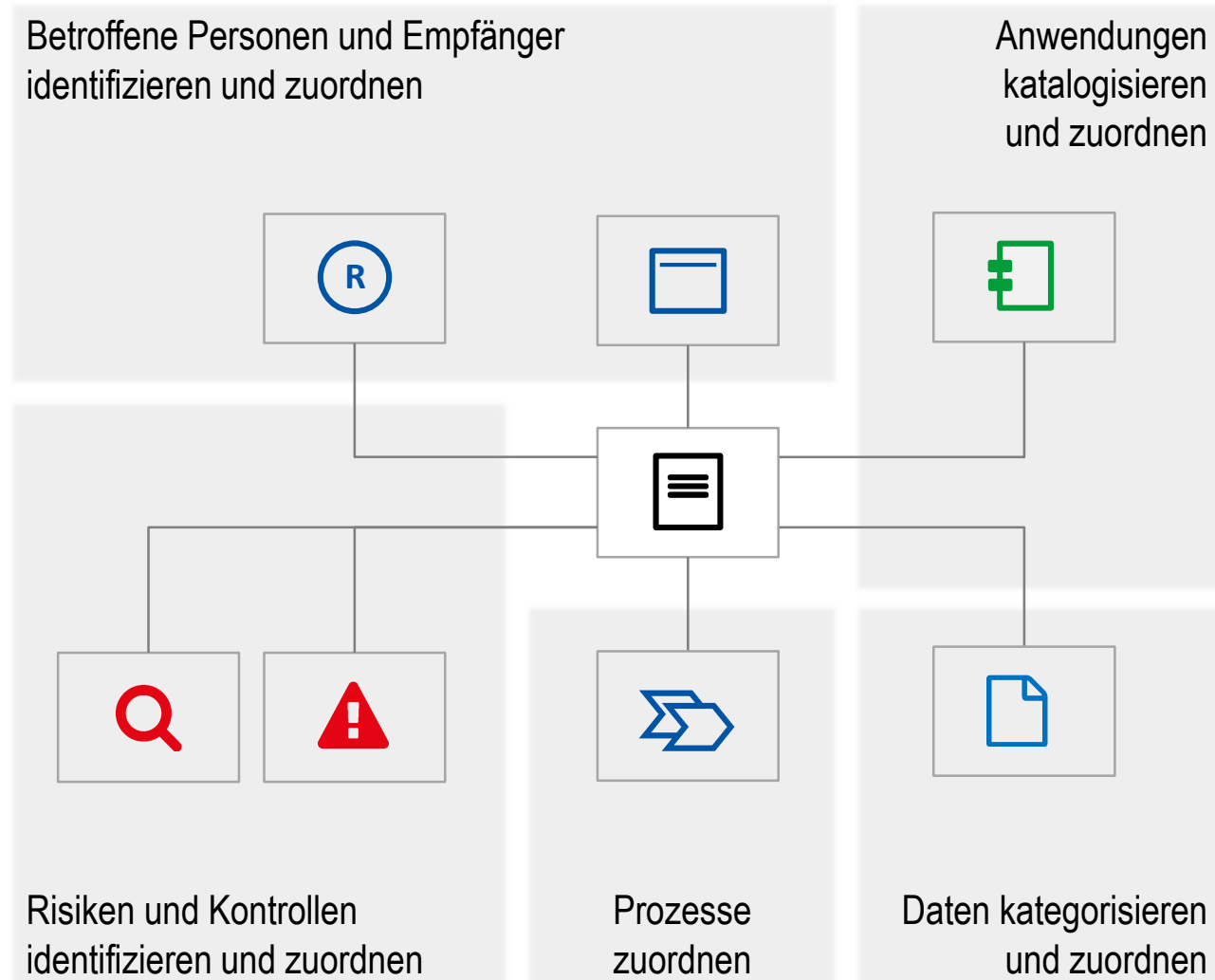
Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen

Unternehmen	Firma XY Straße XY Stadt XY	Geschäftsführung	Name XY Anschrift XY Kontaktdaten XY	Datenschutzbeauftragter	Name XY Kontaktdaten XY					
Bezeichnung der Verarbeitungstätigkeit	Zwecke der Verarbeitung	Rechtsgrundlage der Verarbeitung	Kategorien personenbezogener Daten	Löschfrist	Kategorien betroffener Personen	Kategorien von Empfängern	IT-Anwendung / -Tool	Risiken	Techn. und org. Maßnahmen	Datenschutz-Folgenabschätzung
Bewerbungsverfahren	Bewerber vorauswählen Bewerbungen sichten Bewerbungsgespräch führen	§ X Abs. Y Gesetz Z	Adressdaten Geburtsdaten	10 Jahre	Bewerber	IT Abteilung	Notes Mail Client	Unbefugter Zugriff	Passwortschutz	notwendig
Lohnabrechnung	Lohnabrechnung	§ X Abs. Y Gesetz Z	Adressdaten Bankverbindung Sozialversicherungsdaten	5 Jahre	Mitarbeiter	Finanzamt	SAP HR	Unbefugter Zugriff	Passwortschutz	notwendig



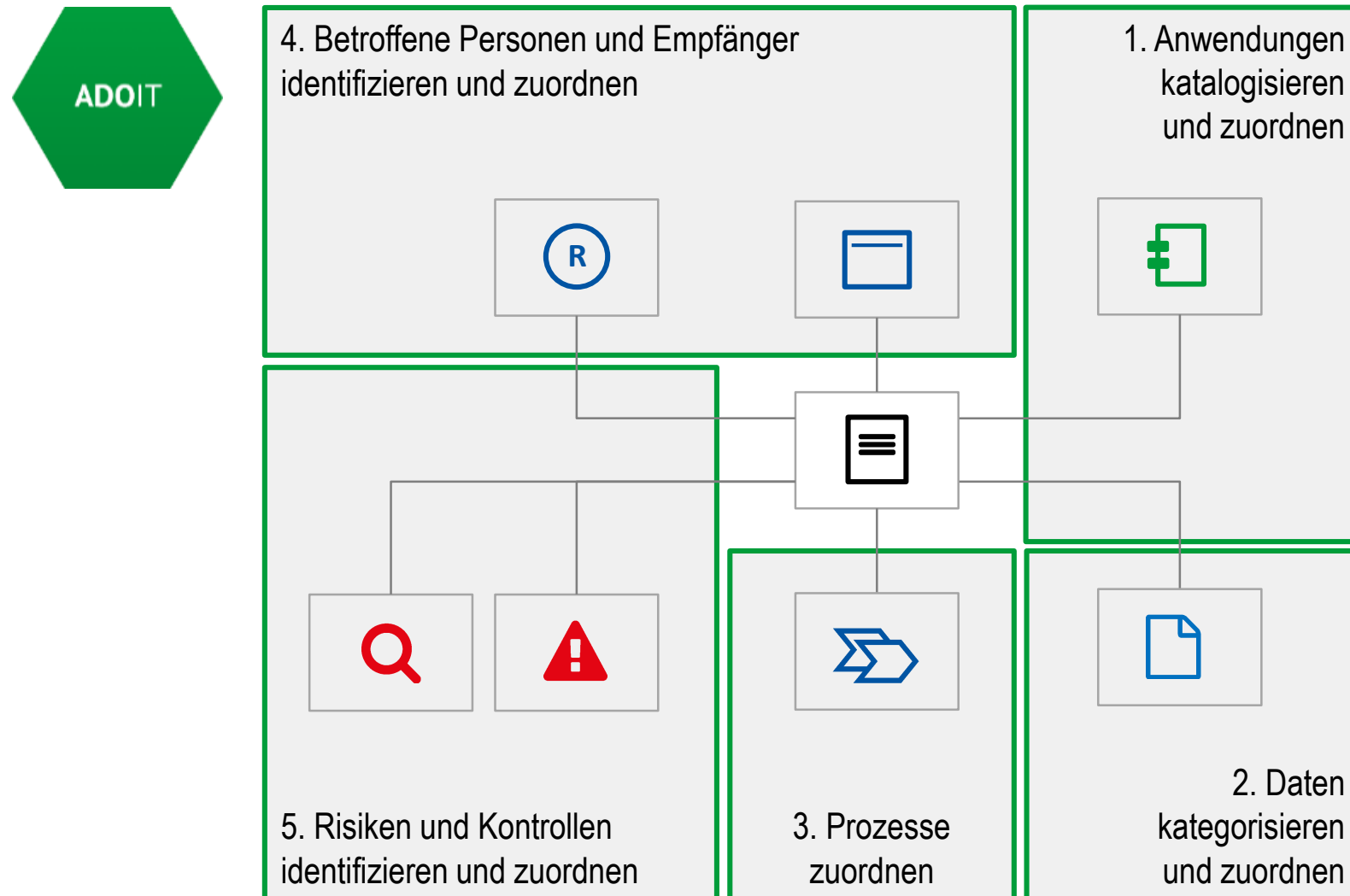
Verzeichnis aller Verarbeitungstätigkeiten

Methodische Herangehensweise



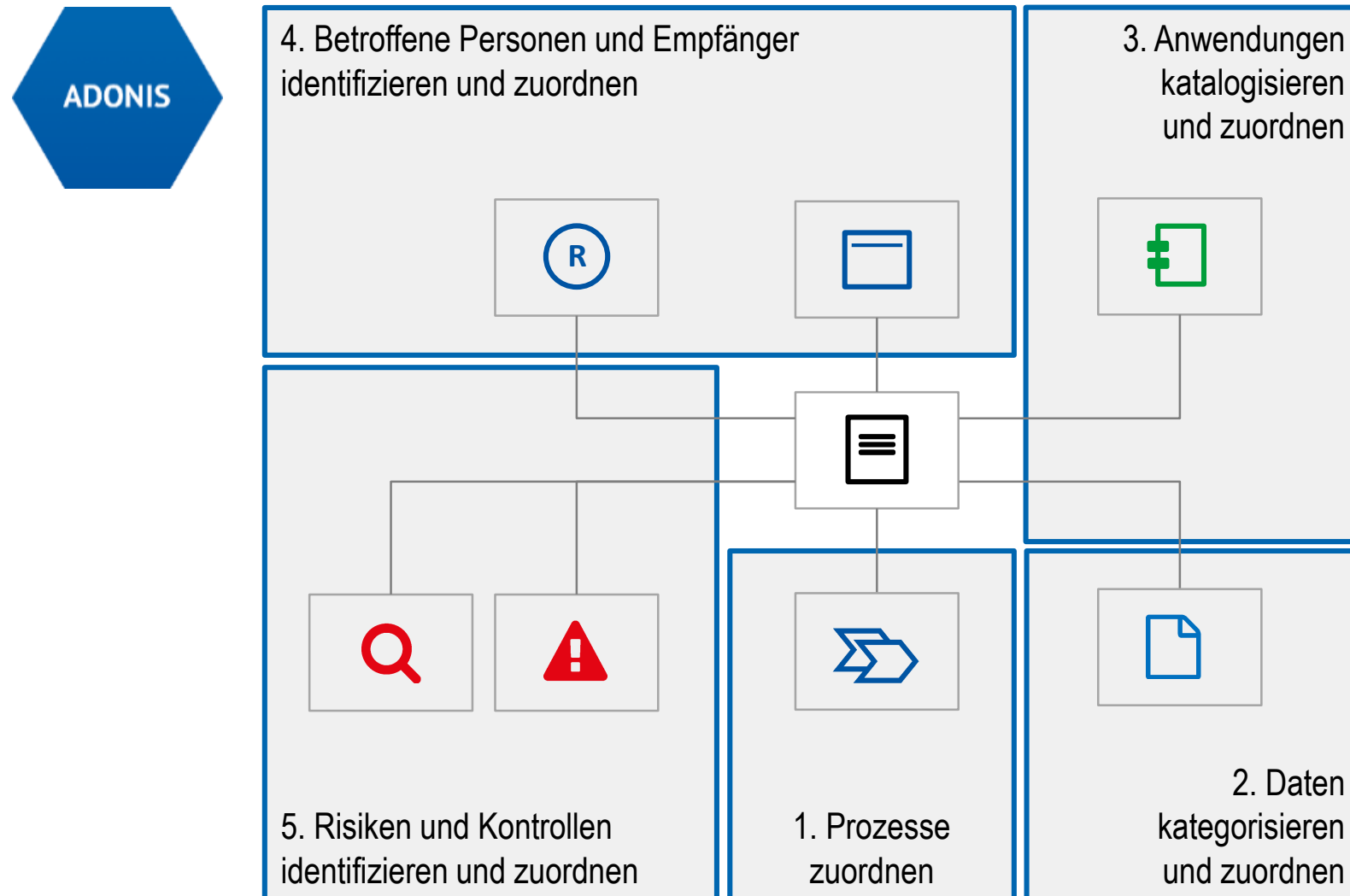
Verzeichnis aller Verarbeitungstätigkeiten

Methodische Herangehensweise in ADOIT



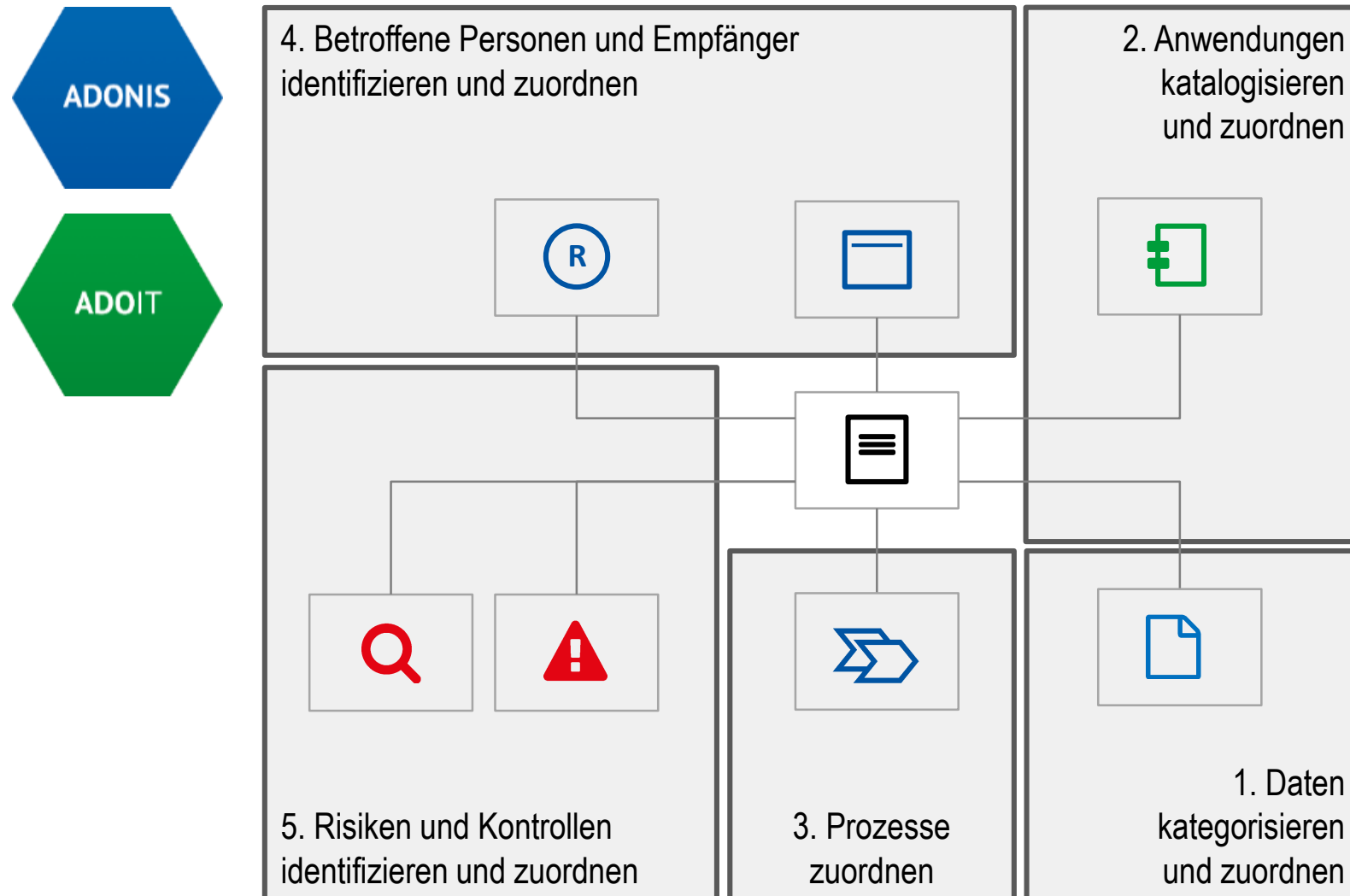
Verzeichnis aller Verarbeitungstätigkeiten

Methodische Herangehensweise in ADONIS



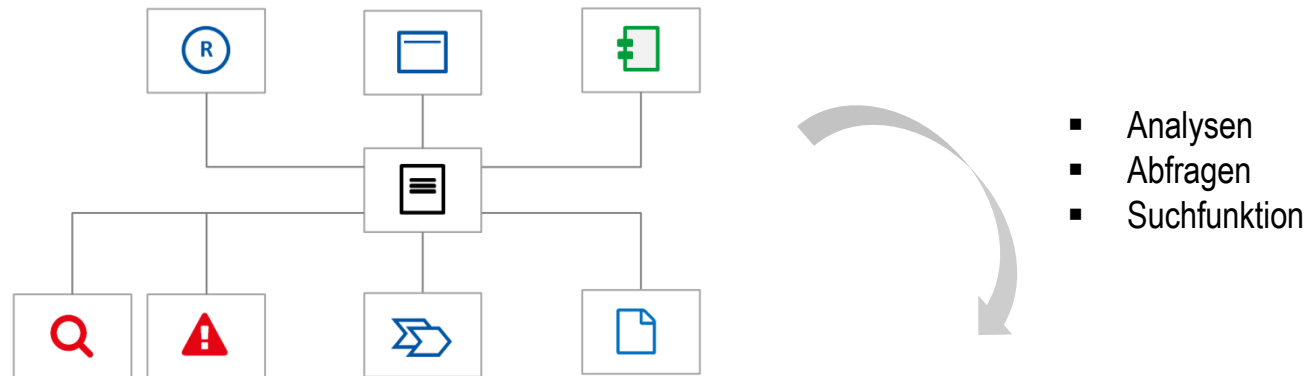
Verzeichnis aller Verarbeitungstätigkeiten

Methodische Herangehensweise: Ausgehend aus dem Datenmanagement



Verzeichnis aller Verarbeitungstätigkeiten

Datenschutz spezifische Auswertungen und Reports



Typ	Name	Kategorien personenbezogener Daten	Kategorien betroffen...	Kategorie von Emp...	Zweck	Verarbeitende Anwe...	Risiken	Eingehende Bezie...
	Bewerbungsverfahren	[2] Adressdaten, Geburtsdaten	[1] Bewerber	[1] IT Abteilung	[3] Bewerber vorausw...	[1] Notes Mail Client	[1] Unbefugter Zugriff	[1] Passwortschutz
	Lohnabrechnung	[3] Adressdaten, Bankverbindung, Sozialversic...	[1] Mitarbeiter	[1] Finanzamt	[1] Lohnabrechnung 0...	[1] SAP HR	[1] Unbefugter Zugriff	[1] Passwortschutz

Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen										
Unternehmen		Geschäftsführung			Datenschutzbeauftragter					
Firma XY Straße XY Stadt XY		Name XY Anschrift XY Kontaktdaten XY			Name XY Kontaktdaten XY					
Bezeichnung der Verarbeitungstätigkeit	Zwecke der Verarbeitung	Rechtsgrundlage der Verarbeitung	Kategorien personenbezogener Daten	Löschfrist	Kategorien betroffener Personen	Kategorien von Empfängern	IT-Anwendung / - Tool	Risiken	Techn. und org. Maßnahmen	Datenschutz-Folgenabschätzung
Bewerbungsverfahren	Bewerber vorauswählen Bewerbungen sichten Bewerbungsgespräch führen	§ X Abs. Y Gesetz Z	Adressdaten Geburtsdaten	10 Jahre	Bewerber	IT Abteilung	Notes Mail Client	Unbefugter Zugriff	Passwortschutz	notwendig
Lohnabrechnung	Lohnabrechnung	§ X Abs. Y Gesetz Z	Adressdaten Bankverbindung Sozialversicherungsdaten	5 Jahre	Mitarbeiter	Finanzamt	SAP HR	Unbefugter Zugriff	Passwortschutz	notwendig

Verzeichnis aller Verarbeitungstätigkeiten

Matrix auswählen ↑

DSGVO: Welche Anwendungen verarbeiten welche Daten in den Verarbeitungstätigkeiten?

DSGVO: Welche Daten werden verarbeitet?

DSGVO: Welche Personen sind von der Verarbeitung betroffen?

DSGVO: Welche sind die verarbeitende Anwendungen?

DSGVO: Wer ist der Verantwortliche?

DSGVO: Wer sind die Empfänger der Daten?

DSGVO: Zweck der Verarbeitung

Das Diagramm zeigt drei überlappende Fenster, die Datenflüsse zwischen verschiedenen Systemen und Datenbanken darstellen. Die Fenster sind durch Pfeile verbunden, die den Datenfluss andeuten.

Fenster 1 (oben links):

- Spaltenüberschriften:** Antrag Haushaltsversicherung..., Antrag Lebensversicherung b..., Bewerbungsverfahren, Lohnabrechnung, Vertragsabwicklung
- Zeilenüberschriften:** Bewerber, Kunden, Mitarbeiter
- Inhalt:** Die Zellen sind größtenteils leer, mit Ausnahme von grünen Pfeilen in den Spalten 'Antrag Lebensversicherung b...' und 'Lohnabrechnung'.

Fenster 2 (unten links):

- Spaltenüberschriften:** Antrag Haushaltsversicherung..., Antrag Lebensversicherung b..., Bewerbungsverfahren, Lohnabrechnung, Vertragsabwicklung
- Zeilenüberschriften:** Adressdaten, Bankverbindung, Geburtsdatum, Geschäftsobjekt, Gesundheitsdaten, Sozialversicherungsdaten
- Inhalt:** Die Zellen sind größtenteils leer, mit Ausnahme von grünen Pfeilen in den Spalten 'Antrag Lebensversicherung b...' und 'Lohnabrechnung'.

Fenster 3 (unten rechts):

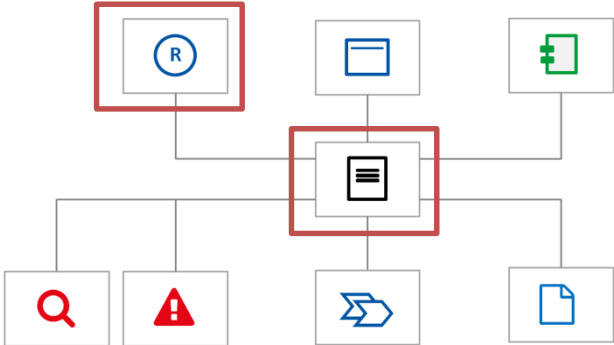
- Spaltenüberschriften:** Antrag Haushaltsversicherung..., Antrag Lebensversicherung b..., Bewerbungsverfahren, Lohnabrechnung, Vertragsabwicklung
- Zeilenüberschriften:** Martha Musterfrau, Max Mustermann, Otto Normalverbraucher
- Inhalt:** Die Zellen sind größtenteils leer, mit Ausnahme von grünen Pfeilen in den Spalten 'Antrag Lebensversicherung b...' und 'Lohnabrechnung'.

Die Pfeile verdeutlichen die Datenflüsse zwischen den verschiedenen Systemen und Datenbanken.

Verzeichnis aller Verarbeitungstätigkeiten

Datenschutz spezifische Auswertungen und Reports

- ▶ Welche Personen sind von der Verarbeitung betroffen?



Legende:

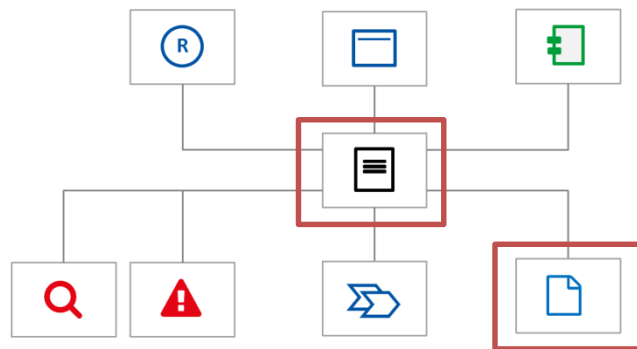
	Verarbeitungstätigkeit
	Rolle
	Kategorie betroffener Personen

	Antrag Haushaltsversicherun...	Antrag Lebensversicherung b...	Bewerbungsverfahren	Lohnabrechnung
Bewerber				
Kunden				
Mitarbeiter				

Verzeichnis aller Verarbeitungstätigkeiten

Datenschutz spezifische Auswertungen und Reports

- ▶ Welche Daten werden verarbeitet?



Legende:

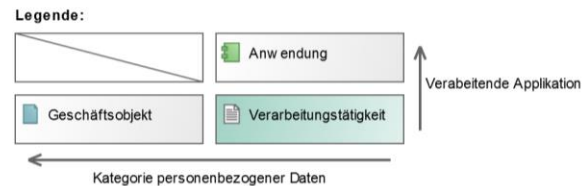
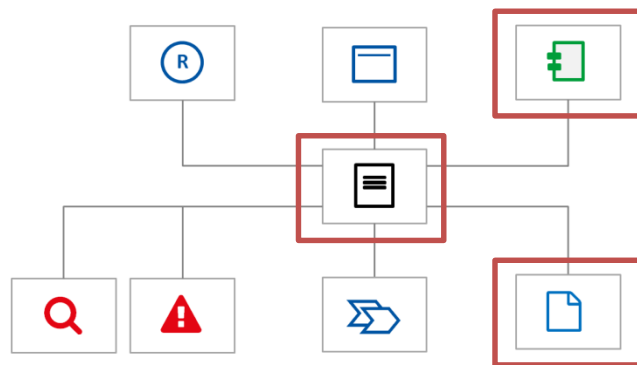
	Verarbeitungstätigkeit
	Geschäftsobjekt
	Kategorie personenbezogener Daten

	Antrag Haushaltsversicherun...	Antrag Lebensversicherung b...	Bewerbungsverfahren	Lohnabrechnung
Adressdaten				
Bankverbindung				
Geburtsdatum				
Geschäftsobjekt				
Gesundheitsdaten				
Sozialversicherungsdaten				

Verzeichnis aller Verarbeitungstätigkeiten

Datenschutz spezifische Auswertungen und Reports

- ▶ Welche Anwendungen verarbeiten welche Daten in den Verarbeitungstätigkeiten?



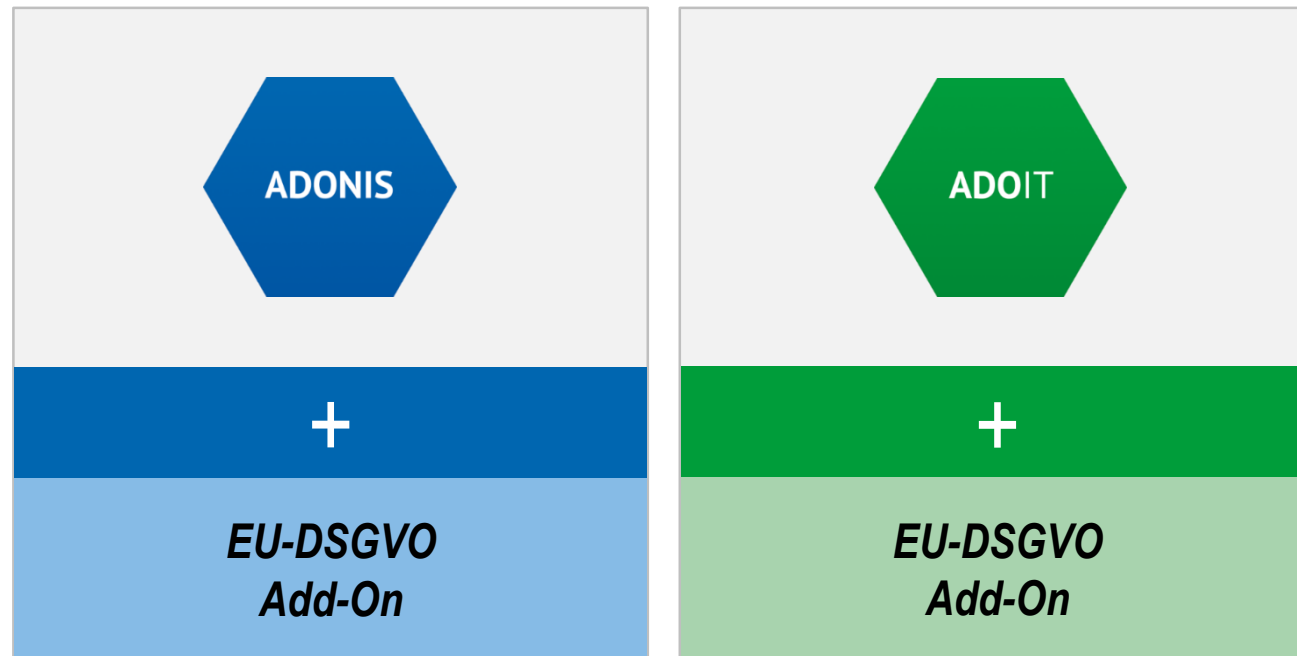
	Anwendung	Notes Mail Client	SAP HR	Versicherungssystem XY	Keine Referenzen
Adressdaten		Bewerbungsverfahren	Lohnabrechnung	Antrag Haushaltsversicheru... Antrag Lebensversicherung ...	
Bankverbindung			Lohnabrechnung		
Geburtsdatum		Bewerbungsverfahren		Antrag Haushaltsversicheru... Antrag Lebensversicherung ...	
Geschäftsobjekt	Verarbeitungstätigkeit				
Gesundheitsdaten				Antrag Lebensversicherung ...	
Sozialversicherungsdaten			Lohnabrechnung		
Keine Referenzen					Vertragsabwicklung

Datenschutz spezifische Auswertungen und Reports



Europäische Datenschutzgrundverordnung

Unser Angebot an Sie!



✓ ADONIS/ADOIT Add-On-Modul (= Methodenerweiterung)

✓ Trainings- und Coaching-Workshop

✓ Weiterführender Beratungssupport

Sprechen Sie uns an! Wir freuen uns auf detailliertere Diskussion und Präsentationen!

Die BOC Group in Sozialen Medien

Folgen Sie uns auf LinkedIn



**ADONIS -
Business Process Management**

Showcase page



BOC Group

Company page



**ADOIT –
Enterprise Architecture**

Showcase page

Folgen Sie uns auf Twitter: @BOC_Group

