ARIS

DSGVO-KONVENTIONEN FÜR ARIS-ACCELERATOREN

VERSION 10.0 - SERVICE RELEASE 10

Oktober 2019

This document applies to ARIS Version 10.0 and to all subsequent releases.

Specifications contained herein are subject to change and these changes will be reported in subsequent release notes or new editions.

Inhalt

1 Textkonventionen

Im Text werden Menüelemente, Dateinamen usw. folgendermaßen kenntlich gemacht:

- Menüelemente, Tastenkombinationen, Dialoge, Dateinamen, Eingaben usw. werden **fett** dargestellt.
- Eingaben, über deren Inhalt Sie entscheiden, werden **<fett und in spitzen Klammern>** dargestellt.
- Einzeilige Beispieltexte werden am Zeilenende durch das Zeichen ↵ getrennt, z. B. ein langer Verzeichnispfad, der aus Platzgründen mehrere Zeilen umfasst.
- Dateiauszüge werden in folgendem Schriftformat dargestellt:

  ```
  Dieser Absatz enthält einen Dateiauszug.
  ```

- Warnungen werden farbig hinterlegt:

  Warnung

  Dieser Absatz enthält eine Warnung.

2 Einleitung

Um das Anlegen von Datenschutz-Management-Informationen und -Funktionalitäten zu vereinfachen und deren Wiederverwendbarkeit zu ermöglichen, können Sie Objekte in ARIS Architect modellieren. Diese Objekte werden dann von den Workflows von ARIS Risk & Compliance Manager verwendet. Dies ist jedoch nur möglich, wenn Sie die methodischen und funktionalen Regeln und Konventionen für das Modellieren in ARIS Architect einhalten. Nur dann können alle modellierten Daten nach ARIS Risk & Compliance Manager übertragen und dort wiederverwendet werden. Um diese Objekte in ARIS Architect ordnungsgemäß pflegen zu können, beachten sie die Informationen im Handbuch **ARCM – General conventions** und im jeweiligen Konventionenhandbuch für die Workflows von ARIS Risk & Compliance Manager.

3 Inhalt des Dokuments

In den nachfolgenden Abschnitten werden die Standards für die Verwendung von Beschreibungssichten, Modelltypen, Objekttypen, Beziehungs- und Kantentypen sowie Attributen erklärt.

3.1 Ziele und Umfang

Ziel: Angabe von Modellierungsrichtlinien

Nicht in diesem Handbuch enthalten: Benutzerdokumentation

3.2 Voraussetzungen

Um die folgenden Konventionen verwenden zu können, importieren Sie zuerst den Filter **GDPR method extension** in ARIS Architect. Er fügt abgeleitete und benutzerdefinierte Methodenkonstrukte (Modelltypen, Objekttypen, Symbole, Kantentypen, Attributtypgruppen und Attributtypen) zur ARIS-Methode hinzu. Diese Methodenkonstrukte sind für die DSGVO erforderlich. Alle anderen Acceleratoren basieren auf dieser erweiterten ARIS-Methode.

Die DSGVO-Methodenerweiterungen verwenden Sie, indem Sie entweder den Filter **Gesamtmethode** anwenden oder die DSGVO-Methodenerweiterungen einem bestehenden ARIS-GRC-Filter hinzufügen. Der DSGVO-Methodenerweiterungsfilter enthält nur zusätzliche Verbesserungen für die DSGVO, die auf der GRC-Methode basieren. Detaillierte Informationen zur GRC-Methode finden Sie in den Konventionshandbüchern im Lieferumfang von ARIS Risk & Compliance Manager. Weitere Informationen zur Installation von ARIS-Acceleratoren für die DSGVO finden Sie im **Installationshandbuch zu ARIS-Acceleratoren für die DSGVO**.

4 ARIS-Konventionen

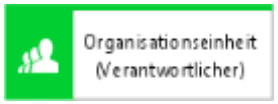
4.1 Verarbeitungsaktivitäten und -beziehungen erstellen

Im Mittelpunkt der ARIS-Datenschutzfunktionen steht das Erkennen von Prozessfunktionen (Verarbeitungstätigkeiten (Seite 13)) nach der Europäischen Datenschutz-Grundverordnung (DSGVO (Seite 13)). Geben Sie mit dem Attribut **DSGVO-Verarbeitungsaktivität** in ARIS an, ob es sich bei einer Prozessfunktion um eine Verarbeitungsaktivität handelt (**true**) oder nicht (**false**).

Verarbeitungsaktivitäten und zugehörige Informationen werden in einem Modell **Diagramm zur Beschreibung von Verarbeitungsaktivität** (API-Name: b0205e20-4aa5-11e7-43b7-08002721906d) in ARIS Architect modelliert, um die Stammdatenpflege zu erleichtern. Dieser Modelltyp ist vom Modelltyp **Funktionszuordnungsdiagramm** abgeleitet.

4.1.1 Objekte und Beziehungen

Sie können folgende Objekte im Modell **Diagramm zur Beschreibung von Verarbeitungstätigkeit** im Rahmen des Datenschutz-Managements verwenden:

Objekttypname	API-Name	Symboltypname	Symbole	ARCM-Name
Funktion	OT_FUNC	Verarbeitungstätigkeit		Prozess (Hierarchieelement)
Organisationseinheit	OT_ORG_UNIT	Organisationseinheit (Auftragsverarbeiter)		Auftragsverarbeiter (Hierarchieelement)
Organisationseinheit	OT_ORG_UNIT	Organisationseinheit (Verantwortlicher)		Organisationsverantwortlicher (Hierarchieelement)
Cluster/Datenmodell	OT_CLST	Cluster		Daten (Hierarchieelement)
Risiko	OT_RISK	Risiko		Risiko
Anwendungssystemtyp	OT_APPL_SYS_TYPE	Anwendungssystemtyp		Anwendungssystemtyp (Hierarchieelement)

Sie können die folgenden Kanten verwenden:

Objekt	Kante/API-Name	Objekt
Organisationseinheit (Verantwortlicher)	ist fachlich verantwortlich für (CT_IS_TECH_RESP_1)	Verarbeitungstätigkeit
Organisationseinheit (Auftragsverarbeiter)	führt aus (CT_EXEC_1)	Verarbeitungstätigkeit
Risiko	tritt auf an (CT_OCCUR)	Verarbeitungstätigkeit
Anwendungssystemtyp	unterstützt (CT_CAN_SUPP_1)	Verarbeitungstätigkeit
Verarbeitungstätigkeit	liest (CT_READ_1), hat als Ausgabe (CT_HAS_OUT)	Cluster

4.1.2 Attribute

4.1.2.1 Verarbeitungstätigkeiten-Attribute

Für die **Verarbeitungstätigkeit** gelten folgende Zuordnungen:

ARIS-Attribut	API-Name	ARCM-Attribut	Hinweistext
Name	AT_NAME	name	Pflichtfeld, auf 250 Zeichen beschränkt.
Beschreibung	AT_DESC	description	Gibt den Zweck der Verarbeitungstätigkeit an.

ARIS-Attribut	API-Name	ARCM-Attribut	Hinweistext
DSGVO-Verarbeitungstätigkeit	2b70adc0-4504-11e7-43b7-08002721906d	gdpr_processingActivity	Benutzerdefiniert - Legt fest, ob die Funktion eine Verarbeitungstätigkeit ist oder nicht.
Punktzahl für Datenschutz	695b1ad0-1df9-11e7-43b7-08002721906d	gdpr_process_privacyScore	Benutzerdefiniert - Gibt eine geschätzte Punktzahl auf einer vordefinierten Skala zur Qualifizierung des Datenschutzniveaus des Hierarchieelements an. Beispiel: Der aus dem Fragebogen Qualifikation Verarbeitungstätigkeit (Processing Activity Qualification) abgeleitete Score.
Sensibilität der Daten	332790f0-1dfa-11e7-43b7-08002721906d	gdpr_process_dataSensitivity	Benutzerdefiniert - Gibt an, ob die Daten eine besondere Handhabung erfordern. Optionen (Standardwerte): ▪ **Öffentliche Daten** ▪ **Sensibel** ▪ **Sehr sensibel** ▪ **Höchst sensibel** ▪ **Äußerst sensibel**
Sign-off-relevant	AT_AAM_SIGN_OFF_RELEVANT	signoff	Markiert die Verarbeitungstätigkeit als Sign-off-relevant. Falls nicht angegeben, ist der Standardwert in ARIS Risk & Compliance Manager

ARIS-Attribut	API-Name	ARCM-Attribut	Hinweistext
			false.

4.1.2.2 Cluster-Attribute

Für den **Cluster** gelten folgende Zuordnungen:

ARIS-Attribut	API-Name	ARCM-Attribut	Hinweistext
Name	AT_NAME	name	Pflichtfeld, auf 250 Zeichen beschränkt.
Beschreibung	AT_DESC	description	
Einschränkungsstufe	15eaceb1-096b-11e7-2959-d4bed9888991	gdpr_restrictionLevel	Benutzerdefiniert - Gibt den Grad der legalen Nutzbarkeit der Daten an. Optionen (Standardwerte): ▪ **Uneingeschränkte Daten** ▪ **Personenbezogene Daten** ▪ **Sensible personenbezogene Daten** ▪ **Vertrauliche Daten**
Punktzahl für Datenschutz	695b1ad0-1df9-11e7-43b7-08002721906d	gdpr_privacyScore	Benutzerdefiniert - Gibt eine geschätzte Punktzahl auf einer vordefinierten Skala zur Qualifizierung des Datenschutzniveaus des

ARIS-Attribut	API-Name	ARCM-Attribut	Hinweistext
			Hierarchieelements an. Beispiel: Der aus einem Fragebogen zur Einstufung eines Datenelements abgeleitete Score.

4.1.2.3 Organisationseinheitsattribute

Für das Objekt **Organisationseinheit** gelten folgende Attributzuordnungen:

ARIS-Attribut	API-Name	ARCM-Attribut	Hinweistext
Name	AT_NAME	name	Pflichtfeld, auf 250 Zeichen beschränkt.
Beschreibung	AT_DESC	description	
Datenschutzbeauftragter	1c2537a1-4072-11e7-43b7-08002721906d	gdpr_protOfficer	Benutzerdefiniert - Zeigt den Namen und die Adresse des Datenschutzbeauftragten an. Muss im Verzeichnis der Verarbeitungstätigkeiten enthalten sein. Muss im Report aufgeführt werden.
Vertreter des Verantwortlichen/Auftragsverarbeiters	8f055dc1-407e-11e7-43b7-08002721906d	gdpr_protRepresentative	Benutzerdefiniert - Zeigt den Namen und die Adresse des Vertreters des

ARIS-Attribut	API-Name	ARCM-Attribut	Hinweistext
			Verantwortlichen/Auftragsverarbeiters an. Muss im Verzeichnis der Verarbeitungstätigkeiten enthalten sein. Muss im Report aufgeführt werden.
Sign-off-relevant	AT_AAM_SIGN_OFF_RELEVANT	signoff	Markiert die Organisationseinheit als Sign-off-relevant. Falls nicht angegeben, ist der Standardwert in ARIS Risk & Compliance Manager false.

4.1.2.4 Anwendungssystemtypattribute

Für den **Anwendungssystemtyp** gelten folgende Attributzuordnungen:

ARIS-Attribut	API-Name	ARCM-Attribut	Hinweistext
Name	AT_NAME	name	Pflichtfeld, auf 250 Zeichen beschränkt.
Beschreibung	AT_DESC	description	
Sensibilität der Daten	332790f0-1dfa-11e7-43b7-08002721906d	gdpr_dataSensitivity	Benutzerdefiniert - Gibt an, ob die Daten eine besondere Handhabung erfordern. Optionen (Standardwerte): ▪ **Öffentliche Daten**

ARIS-Attribut	API-Name	ARCM-Attribut	Hinweistext
			▪ **Sensibel** ▪ **Sehr sensibel** ▪ **Höchst sensibel** ▪ **Äußerst sensibel**
Punktzahl für DSGVO-Qualifizierung	badc1630-2014-11e7-43b7-08002721906d	gdpr_qualificationScore	Benutzerdefiniert - Gibt eine geschätzte Punktzahl auf einer vordefinierten Skala zur Qualifizierung des Hierarchieelements an. Beispiel: Ein aus einem Fragebogen zur Einstufung des Anwendungssystems abgeleiteter Score.
Punktzahl für DSGVO-Risikorelevanz	da6e5cb1-2014-11e7-43b7-08002721906d	gdpr_riskRelevanceScore	Benutzerdefiniert - Gibt eine geschätzte Punktzahl auf einer vordefinierten Skala zur Qualifizierung der Risikorelevanz des Hierarchieelements an. Beispiel: Der aus der DSGVO-Risikobewertung abgeleitete Score.
Punktzahl für Datenschutz	695b1ad0-1df9-11e7-43b7-08002721906d	gdpr_privacyScore	Benutzerdefiniert - Gibt eine geschätzte Punktzahl auf einer vordefinierten Skala zur Qualifizierung des Datenschutzniveaus des Hierarchieelements an. Beispiel: Der aus einem Fragebogen zur Einstufung des Anwendungssystems abgeleitete Score.

4.2 Verarbeitungsaktivität/Prozesshierarchie erstellen

Zum Modellieren eines Business-Clusters von Verarbeitungstätigkeiten, z. B. Abteilungen oder Länder, in denen eine Organisation vertreten ist, verwenden Sie das Modell **Verzeichnis der Verarbeitungstätigkeiten** (API-Name: c45962f1-4b87-11e7-43b7-08002721906d), das vom Modell **Wertschöpfungskettendiagramm** abgeleitet ist. Eine Hierarchie zwischen den Verarbeitungsaktivitäten kann durch die Kante **ist prozessorientiert übergeordnet** / **ist prozessorientiert untergeordnet** (CT_IS_PRCS_ORNT_SUPER) dargestellt werden.

In ARIS Risk & Compliance Manager ist nur eine Baumstruktur für Hierarchien zulässig. Daher kann jede Verarbeitungsaktivität nur genau eine übergeordnete Verarbeitungsaktivität/Funktion besitzen.

4.3 Cluster/Daten-Hierarchie erstellen

Zum Erstellen einer Hierarchie zwischen Clustern verwenden Sie das **IE-Datenmodell** oder das **eERM**-Modell. Die Hierarchie zwischen Clustern wird von der Kante **besteht aus**/**ist Teil von** (CT_CONS_OF_2) als direkte Kante zwischen zwei Clustern im IE-Datenmodell repräsentiert oder als eine implizite Kante, die durch Zuordnung eines eERM-Modells zum Cluster entsteht.

In ARIS Risk & Compliance Manager ist nur eine Baumstruktur für Hierarchien zulässig. Deshalb kann es zu jedem Cluster nur ein übergeordnetes Cluster geben.

5 Glossar

DSGVO

Die **D**aten**s**chutz-**G**rund**v**er**o**rdnung (DSGVO) schützt personenbezogene Daten innerhalb der Europäischen Union. Sie reguliert zudem die Ausfuhr personenbezogener Daten an Standorte außerhalb der EU. Die DSGVO ist eine Verordnung des Europäischen Parlaments, des Rates der Europäischen Union und der Europäischen Kommission.

VERARBEITUNGSTÄTIGKEIT

Verarbeitungstätigkeiten sind sämtliche Operationen, die an personenbezogenen Daten von Einzelpersonen ausgeführt werden, z. B. das Sammeln, das Aufzeichnen oder die Weitergabe durch Übermittlung. Deshalb unterliegen Sie den Regeln der Datenschutz-Grundverordnung (DSGVO (Seite 13)).

Verarbeitungstätigkeiten und zugehörige Informationen werden in ARIS Architect in den Modellen **Processing activity description diagram** und **Record of processing activities** modelliert. Detaillierte Informationen finden Sie im Handbuch **ARIS Risk & Compliance Manager - Datenschutz-Management**.

SINGLE SIGN-ON (SSO)

Durch **SSO** oder **Single Sign-on** (Einmalanmeldung) braucht sich ein Benutzer nur einmal per Benutzername und Kennwort zu authentifizieren, um ohne erneute Anmeldung auf alle Dienste, Programme und Rechner zuzugreifen.

Wenn Dienste, Programme und Rechner beim Zugriff durch den Benutzer eine erneute Authentifizierung verlangen, wird diese durch den zugrunde liegenden SSO-Mechanismus vorgenommen.

6 Rechtliche Hinweise

6.1 Dokumentationsumfang

Die zur Verfügung gestellten Informationen beschreiben die Einstellungen und Funktionalitäten, die zum Zeitpunkt der Veröffentlichung gültig waren. Da Software und Dokumentation verschiedenen Fertigungszyklen unterliegen, kann die Beschreibung von Einstellungen und Funktionalitäten von den tatsächlichen Gegebenheiten abweichen. Informationen über solche Abweichungen finden Sie in den mitgelieferten Release Notes. Bitte lesen und berücksichtigen Sie diese Datei bei Installation, Einrichtung und Verwendung des Produkts.

Wenn Sie das System technisch und/oder fachlich ohne Service-Leistung der Software AG installieren möchten, benötigen Sie umfangreiche Kenntnisse hinsichtlich des zu installierenden Systems, der Zielthematik sowie der Zielsysteme und ihren Abhängigkeiten untereinander. Aufgrund der Vielzahl von Plattformen und sich gegenseitig beeinflussender Hardware- und Softwarekonfigurationen können nur spezifische Installationen beschrieben werden. Es ist nicht möglich, sämtliche Einstellungen und Abhängigkeiten zu dokumentieren.

Beachten Sie bitte gerade bei der Kombination verschiedener Technologien die Hinweise der jeweiligen Hersteller, insbesondere auch aktuelle Verlautbarungen auf deren Internet-Seiten bezüglich Freigaben. Für die Installation und einwandfreie Funktion freigegebener Fremdsysteme können wir keine Gewähr übernehmen und leisten daher keinen Support. Richten Sie sich grundsätzlich nach den Angaben der Installationsanleitungen und Handbücher der jeweiligen Hersteller. Bei Problemen wenden Sie sich bitte an die jeweilige Herstellerfirma.

Falls Sie bei der Installation von Fremdsystemen Hilfe benötigen, wenden Sie sich an Ihre lokale Software AG-Vertriebsorganisation. Beachten Sie bitte, dass solche Hersteller- oder kundenspezifischen Anpassungen nicht dem Standard-Softwarepflege- und Wartungsvertrag der Software AG unterliegen und nur nach gesonderter Anfrage und Abstimmung erfolgen.

Bezieht sich eine Beschreibung auf ein spezifisches ARIS-Produkt, wird dieses genannt. Andernfalls werden die Bezeichnungen für die ARIS-Produkte folgendermaßen verwendet:

Name	Umfasst
ARIS-Produkte	Bezeichnet sämtliche Produkte, für die die Lizenzbedingungen der Software AG-Standard-Software gelten.
ARIS-Clients	Bezeichnet alle Programme, die über ARIS Server auf gemeinsam verwendete Datenbanken zugreifen.
ARIS-Download-Clients	Bezeichnet ARIS-Clients, die aus dem Browser gestartet werden können.

6.2 Datenschutz

Die Produkte der Software AG stellen Funktionalität zur Verfügung, die für die Verarbeitung persönlicher Daten entsprechend der EU-Datenschutz-Grundverordnung (DSGVO) genutzt werden kann.

Die Beschreibungen zur Nutzung dieser Funktionalität finden Sie in der Administrationsdokumentation des jeweiligen Produkts.

6.3 Disclaimer

ARIS-Produkte sind für die Verwendung durch Personen gedacht und entwickelt. Automatische Prozesse wie das Generieren von Inhalt und der Import von Objekten/Artefakten per Schnittstellen können zu einer immensen Datenmenge führen, deren Verarbeitung wiederum Verarbeitungskapazitäten und physische Grenzen überschreiten können. Verarbeitungsgrenzen werden zum Beispiel dann überschritten, wenn Modelle und Diagramme größer als die maximale Modellierungsfläche sind oder wenn eine extrem hohe Anzahl von Verarbeitungsprozessen gleichzeitig gestartet wird. Physikalische Grenzen können dann überschritten werden, wenn der verfügbare Speicherplatz für die Ausführung der Operationen oder die Speicherung der Daten nicht ausreicht.

Der ordnungsgemäße Betrieb von ARIS setzt voraus, dass eine zuverlässige und schnelle Netzwerkverbindung vorhanden ist. Ein Netzwerk mit unzureichender Antwortzeit reduziert die Systemperformanz und kann zu Timeouts führen.

ARIS Dokumentablage wurde mit 40.000 Artefakten getestet. Dies enthält Dokumente, Dokumentversionen oder Ordner. Es empfiehlt sich, die Anzahl und Gesamtgröße gespeicherter Artefakte zu überwachen und gegebenenfalls einige Artefakte zu archivieren.

Wenn ARIS-Produkte in einer virtuellen Umgebung genutzt werden, müssen ausreichende Ressourcen verfügbar sein, um das Risiko einer Überbuchung zu vermeiden.

Das System wurde in Szenarien getestet, die 100.000 Gruppen (Verzeichnisse), 100.000 Benutzer und 1.000.000 Modellierungsartefakte beinhalten. Es unterstützt eine Modellierungsfläche von 25 Quadratmetern.

Wenn Projekte oder Repositorys diese Grenzen überschreiten, steht eine leistungsstarke Funktionalität zur Verfügung, um sie in kleinere, bearbeitbare Teile zu gliedern.

In der Prozessadministration, der ARIS Administration, ARIS Dokumentablage, ARIS Process Board sowie beim Generieren von ausführbaren Prozessen können Einschränkungen auftreten. Process Governance ist für 1000 parallele Prozessinstanzen getestet und freigegeben. Diese Zahl kann dennoch unterschiedlich sein, je nach Komplexität des Prozesses, z. B. wenn eigene Reporte integriert sind.

ARIS Dokumentablage wurde mit 40.000 Artefakten getestet. Dies enthält Dokumente, Dokumentversionen oder Ordner. Es empfiehlt sich, die Anzahl und Gesamtgröße gespeicherter Artefakte zu überwachen und gegebenenfalls einige Artefakte zu archivieren.