



Koordinierungsstelle
für IT-Standards

Datenschutzcockpit-Standard

XDatenschutzcockpit

Teil 1: Technologieunabhängige Spezifikation

Version 1.0.1

Januar 2024

Koordinierungsstelle für IT-Standards (KoSIT)

Langenstr. 10-12

28195 Bremen

E-Mail: kosit@finanzen.bremen.de

© Koordinierungsstelle für IT-Standards 2024

Inhaltsverzeichnis

1	Übersicht	4
2	Rahmenbedingungen im Projektes XDatenschutzcockpit	6
2.1.	Registermodernisierung	6
2.2.	Projekt Datenschutzcockpit	7
2.2.1.	Einordnung des Datenschutzcockpits und des Standards.....	7
2.2.2.	Einfache Anschlussfähigkeit	8
2.2.3.	Grundlegende Abläufe	8
2.2.4.	Umfang der Auskünfte an betroffene Personen	9
2.3.	Anforderungen an die Einsatzumgebung.....	9
3	Methodik	11
4	Begriffsbestimmungen	13
5	Abläufe zum Abruf von Informationen zu auskunftspflichtigen Datenübermittlungen.....	14
6	Nachrichten und Datentypen.....	15
6.1.	Statusabfrage.....	15
6.1.1.	Ziel/Aufgabe	15
6.1.2.	Signatur: abfrageStatus	15
6.1.3.	Datenstrukturen	16
6.1.4.	Fehler/Ausnahmen	16
6.1.5.	Rahmenbedingungen	16
6.1.6.	Vorbedingungen	16
6.2.	Abruf der Protokolldaten.....	17
6.2.1.	Ziel/Aufgabe	17
6.2.2.	Signatur: abfrageListeProtokolldaten	17
6.2.3.	Datenstrukturen	18
6.2.4.	Fehler/Ausnahmen	22
6.2.5.	Rahmenbedingungen	22
6.2.6.	Vorbedingungen	22
6.3.	Abruf der Inhaltsdaten	22
6.3.1.	Ziel/Aufgabe	22
6.3.2.	Signatur: abfrageInhaltsdaten	22
6.3.3.	Datenstrukturen	23
6.3.4.	Fehler/Ausnahmen	24
6.3.5.	Rahmenbedingungen	24
6.3.6.	Vorbedingungen	25
7	Änderungshistorie.....	26

1 Übersicht

Bürger:innen sollen unterstützt werden, wenn sie digital Leistungen der Verwaltung beantragen, in dem die Verwaltung die ihr bereits vorliegenden Informationen zur Verfügung stellt. Das Gesetz zur Registermodernisierung (RegMoG) sieht die Einführung einer Identifikationsnummer und eines Dienstes „Datenschutzcockpit“ vor. Mit der Identifikationsnummer sollen Daten in den Verwaltungsregistern den Bürger:innen eindeutig zugeordnet werden, so dass die Verwaltung die richtigen Daten den richtigen Personen digital zur Verfügung stellen kann. Das Datenschutzcockpit soll interessierten Bürger:innen eine einfache, transparente und zeitnahe Übersicht über Datenübermittlungen zwischen öffentlichen Stellen unter Nutzung der Identifikationsnummer ermöglichen. Der Standard XDatenschutzcockpit, der in diesem Dokument festgelegt wird, definiert Nachrichten und Datenstrukturen für den fachlichen Austausch zwischen dem Datenschutzcockpit und den betroffenen Registern.

Das vorliegende Dokument ist der erste, technologieunabhängige Teil des Standards XDatenschutzcockpit (Teil 1). In diesem Teil wird die Semantik im fachlichen Datenaustausch mit dem Datenschutzcockpit festgelegt. Zum besseren Verständnis des Standards beschreibt er zudem den Kontext und das Vorgehen zur Entwicklung des Standards. Somit adressiert der Teil 1 des Standards XDatenschutzcockpit alle Teilnehmenden am Projekt Datenschutzcockpit und im Kontext der Entwicklung des Datenschutzcockpits gleichermaßen. Für die Umsetzung des Standards ist die Abbildung der technologieunabhängig definierten Semantik in eine konkrete technische Syntax erforderlich, dies erfolgt im zweiten Teil des Standards. Entwickler:innen werden die notwendigen Informationen für eine konkrete Umsetzung des Standards daher in den Modulen des zweiten Teils finden und können zum vertiefenden Verständnis auf dieses Dokument zurückgreifen.

Die nachfolgenden Kapitel dieses ersten Teils des Standards XDatenschutzcockpit enthalten die Rahmenbedingungen des Projektes, die gewählte Methodik, Begriffsbestimmungen, Abläufe im fachlichen Datenaustausch zwischen Register und Datenschutzcockpit sowie eine technologie neutrale Spezifikation der Nachrichten und Datentypen. Die Module des zweiten Teils beschreiben den Aufbau und die Verwendung der Module (Teil 2-1), Nachrichten und Datentypen in XML (Teil 2-2), die Datenübermittlung über OSCI (Teil 2-3) sowie von XML über HTTP (Teil 2-4).

Der Entwurf des Standards XDatenschutzcockpit ist ein Teilprojekt zur Entwicklung des Datenschutzcockpits. Das Projekt Datenschutzcockpit ist ein Projekt der Registermodernisierung. Der Standard und das Datenschutzcockpit werden begleitend zu anderen Vorhaben der Registermodernisierung entwickelt, insbesondere zur Einführung der Identifikationsnummer in den Registern. Die Rahmenbedingungen und Projektziele müssen also erst identifiziert und anschließend weiterentwickelt werden. Um die parallelen Entwicklungen der Registermodernisierung zu unterstützen, muss die Versionierung sowohl projektintern pilotierungsfähige Entwurfskandidaten (Release Candidate) als auch projektextern den Pilotcharakter des Arbeitsstandes kennzeichnen.

Die Festlegung der Versionsnummer erfolgt durch das Projekt Datenschutzcockpit. Für die Versionierung werden drei Stellen verwendet, die wie folgt verwendet werden sollen:

- Die Hauptversionsnummer steht an erster Stelle und kennzeichnet über alle Dokumente des Standards die laufende, vom Gesamtprojekt Datenschutzcockpit gesteuerte Entwicklung des Standards. Eine Änderung der Hauptversionsnummer kann dazu verwendet werden, wesentliche, weitreichende Änderungen am Standard anzuzeigen, z.B. an neue oder grundlegend überarbeitete, verpflichtende Abläufe, Nachrichten oder Datenstrukturen.
- Die zweite Stelle kennzeichnet über alle Dokumente des Standards Weiterentwicklungen bestehender Abläufe und Datenstrukturen, z.B. die Aufnahme neuer oder Er-

ganzung bestehender Ablaufe, Nachrichten oder Datenstrukturen. Sie wird auf Anforderung des Gesamtprojektes erhohet und mit bei einer anderung der vorangehenden Stelle auf „0“ zuruckgesetzt.

- Die dritte Stelle beginnt bei „0“ und kennzeichnet die fortlaufend nummerierte Arbeitsfassung des jeweiligen Dokumentes, wie sie zum Beispiel durch redaktionelle anderungen oder Klarstellungen sowie optionalen Erweiterungen von Ablaufen, Nachrichten und Datenstrukturen entstehen konnen. Die dritte Stelle wird durch das Teilprojekt XDatenschutzcockpit in Abstimmung mit dem Gesamtprojekt erhohet und mit bei einer anderung der vorangehenden Stellen auf „0“ zuruckgesetzt.
- Der Zusatz „-pilot“ kennzeichnete vor der Version 1.0.0 Fassungen des Standards, die ausdrucklich einen Pilotcharakter hatten. Sie wurde in Abstimmung mit dem Gesamtprojekt Datenschutzcockpit entfernt.

Das Datenschutzcockpit wird vom Land Bremen im Auftrag des Bundesministeriums des Innern und fur Heimat (BMI) entwickelt, der Standard XDatenschutzcockpit wird von der Koordinierungsstelle fur IT-Standards im Auftrag des Landes Bremen erstellt. Der Standard wird aktuell wesentlich in Zusammenarbeit mit Pilotprojekten fortentwickelt, um Erfahrungen aus der Erprobung und Anforderungen aus dem Anschluss neuer Register abzubilden. Die Gesamtprojektlaufzeit endet mit Abschluss der Registermodernisierung Ende 2025, dies ist auch der Endzeitpunkt fur das Teilprojekt XDatenschutzcockpit. Die Weiterentwicklung und Pflege des Standards erfolgt anschlieend im Kontext des Betriebs des Datenschutzcockpits.

Der Standard XDatenschutzcockpit definiert den fachlichen Austausch zwischen dem Datenschutzcockpit und den betroffenen Registern. Der Standard XDatenschutzcockpit ist kein Ersatz fur Kommunikationsprotokolle zur technischen Datenubermittlung, wie zum Beispiel HTTP. Er legt dementsprechend keine Manahmen fur den sicheren Betrieb von Umsetzungen fest.

Nachfolgend wird zunachst der Rahmen beschrieben, in dem der Standard entwickelt wird: Der Anwendungsbereich des Standards, die Methodik zu seiner Entwicklung und grundlegende Begriffe. Darauf aufbauend wird der Ablauf zum Abruf von Informationen zu Datenubermittlungen aus den Registern festgelegt. Fur diese Abrufe werden abschlieend die Nachrichten und Datentypen definiert. Die Spezifikation erfolgt so weit wie moglich technologieunabhangig, definiert also was in welcher Abfolge und zu welchem Zweck ausgetauscht wird, nicht jedoch wie die konkrete technische Umsetzung aussehen kann. Technologiespezifische Auspragungen des Standards, die den Vorgaben in diesem Standard entsprechen, werden begleitend zum Standard entwickelt und in separaten Dokumenten veroffentlicht.

2 Rahmenbedingungen im Projektes XDatenschutzcockpit

Der Standard XDatenschutzcockpit wird im Rahmen des Projektes Datenschutzcockpit, einem Projekt der Registermodernisierung, entwickelt und soll auch nach Abschluss des Projektes im Kontext des Datenschutzcockpits fortgeführt werden. In der Entwurfsphase, insbesondere den Workshops und Projektsprechstunden zum Austausch mit anderen Teilnehmenden an der Registermodernisierung, wurden die Rahmenbedingungen des Projektes XDatenschutzcockpit vermittelt und gegenüber anderen Aufgabenfeldern des Gesamtprojektes Datenschutzcockpit sowie der Registermodernisierung allgemein abgegrenzt. Nachfolgend werden die wesentlichen, aktuellen Rahmenbedingungen aufgeführt, die zu einem besseren Verständnis des Teilprojektes XDatenschutzcockpit und dem darin entwickelten Standard beigetragen haben. Sie werden dem Fortgang des Projektes und der Nutzung des Standards entsprechend angepasst.

2.1. Registermodernisierung

Das Gesetz zur Registermodernisierung (RegMoG) sieht vor, dass für Bürger:innen ein Dienst „Datenschutzcockpit“ entwickelt und angeboten wird. Das Datenschutzcockpit soll interessierten Bürger:innen eine einfache, transparente und zeitnahe Übersicht über Datenübermittlungen zwischen öffentlichen Stellen unter Nutzung der Identifikationsnummer ermöglichen. Es ist ein zusätzliches Transparenzangebot und ersetzt weder Informationspflichten noch bestehende Auskunftsansprüche, wie zum Beispiel die Informationspflicht Verantwortlicher nach Artikel 14 DSGVO oder das Auskunftsrecht der betroffenen Person nach Artikel 15 DSGVO. Hierfür ist die Entwicklung eines offenen Standards „XDatenschutzcockpit“ die Grundlage für einen einheitlichen Informationsaustausch und die Entwicklung interoperabler Lösungen.

Das Datenschutzcockpit ermöglicht Bürger:innen sich darüber zu informieren, ob, in welchem Umfang und welche Daten mit Bezug zur Identifikationsnummer angefragt oder übermittelt wurden. Bürger:innen initiieren hierfür über das Datenschutzcockpit eine Kommunikation mit einem Register, um Informationen über solche Datenübermittlungen abzurufen. Der Standard XDatenschutzcockpit definiert den fachlichen Austausch zwischen dem Datenschutzcockpit und den betroffenen Registern. Der Standard XDatenschutzcockpit ist folglich kein Ersatz für Kommunikationsprotokolle zur technischen Datenübermittlung, wie zum Beispiel HTTP. Er legt dementsprechend keine Maßnahmen für den sicheren Betrieb von Umsetzungen fest. Der Standard bildet keine Zusatzdienste oder steuert deren Nutzung, z.B. zur Nutzerauthentifizierung oder Steuerung der grafischen Darstellungen von Informationen. Entsprechende, zwingend erforderliche Datenelemente können im Standard abgebildet werden, die Ausgestaltung und Nutzung der darin enthaltenen Informationen ist jedoch nicht Gegenstand des Standards XDatenschutzcockpit. Die Dokumentation der Datenelemente folgt ihrer Dokumentation in den vorgehenden Standards.

Folgende Abgrenzung zu anderen Bereichen der Registermodernisierung, deren Vorhaben und Projekte sich parallel entwickeln, war in der Entwurfsphase hilfreich für das Verständnis der Rahmenbedingungen des Teilprojektes XDatenschutzcockpit. Nicht Gegenstand des Teilprojektes und des Standards XDatenschutzcockpit sind rechtlichen Grundlagen der Datenverarbeitung im Datenschutzcockpit, in den Registern oder anderen Verfahren, auch wenn diese der Umsetzung des Onlinezugangsgesetzes (OZG) oder der Single Digital Gateway Verordnung (SDGVO) dienen. Ebenso außerhalb des Teilprojektes sind entsprechende fachliche Prozesse, z.B. zur Aufbereitung der Datenlieferungen an das Datenschutzcockpit in Registern, oder die Funktionsweise des Datenschutzcockpits, z.B. in der Kombination standardisierter Abläufe oder der Präsentation von Informationen. Aus diesem Teilprojekt werden keine Anforderungen an andere Vorhaben oder Gremien gerichtet, um eine geordnete Kommunikation der parallelen Entwicklungen im Kontext der Registermodernisierung zu unterstützen. Sofern ein entsprechender Bedarf erkannt wird, werden die Erkenntnisse dem Pilotprojekt Daten-

schutzcockpit zur weiteren Verwendung zur Verfügung gestellt. Diese Auflistung ist naturgemäß nicht abschließend, sie enthält jene Abgrenzungen, die in der offenen Entwurfsphase wesentlich zum Verständnis des Teilprojektes und des Standards XDatenschutzcockpit beigetragen haben.

Ziel und Gegenstand des Teilprojektes XDatenschutzcockpit ist ein offener Standard, in dem grundlegende Abläufe im Datenaustausch zwischen Register und Datenschutzcockpit ermittelt und festlegt werden. Dies schließt die Definition der notwendigen Nachrichten und Datenstrukturen mit ein. Zusätzlich soll durch technologieunabhängige Definitionen und zugehörige technologiespezifische Abbildungen ein möglichst ausgewogenes Maß an technischer Offenheit und zugleich einheitlicher Vorgabe für interoperable Lösungen angestrebt werden.

2.2. Projekt Datenschutzcockpit

Die Entwicklung des Standards soll offen innerhalb des Projektes Datenschutzcockpit erfolgen, indem Teilnehmende am Projekt sowie der Registermodernisierung über den Entwicklungsstand informiert werden und Rückmeldungen einreichen können. Der Kreis der Teilnehmenden wird durch das Pilotprojekt Datenschutzcockpit bestimmt. Eingehende Rückmeldungen zum Standard XDatenschutzcockpit werden soweit wie möglich und unter Vorbehalt der Projektleitung Datenschutzcockpit berücksichtigt. Aus der offenen Entwicklung, insbesondere den durchgeführten Workshops, stammen die nachfolgenden wesentlichen Anforderungen an das Datenschutzcockpit mit Bezug zum Standard XDatenschutzcockpit.

2.2.1. Einordnung des Datenschutzcockpits und des Standards

Das Registermodernisierungsgesetz konkretisiert die Anforderungen an das Datenschutzcockpit und ist eine entsprechend zentrale Quelle für die Entwicklung des Standards XDatenschutzcockpit. Dieses Gesetz ist zudem die zentrale Quelle für Anforderungen an öffentliche Stellen in Bund und Ländern, welche Register nach dem Identifikationsnummerngesetz (IDNrG) führen. Das Registermodernisierungsgesetz wird diese Stellen unter anderem dazu verpflichten, Betroffenen die unter Verwendung der Identifikationsnummer erfolgte Übermittlung ihrer Daten digital über eine zentrale Stelle transparent zu machen. Diese zentrale Stelle ist das Datenschutzcockpit. Die so durch das Gesetz verpflichteten Stellen müssen hierfür Informationen an das Datenschutzcockpit liefern. Das Datenschutzcockpit gibt für diese Zulieferungen ausschließlich die technischen Aspekte im Standard XDatenschutzcockpit vor. Die Verständlichkeit oder fachliche Angemessenheit der vom Register gelieferten Informationen ist nicht Gegenstand des Standards oder des Datenschutzcockpits.

Das Datenschutzcockpit ist ein zusätzliches Transparenzangebot neben den rechtlich bereits bestehenden Informationspflichten und Auskunftsrechten, insbesondere aus der DSGVO. Über die Änderungen am OZG und mit der Schaffung des IDNrG werden im Rahmen der Registermodernisierung die Informationen zu Datenübermittlungen festgelegt, welche von natürlichen Personen im Datenschutzcockpit abgerufen werden können. Diese Informationen müssen geeignet sein, die Betroffenen in der Wahrnehmung ihrer Rechte zu unterstützen, also von Anwenderinnen und Anwendern des Datenschutzcockpits verstanden werden können. Mangels eines rechtlich festgelegten Datenkranzes über Informationen zu Datenübermittlungen und um die von Registermodernisierungsgesetz betroffenen Stellen zu entlasten, orientiert sich der Standard für den Informationsumfang daher an den bestehenden Anforderungen der DSGVO, konkret am Verzeichnis von Verarbeitungstätigkeiten nach Artikel 30 DSGVO und am Auskunftsrecht nach Artikel 15 DSGVO.

Im Datenschutzcockpit wird Transparenz nur für die Datenübermittlungen hergestellt, bei denen eine Identifikationsnummer nach Vorgabe des Identifikationsnummerngesetzes zum Einsatz kommt. Dieses Gesetz legt Zweck und Vergabe der Identifikationsnummer (IDNr) fest. Andere Datenübermittlungen werden nicht im Datenschutzcockpit angezeigt. Grundsätzlich nicht angezeigt werden Datenübermittlungen, die aufgrund anderer Rechtsvorschriften von

der Verpflichtung zur Transparenz ausgenommen sind (nachfolgend als „Übermittlung mit Sperrvermerk“ bezeichnet). Dies können zum Beispiel Datenübermittlungen an Sicherheitsbehörden sein.

Als Projekt zur Umsetzung des Registermodernisierungsgesetzes, sollten die Vorgaben des Standards XDatenschutzcockpit andere Maßnahmen und rechtliche Vorgaben nicht berühren. Insbesondere sind Maßgaben und Empfehlungen zur Kommunikation mit dem Datenschutzcockpit kein Ersatz für Betriebs-, Sicherheits- oder Datenschutzkonzepte der vom Registermodernisierungsgesetz betroffenen Stellen.

2.2.2. Einfache Anschlussfähigkeit

Für eine einfache Anschlussfähigkeit der Register und Anwendung des Standards, soll der Standard so wenig technische Vorgaben zur Datenlieferung machen, wie möglich. Die Festlegungen im Standard müssen daher so weit wie möglich technologieunabhängig erfolgen. Die Entwicklung verwendet dementsprechend:

- die erweiterte Backus-Naur-Form zur Definition der Datenstrukturen,
- einfache Sequenzdiagramme zur Beschreibung von Kommunikationsabläufen
- ausschließlich Zeichenketten, boolesche Werte und dateTime als Datentypen
- universale Format- und Zeichenvorgaben wie
 - UTF-8 als Zeichensatz
 - Base64 als Kodierung für die zu übermittelnden Inhalte

Die Entscheidung, für den registerübergreifenden Standard allgemeine Zeichenketten anstelle konkreter Datentypen zu verwenden, führt in der Implementierung unmittelbar zu der Anforderung, die Inhalte und Verwendung der Zeichenketten stets sorgfältig zu prüfen (z.B. Länge, Format, verwendete Zeichen)

2.2.3. Grundlegende Abläufe

Ergänzend zu den verwaltungsorientierten Namen von Datenkategorien, von denen anzunehmen ist, dass sie aus Sicht fachlicher Laien in der Regel schwer nachvollziehbar sind, werden im Datenschutzcockpit auch Informationen zur Gruppenstruktur und aller darin enthaltenen Informationskennzeichen angezeigt, um über Art und Umfang der Auskunft zu informieren. Die zugehörigen, konkreten Inhaltsdaten werden erst auf explizite Anforderung der Bürger:innen abgefragt und im Datenschutzcockpit angezeigt. Diesen beiden Abfragen ist eine Statusabfrage vorangestellt, mit der Bürger:innen zunächst ermitteln können, ob an einem Register eine Datenübermittlung unter Verwendung der Identifikationsnummer stattgefunden hat. Der Standard muss somit die folgenden drei Abrufe abbilden:

- Statusabfrage, um festzustellen, ob an einem Register eine Datenübermittlung stattgefunden hat.
- Protokolldatenabruf, um Art und Umfang von Datenübermittlungen des Registers zu erfahren.
- Inhaltsdatenabruf, um den konkreten Inhalt einer bestimmten Datenübermittlung eines Registers abzurufen. (Setzt Protokolldatenabruf voraus)

Für die Abbildung dieser drei Abrufe werden die Begriffe „Status“, „Protokolldaten“ und „Inhaltsdaten“ im Standard definiert. Mit einer Ausnahme sind die Abrufe voneinander unabhängig, vor dem Inhaltsdatenabruf muss ein Protokolldatenabruf vorausgehen. Jeder Abruf soll unmittelbar eine Antwort erhalten und muss als synchrone Kommunikation abgebildet und entsprechend umgesetzt werden.

2.2.4. Umfang der Auskünfte an betroffene Personen

Der Umfang der Protokolldaten folgt den Angaben zum Verzeichnis von Verarbeitungstätigkeiten (Artikel 30 Datenschutz-Grundverordnung (DSGVO)), um das Auskunftsrecht (Artikel 15 DSGVO) betroffener Personen zu unterstützen.

In der Anzeige von Inhaltsdaten unterstützt das Datenschutzcockpit eine festgelegte Liste von Datenformaten. Diese Liste der unterstützten Datenformate wird von den Verantwortlichen für das Datenschutzcockpit festgelegt und in einem menschen- und maschinenlesbaren Format mit einer eindeutigen Bezeichnung an einer festgelegten Stelle veröffentlicht. Damit eine Aktualisierung dieser Liste unabhängig vom Standard erfolgen kann, wird die Version der Liste nicht im Standard vorgegeben, es ist die jeweils aktuellste veröffentlichte Version zu nutzen.

Um eine grundlegend strukturierte Anzeige der übermittelten Informationen im Datenschutzcockpit zu ermöglichen, muss für alle übermittelten Informationen ein Kennzeichen übergeben werden, welches der fachlichen Semantik entspricht. Jede Information wird damit als Wertepaar (Kennzeichen, Inhalt) übermittelt, so dass zum Beispiel durch („Geburtsort“, „Berlin“) im Datenschutzcockpit „Geburtsort: Berlin“ angezeigt werden kann. Zusätzlich können Informationen genau einer Gruppe zugeordnet werden, deren Name und optionale Beschreibung ebenfalls der fachlichen Semantik entsprechen. Gruppen können in Gruppen enthalten sein, so dass eine baumartige Struktur angezeigt werden kann. In Ausführung des vorangegangenen Beispiels, kann die unbeschriebene Gruppe („Angaben zur Person“) die beschriebene Untergruppe („Angaben zur Geburt“, „Geburtstag und -ort“) enthalten, welche die Wertepaare („Geburtstag“, „12.08.1983“) und („Geburtsort“, „Berlin“) enthält. Ein mögliches Beispiel für eine einfach strukturierte Darstellung, welche durch diese Angaben ermöglicht wird, ist:

Angaben zur Person
Angaben zur Geburt (Geburtstag und –ort)
Geburtstag: 12.08.1983
Geburtsort: Berlin

Beispiel 1: Einfach strukturierte Darstellung der Angaben zur Geburt mit zwei Elementen und als Teil der Angaben zur Person

Die fachlichen Kennzeichnungen von Informationen, ihre Zuordnung zu einer Datenkategorie nach DSGVO, ihre Gruppierung sowie Bezeichnung und Beschreibung der Gruppen werden ausschließlich durch die jeweiligen Fachlichkeiten bestimmt. Eine fachübergreifend einheitliche Verwendung von Einordnungen, Kennzeichnungen und Gruppen wäre zwar wünschenswert, ist jedoch nicht Gegenstand des Datenschutzcockpits.

2.3. Anforderungen an die Einsatzumgebung

Die erfolgreiche Authentifizierung des Nutzers am Datenschutzcockpit und die erfolgreiche Authentifizierung des Datenschutzcockpits am Register wird vorausgesetzt, deren Mechanismus ist nicht Bestandteil des Standards XDatenschutzcockpit. Die Umsetzung der Schutzziele Authentizität, Integrität und Vertraulichkeit der Kommunikation zwischen Datenschutzcockpit und Register ist abhängig von den jeweils konkret in der Umsetzung eingesetzten technischen Mitteln zur Datenübermittlung. Der Standard legt grundsätzliche, fachliche Inhalte und Abläufe der Kommunikation fest. Die Implementierung und der Betrieb des Datenschutzcockpits müssen Maßnahmen zur Umsetzung der Ziele für ein angemessenes Schutzniveau ein- und umsetzen. Dabei ist zu berücksichtigen, dass zwischen dem Datenschutzcockpit und Registern personenbezogene Daten ausgetauscht werden, die zudem mit der Identifikationsnummer eine eindeutige, fachunabhängige Identifizierung betroffener Personen ermöglicht. Für die Bestimmung des Risikos bei der Verarbeitung der personenbezogenen Daten und die darauf

basierende Ableitung des Schutzniveaus, kann unter anderem auf etablierte Normen und Richtlinien zurückgegriffen werden, z.B. im Rahmen eines ISMS nach ISO 27001 oder BSI IT-Grundschutz sowie auf das Standard-Datenschutzmodell.

3 Methodik

Der Ablauf der Kommunikation zwischen Datenschutzcockpit und Register wird mittels eines Sequenzdiagrammes dargestellt. Das Sequenzdiagramm beschreibt den zeitlichen Ablauf von Interaktionen unterschiedlicher Akteure in Form von Request-Response Sequenzen. Die Darstellung der Dialogsequenzen ist in Kapitel 5 „Abläufe zum Abruf von Informationen zu auskunftspflichtigen Datenübermittlungen“ dokumentiert.

Ein Request-Response Paar kann durch eine Funktion im Sinne einer Programmiersprache dargestellt werden:

- Die Parameter des Request werden auf die Eingabeparameter der Funktion und
- die Parameter des Response werden auf die Ausgabeparameter der Funktion

abgebildet.

Alle Definitionen erfolgen innerhalb des jeweiligen Kommunikationsablaufs (Statusabfrage, Abruf der Protokolldaten, Abruf der Inhaltsdaten), um eine zentrale, in sich geschlossene Stelle in der Spezifikation für die Abbildung eines Ablaufs zu erzeugen und die Abläufe unabhängig voneinander entwickeln zu können. In der technologiespezifischen Umsetzung wird es in der Regel üblich sein, mehrfachverwendete, identische Datenstrukturen (z.B. Zeitraum, InhaltsdatenBeschreibung) einmal zu definieren und dann, unter Beachtung der dadurch erzeugten Abhängigkeiten, wiederzuverwenden. Die Bezeichnungen der Nachrichten, Datenstrukturen und Elemente erfolgt in deutscher Sprache, soweit nicht englischsprachige Bezeichnungen etabliert sind, die ein Zusammenwirken von Informationssystemen unmittelbar unterstützen (z.B. correlationID zur Kennzeichnung von Kommunikationen oder Label als Kennzeichnung von Informationsfeldern). Für die Schreibweise wird, soweit auch hier keine fachlichen Gründe entgegenstehen, zudem festgelegt:

- Variablennamen und Nachrichtennamen werden als lowerCamelCase notiert, z.B. „zeitraumAuskunft“, „abfrageStatus“, aber „IDNr“ (gleich der Abkürzung im fachlichen Kontext).
- Definierte Elemente und Strukturen werden in UpperCamelCase bezeichnet, z.B. „ProtokolldatenListe“ oder „UebermittlungID“.

Die Beschreibung der einzelnen Funktionen erfolgt in Kapitel 6 Nachrichten und Datentypen gemäß folgender Struktur/Gliederung:

Tabelle 1: Struktur und Gliederung für die Beschreibung von Funktionen

Abschnitt	Bedeutung
Ziel / Aufgabe	Wann hat die Funktion ihr Ziel erreicht, welche Aufgabe wurde erfüllt?
Signatur	Wie heißt die Funktion, welche Ein- und Ausgangswerte hat sie?
Datenstrukturen	Wie sind die Ein- und Ausgangswerte strukturiert?
Fehler / Ausnahmen	Welche Fehler- und welche Ausnahmefälle müssen abgebildet werden?
Rahmenbedingungen	Welche Bedingungen müssen unabhängig vom Aufruf einer Funktion erfüllt sein?
Vorbedingungen	Welche Bedingungen müssen vor dem Aufruf der Funktion erfüllt sein?

In diesem Dokument werden ausschließlich fachliche Fehler und Ausnahmen definiert. Technologiespezifische Fehlersituationen werden in den jeweiligen Ausprägungen des Standards dokumentiert.

Die Beschreibung der Datenstrukturen erfolgt in einem aus der „Erweiterten Backus-Naur-Form“ (EBNF) abgeleiteten Format. Anders als bei den Produktionsregeln der EBNF startet die Definition der Datenstruktur mit den sogenannten Nichtterminalsymbolen und endet mit der konkreten Angabe eines Datentyps, der dem Terminalsymbol der EBNF Definition entspricht. Im vorliegenden Standard werden den Rahmenbedingungen entsprechend ausschließlich die Datentypen „boolean“ und „string“ und „dateTime“ verwendet, als Kodierung für Zeichenketten ist UTF-8 und als Kodierung für Inhaltsdaten ist Base64 zu verwenden. Die sichere Handhabung der Zeichenketten muss in der Implementierung berücksichtigt werden.

In der Darstellung im Tabellenformat wird die linke-Seite durch die rechte Seite ersetzt und weiter konkretisiert, bis ausschließlich ein konkreter Datentyp angegeben wird. Nichtterminalsymbole werden vom „<“ und „>“ Symbol umschlossen. Terminalsymbole weisen dieses Zeichen nicht auf. Eine rechte Seite kann eine Folge von Terminal- oder Nichtterminalsymbolen enthalten, wobei die Bestandteile durch Kommata verbunden werden. Dabei wird folgende Syntax verwendet:

- Der vertikale Strich“|“ kennzeichnet eine (exklusive) Alternative.
- Eine Option wird durch eckige Klammern [...] dargestellt.
- Ausdrücke, die ausgelassen oder wiederholt werden dürfen, werden von geschweiften Klammern { ... } umgeben.

Definitionen werden genau einmal bei ihrem ersten Vorkommen innerhalb einer Datenstruktur aufgeführt und nicht wiederholt.

Der Standard geht davon aus, dass alle Datenstrukturelemente als Schlüssel-Wert-Paare repräsentiert werden. Dies wird nicht explizit dargestellt, weil die Art, wie dies umgesetzt wird, technologiespezifisch ist.

4 Begriffsbestimmungen

In den weiteren Abschnitten werden die Begriffsdefinitionen der folgenden Tabelle verwendet.

Tabelle 2: Begriffsdefinitionen

Begriff	Bedeutung
Status	Information, dass von einem Register* Nachrichten zu einer Identifikationsnummer (IDNr) übermittelt wurden
Protokolldaten	Informationen, welche Nachrichten zu einer Identifikationsnummer von einem Register* mit welchen Kategorien an Daten wann an wen übermittelt wurden
Inhaltsdaten	Informationen, welche Nachrichten zu einer Identifikationsnummer von einem Register* mit welchen Inhalten wann an wen übermittelt wurden
Bestandsdaten ¹	Aktuelle Daten des Registers zu einer Identifikationsnummer.

* oder andere protokollierungspflichtige Stelle

¹ Bestandsdaten werden in der Weiterentwicklung des Standards berücksichtigt, jedoch nicht in der aktuellen Fassung des Standards. Die Definition wurde zur Abgrenzung des Begriffs Inhaltsdaten aufgenommen.

5 Abläufe zum Abruf von Informationen zu auskunftspflichtigen Datenübermittlungen

Der Abruf der Protokoll- und Inhaltsdaten zu einer spezifischen Identifikationsnummer erfolgt in einem dreistufigen Prozess mit aufeinander aufbauenden Abfragen:

1. Statusabfrage
2. Abruf der Protokolldaten
3. Abruf der Inhaltsdaten

Die nachfolgende Abbildung 1 zeigt die Verwendung der drei Abrufe beispielhaft in einer Sequenz.

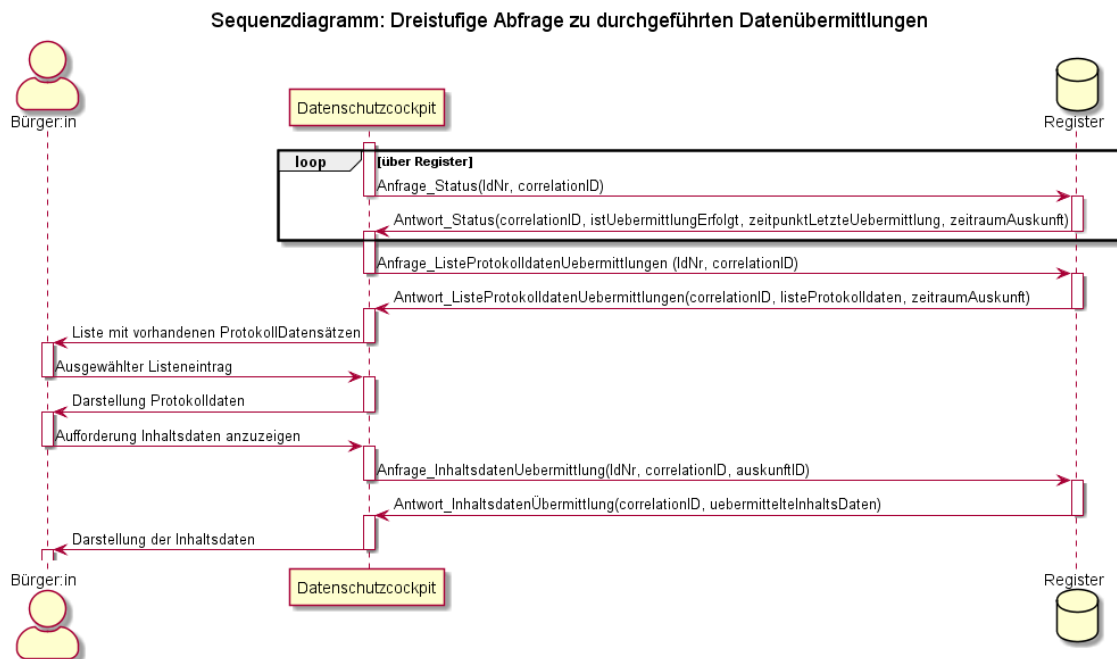


Abbildung 1: Ein Beispiel für den aufeinanderfolgenden Abruf von Status, Protokoll- und Inhaltsdaten

In der Umsetzung des Standards, zum Beispiel durch ein Register, müssen alle drei Abrufe unterstützt werden. Die genaue Verwendung dieser Abrufe wird in den Pilotprojekten weiter konkretisiert werden.

6 Nachrichten und Datentypen

6.1. Statusabfrage

6.1.1. Ziel/Aufgabe

Die Statusabfrage liefert die Information, ob am Register eine Datenübermittlung zu der gegebenen Identifikationsnummer stattgefunden hat. Im positiven Fall wird das Datum der letzten Datenübermittlung angegeben.

6.1.2. Signatur: `abfrageStatus`

abfrageStatus (EIN: `correlationID:string`, `DSCRequestToken:string`; AUS: `correlationID:string`, `istUebermittlungErfolgt:boolean`, `zeitpunktLetzteUebermittlung:dateTime`, `zeitraumAuskunft:Zeitraum`)

Der Aufbau der **IDNr** im `DSCRequestToken` entspricht der Definition der Basisdaten.IDNr.

Tabelle 3: Ein- und Ausgabeparameter `abfrageStatus`

Parameter EIN	Bedeutung
<code>correlationID²</code>	Eine vom Datenschutzcockpit zu erzeugende ID, mit der eine konkrete Abfrage eindeutig referenziert werden kann. Dient zur Nachverfolgbarkeit von Nachrichten und zur Fehlersuche.
<code>DSCRequestToken</code>	Ein vom Datenschutzcockpit für jede Registerabfrage neu erzeugtes Token, mit dem der Nutzer / die Nutzerin des Datenschutzcockpits anhand der Identifikationsnummer sowie das angefragte Register eindeutig identifiziert werden können. Das Token wird vom Datenschutzcockpit kryptographisch gesichert, damit diese Informationen vom Register zur Verifikation genutzt werden kann. Die innere Struktur und Funktionsweise des <code>DSCRequestToken</code> ist im Integrationskonzept des Datenschutzcockpits festgelegt. Die jeweils aktuellste Version kann beim Betreiber des Datenschutzcockpits oder beim Projektbüro Datenschutzcockpit angefragt werden.
Parameter AUS	Bedeutung
<code>correlationID</code>	Der unveränderte Eingabeparameter <code>correlationID</code> .
<code>istUebermittlungErfolgt</code>	Beantwortet die Frage, ob eine Datenübermittlung stattfand mit <i>true</i> oder <i>false</i> (falsch).

² Die Bezeichnung `correlationID` ist ein etablierter Bezeichner zur Identifikation einer Kommunikation in föderativen Umgebungen und wird, abweichend vom Namensmuster des Standards, unverändert in englischer Sprache übernommen, um die Anbindung an Lösungen zur Datenübermittlung zu erleichtern.

zeitpunktLetzteUebermittlung	Gibt das Datum der letzten Datenübermittlung an. Für den Fall, dass keine Übermittlung erfolgt ist – IstUebermittlungErfolgt hat den Wert <i>false</i> - , entfällt der Parameter in der Rückmeldung des Registers Die Angabe des Zeitpunkts erfolgt sekundengenau in der UTC-Zeitzone. Ist das nicht möglich, sind die nicht vorhandenen Angaben mit 0 aufzufüllen und darüber hinausgehende Millisekundenangaben zu entfernen.
zeitraumAuskunft	Gibt den konkreten Zeitraum (von, bis) an, der bei der Anfrage berücksichtigt wurde. Im IDNrG ist die Länge des Auskunftszeitraums definiert. Nur für diesen Zeitraum liegen Protokoll Daten vor.

6.1.3. Datenstrukturen

6.1.3.1. Zeitraum

Über den Datentyp Zeitraum wird eine Zeitspanne angegeben, die mit dem Startzeitpunkt (einschließlich) beginnt und mit dem Endzeitpunkt (einschließlich) endet.

Tabelle 4: Definition der Datenstruktur Zeitraum

Linke Seite	Rechte Seite
<Zeitraum>	<StartZeitpunkt>, <EndZeitpunkt>
<StartZeitpunkt>	dateTime
<EndZeitpunkt>	dateTime

StartZeitpunkt und **EndZeitpunkt** sind vom Datentyp dateTime. Die Angabe des Zeitpunkts erfolgt sekundengenau in der UTC-Zeitzone. Ist das nicht möglich, sind die nicht vorhandenen Angaben mit 0 aufzufüllen und darüber hinausgehende Millisekundenangaben zu entfernen.

Der Datentyp Zeitraum wird auch im Abruf der Protokoll Daten verwendet.

6.1.4. Fehler/Ausnahmen

Keine.

6.1.5. Rahmenbedingungen

- Antworten des Registers beschränken sich auf den im IDNrG vorgegebenen Zeitraum
- Register wird Übermittlungen mit Sperrvermerk nicht anzeigen

6.1.6. Vorbedingungen

Keine.

6.2. Abruf der Protokolldaten

6.2.1. Ziel/Aufgabe

Die Funktion liefert Informationen, welche Datenübermittlungen zu einer Identifikationsnummer bei dem angesprochenen Register stattgefunden haben. Das beinhaltet, welche Kategorien an Daten wann an wen übermittelt wurden. Die Informationen umfassen für jede Registerauskunft Daten zur eindeutigen Identifikation der Übermittlung aus fachlicher Sicht (Datenübermittlungen zwischen öffentlichen Stellen unter Nutzung einer Identifikationsnummer) sowie optionale Informationen in Orientierung an Artikel 30 und 15 DSGVO (vgl. Rahmenbedingungen aus Kapitel 2):

- eine eindeutige Referenz
- den Zeitpunkt
- eine eindeutige Bezeichnung der Auskunftsempfänger (z.B. AGS)
- Kontaktdaten des Auskunftsempfängers (die Stelle, an die man weiterführende Auskunftsersuchen richten kann)
- die Bezeichnungen der übermittelten Datenkategorien
 - Verarbeitungszwecke
 - Bezeichnung der Kategorien personenbezogener Daten, die verarbeitet werden, durch Angabe der Inhaltsstruktur anstelle einer fachlichen Datenkategorie
 - Empfänger oder Kategorien von Empfängern, denen gegenüber die Daten offengelegt worden sind oder noch offengelegt werden
 - Falls möglich: die geplante Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer
 - Das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung
 - Das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
 - Wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten
 - Das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

6.2.2. Signatur: `abfrageListeProtokolldaten`

abfrageListeProtokolldaten (EIN: correlationID:string, DSCRequestToken:string; AUS: correlationID:string, listeProtokolldaten:ProtokolldatenListe, zeitraumAuskunft:Zeitraum)

Der Aufbau der **IDNr** im `DSCRequestToken` entspricht der der Definition der Basisdaten.IDNr.

Tabelle 5: Ein- und Ausgabeparameter abfrageListeProtokolldaten

Parameter EIN	Bedeutung
correlationID	Eine vom Datenschutzcockpit zu erzeugende ID, mit der eine konkrete Abfrage eindeutig referenziert werden kann. Dient zur Nachverfolgbarkeit von Nachrichten und zur Fehlersuche.
DSCRequestToken	Ein vom Datenschutzcockpit für jede Registerabfrage neu erzeugtes Token, mit dem der Nutzer / die Nutzerin des Datenschutzcockpits anhand der Identifikationsnummer sowie das angefragte Register eindeutig identifiziert werden können. Das Token wird vom Datenschutzcockpit kryptographisch gesichert, damit diese Informationen vom Register zur Verifikation genutzt werden kann. Die innere Struktur und Funktionsweise des DSCRequestToken ist im Integrationskonzept des Datenschutzcockpits festgelegt. Die jeweils aktuellste Version kann beim Betreiber des Datenschutzcockpits oder beim Projektbüro Datenschutzcockpit angefragt werden.
Parameter AUS	Bedeutung
correlationID	Der unveränderte Eingabeparameter correlationID.
listeProtokolldaten	Liste von Elementen mit den Protokolldaten zu jeder für die Identifikationsnummer durchgeführte Datenübermittlung. Jedes Listenelement beschreibt genau eine Datenübermittlung und ermöglicht die eindeutige Referenzierung der durchgeführten Übermittlung. Die Liste hat die Länge 0, wenn beim Register keine Protokolldaten für die Identifikationsnummer vorliegen.
zeitraumAuskunft	Gibt den konkreten Zeitraum (von, bis) an, der bei der Anfrage berücksichtigt wurde. Im IDNrG ist die Länge des Auskunftszeitraums definiert. Nur für diesen Zeitraum liegen Protokolldaten vor.

6.2.3. Datenstrukturen

6.2.3.1. Zeitraum

Über den Datentyp Zeitraum wird eine Zeitspanne angegeben, die mit dem Startzeitpunkt (einschließlich) beginnt und mit dem Endzeitpunkt (einschließlich) endet.

Tabelle 6: Definition der Datenstruktur Zeitraum

Linke Seite	Rechte Seite
<Zeitraum>	<StartZeitpunkt>, <EndZeitpunkt>

<StartZeitpunkt>	dateTime
<EndZeitpunkt>	dateTime

StartZeitpunkt und **EndZeitpunkt** sind vom Datentyp `dateTime`. Die Angabe des Zeitpunkts erfolgt sekundengenau in der UTC-Zeitzone. Ist das nicht möglich, sind die nicht vorhandenen Angaben mit 0 aufzufüllen und darüberhinausgehende Millisekundenangaben zu entfernen.

Der Datentyp Zeitraum wird auch im Statusabruf verwendet.

6.2.3.2. ProtokolldatenListe

In der Datenstruktur `ProtokolldatenListe` sind alle Informationen enthalten, mit denen Bürger:innen nachvollziehbar dargestellt werden kann, welche Kategorien von Daten wann an wen übermittelt wurden. Die Beschreibung einer Datenübermittlung besteht aus den Protokollinformationen, welche eine Datenübermittlung eindeutig referenzierbar machen, Zeitpunkt und Empfänger der Daten dokumentieren sowie anhand von Datenkategorien den Umfang der Datenübermittlung nachvollziehbar beschreiben.

Die Datenkategorien zur Beschreibung der Datenübermittlung aus der Zielvorgabe für den Abruf von Protokollinformationen, die sich in Inhalt und Umfang an Artikel 30 DSGVO (Verzeichnis von Verarbeitungstätigkeiten) und insbesondere Artikel 15 DSGVO (Auskunftsrecht der betroffenen Person) orientiert, wurden in der Datenstruktur mit Ausnahme der Benennung von Datenkategorien direkt abgebildet (vgl. Abschnitt 6.2.1). Die nachfolgende Dokumentation fokussiert daher die Abbildung der Kategorien personenbezogener Daten, die über eine reine Benennung der Datenkategorien hinausgeht. In Vorbereitung auf eine mögliche Inhaltsdatenabfrage wird hier bereits in gleicher Weise der Aufbau der gruppenbezieharen, am Inhalt der Übermittlung orientierten Auskunft zu Art und Umfang der Datenübermittlung abgebildet.

In Analogie zu einem leeren Formularblatt, soll in der Auskunft zu den Protokolldaten einer Übermittlung dieselbe Struktur angezeigt werden, die mit der Auskunft zu den übermittelten Inhaltsdaten befüllt werden kann. Dafür werden, zusätzlich zur fachlichen Bezeichnung der Kategorie übermittelter personenbezogener Daten, der „Kategorie personenbezogener Daten“ auch die Beschreibungen aller übermittelten Inhaltsdaten optional zusammen mit einer einfachen Gruppenstruktur für eine grundlegend strukturierte Anzeige der Informationen zugeordnet. Die „Kategorie personenbezogener Daten“ besteht somit aus mindestens einer Inhaltsdatenbeschreibung, kann optional aber auch Gruppen enthalten. Eine Gruppe enthält mindestens eine Kennzeichnung („Label“) sowie optional eine Beschreibung. Der Rückbezug in der Definition der Gruppe zur „Kategorie personenbezogener Daten“ ermöglicht die geforderte Zuordnung in eine Baumstruktur.

Die Inhaltsdatenbeschreibung besteht aus einer Kennzeichnung („Label“) und einer Angabe zur Kategorie des Inhalts (zur Kategorie vgl. Artikel 15 DSGVO), optional können auch eine Beschreibung und eine Formatangabe zum übermittelten Inhalt angegeben werden. Die Formatangabe muss dabei entsprechend einer Vorgabe der Verantwortlichen für das Datenschutzcockpit gewählt werden. Damit eine Aktualisierung dieser Vorgabe unabhängig vom Standard erfolgen kann, wird diese nicht im Standard fest vorgegeben, es ist die jeweils aktuellste veröffentlichte Vorgabe zu nutzen.

Tabelle 6: Definition der Datenstruktur `ProtokolldatenListe`

Linke Seite	Rechte Seite
<ProtokolldatenListe>	{<DatenuebermittlungBeschreibung>}
<DatenuebermittlungBeschreibung>	<UebermittlungID> ,

	<UebermittlungZeitpunkt>, <UebermittlungEmpfaengerBezeichnung>, [<UebermittlungEmpfaengerKontaktdaten>], <UebermittlungSenderBezeichnung>, [<UebermittlungSenderKontaktdaten>] <UebermittlungAnlass>, <Datenkategorien>
<UebermittlungID>	string
<UebermittlungZeitpunkt>	dateTime
<UebermittlungEmpfaengerBezeichnung>	string
<UebermittlungEmpfaengerKontaktdaten>	string, {string}
<UebermittlungSenderBezeichnung>	string
<UebermittlungSenderKontaktdaten>	string, {string}
<UebermittlungAnlass>	string
<Datenkategorien>	<Verarbeitungszwecke>, <KategorienPersonenbezogenerDaten>, [<OffenlegungDaten>], [<DauerSpeicherung>], [<HinweisIntervention>], [<HinweisBeschwerderecht>], [<DatenHerkunft>], [<HinweisProfiling>]
<Verarbeitungszwecke>	string, {string}
<KategorienPersonenbezogenerDaten>	(<Gruppe> <InhaltsdatenBeschreibung>), {<Gruppe> <InhaltsdatenBeschreibung >}
<Gruppe>	<Label>,<Beschreibung>, <KategorienPersonenbezogenerDaten>
<InhaltsdatenBeschreibung>	<Label>,<Beschreibung>,<Typ>, [<Kategorie>]
<Label>	string
<Beschreibung>	string
<Typ>	string
<Kategorie>	string
<OffenlegungDaten>	string, {string}
<DauerSpeicherung>	string, {string}

<HinweisIntervention>	string, {string}
<HinweisBeschwerderecht>	string, {string}
<DatenHerkunft>	string, {string}
<HinweisProfiling>	string, {string}

ÜbermittlungID ist das einzigartige Identifikationskennzeichen der Übermittlung. Sie wird vom Register oder einer anderen protokollierungspflichtigen Stelle für jede Übermittlung, die im Datenschutzcockpit angezeigt werden muss, erstellt.

ÜbermittlungZeitpunkt bezeichnet das Datum und die Uhrzeit der durchgeführten Datenübermittlung. Die Angabe des Zeitpunkts erfolgt sekundengenau in der UTC-Zeitzone. Ist das nicht möglich, sind die nicht vorhandenen Angaben mit 0 aufzufüllen und darüberhinausgehende Millisekundenangaben zu entfernen.

ÜbermittlungEmpfängerBezeichnung enthält die bürgerfreundliche Bezeichnung des Empfängers der Datenübermittlung.

ÜbermittlungEmpfängerKontaktdaten enthält Kontaktinformationen des fachlichen Empfängers der Datenübermittlung.

ÜbermittlungSenderBezeichnung enthält die bürgerfreundliche Bezeichnung des Senders der Datenübermittlung.

ÜbermittlungSenderKontaktdaten enthält Kontaktinformationen des fachlichen Senders der Datenübermittlung.

ÜbermittlungAnlass beschreibt den Anlass der Datenübermittlung in bürgerfreundlicher Formulierung.

Gruppe: Mittels des Konstrukts <Gruppe> werden zusammengehörende Inhaltsdaten (z.B. eine Adresse) als zusammengehörend gekennzeichnet, so dass die Daten, wenn möglich, entsprechend gruppiert dargestellt werden können.

Label: Ein Text, mit dem aus fachlicher Sicht die Art des Inhalts gekennzeichnet wird (z.B. „Geburtsort“).

Beschreibung: Eine optionale Beschreibung, die als zusätzliche Information zur Erläuterung im Datenschutzcockpit verwendet werden kann.

Typ: Gültige Werte sind in der außerhalb dieses Standards gepflegten Werteliste

Kategorie: Kategorie des Inhalts im Sinne der DSGVO Artikel 15. Die Bezeichnung der Kategorie wird von fachlicher Seite festgelegt, nicht vom Datenschutzcockpit.

Verarbeitungszwecke: siehe DSGVO Artikel 15 (1) a)

KategorienPersonenbezogenerDaten: siehe DSGVO Artikel 15 (1) b)

OffenlegungDaten: siehe DSGVO Artikel 15 (1) c)

DauerSpeicherung: siehe DSGVO Artikel 15 (1) d)

HinweisIntervention: siehe DSGVO Artikel 15 (1) e)

HinweisBeschwerderecht: siehe DSGVO Artikel 15 (1) f)

DatenHerkunft: siehe DSGVO Artikel 15 (1) g)

HinweisProfiling: siehe DSGVO Artikel 15 (1) h)

6.2.4. Fehler/Ausnahmen

Keine.

6.2.5. Rahmenbedingungen

- Antworten des Registers beschränken sich auf den im IDNrG vorgegebenen Zeitraum
- Register wird Übermittlungen mit Sperrvermerk nicht anzeigen
- Die antwortende Stelle ist immer identisch mit dem Register, das Auskünfte erstellt hat
- Für das Element „Typ“ gibt es eine eindeutig referenzierbare Werteliste, in der die vom Datenschutzcockpit anzeigbaren Datentypen aufgelistet sind. Diese wird von den Verantwortlichen für das Datenschutzcockpit veröffentlicht und zur Verwendung vorgegeben. In den technologiespezifischen Standards kann zum Beispiel auf eine Veröffentlichung als Codeliste unter www.XRepository.de verwiesen werden. Die Register greifen auf diese Einträge zu und übergeben so abgestimmte Bezeichnungen an das Datenschutzcockpit.
- Die zurückgegebene <UebermittlungID> des Registers muss in nachfolgenden Verwendungen eine eindeutige Referenz auf die erteilte Auskunft abbilden. Sie ist so zu implementieren, dass sie eindeutig ist und über unterschiedliche Aufrufe gleichbleibt.

6.2.6. Vorbedingungen

Keine.

6.3. Abruf der Inhaltsdaten

6.3.1. Ziel/Aufgabe

Die Funktion liefert die Informationen für die angegebene Datenübermittlung zu einer Identifikationsnummer. Diese Informationen umfassen alle beauskunfteten Werte und ihre Bezeichnungen.

6.3.2. Signatur: abfrageInhaltsdaten

abfrageInhaltsdaten (EIN: uebermittlungID:string, correlationID:string, DSCRequestToken:string; AUS: correlationID:string, uebermittelteInhaltsdaten:Inhaltsdaten)

Der Aufbau der **IDNr** entspricht der Definition der Basisdaten.IDNr.

Tabelle 7: Ein- und Ausgabeparameter abfrageInhaltsdaten

Parameter EIN	Bedeutung
uebermittlungID	Kennung der Datenübermittlung, zu der die Inhaltsdaten geliefert werden sollen.
correlationID	Eine vom Datenschutzcockpit zu erzeugende ID, mit der eine konkrete Abfrage eindeutig referenziert werden kann. Dient zur Nachverfolgbarkeit von Nachrichten und zur Fehlersuche.
DSCRequestToken	Ein vom Datenschutzcockpit für jede Registerabfrage neu er-

	<p>zeugtes Token, mit dem der Nutzer / die Nutzerin des Datenschutzcockpits anhand der Identifikationsnummer sowie das angefragte Register eindeutig identifiziert werden können. Das Token wird vom Datenschutzcockpit kryptographisch gesichert, damit diese Informationen vom Register zur Verifikation genutzt werden kann.</p> <p>Die innere Struktur und Funktionsweise des DSCRequest-Token ist im Integrationskonzept des Datenschutzcockpits festgelegt. Die jeweils aktuellste Version kann beim Betreiber des Datenschutzcockpits oder beim Projektbüro Datenschutzcockpit angefragt werden.</p>
Parameter AUS	Bedeutung
correlationID	Der unveränderte Eingabeparameter correlationID.
uebermitteltInhaltsdaten	Datenstruktur mit den Inhaltsdaten der referenzierten Datenübermittlung.

6.3.3. Datenstrukturen

6.3.3.1. Inhaltsdaten

Das Datenschutzcockpit muss die Inhaltsdaten anzeigen können, die vom Register über die Abfrage der Inhaltsdaten zur Verfügung gestellt werden. Das Register muss diese Informationen in der hierfür definierten Datenstruktur Inhaltsdaten übergeben. Die Datenstruktur ermöglicht es, zusammenhängende Inhaltsdaten, wie zum Beispiel eine Adresse, durch Zuordnung zu einer Gruppe einfach strukturiert anzuzeigen. Dies unterstützt eine grundlegend verständliche Anzeige der Inhaltsdaten im Datenschutzcockpit. Mit diesem Gruppierungsmechanismus können die Inhaltsdaten in Form einer Baumstruktur vom Register an das Datenschutzcockpit übergeben werden. Das Register verwendet die übergebene Baumstruktur bereits ohne Inhaltsdaten im Abruf der Protokolldaten.

Mittels der Unterstruktur „InhaltsdatenBeschreibung“ wird für jedes Inhaltsdatum eine Kennzeichnung (ein sog. „Label“), eine optionale erläuternde Beschreibung, der Inhaltswert und die Kategorie des Inhalts angegeben. Damit lässt sich eine einfache Darstellung in der Form von: <Label>:<Wert> oder konkret: „Geburtsort: Berlin“ umsetzen.

Im Element Inhalt kann der anzuzeigende Wert als Zeichenkette übermittelt werden, in diesem Fall ist die Angabe des Datenformats im Element <Typ> optional. Anstelle einer Zeichenkette kann im Element Inhalt optional auch ein anderes Datenformat im Form einer Zeichenkette übermittelt werden. Damit der Inhalt im Datenschutzcockpit angezeigt werden kann, muss das Datenformat in diesem Fall im Element <Typ> angegeben werden. Das Datenschutzcockpit unterstützt die Anzeige einer festgelegten Liste von Datenformaten. Dabei kann es sich um primitive Typen (zum Beispiel dateTime) oder Dateitypen (zum Beispiel PDF- oder JPEG-Dateien) handeln, nicht aber um komplexe XML-Datentypen. Diese Liste der unterstützten Datenformate wird von den Verantwortlichen für das Datenschutzcockpit festgelegt und in einem menschen- und maschinenlesbaren Format mit einer eindeutigen Bezeichnung an einer festgelegten Stelle veröffentlicht. Damit eine Aktualisierung dieser Liste unabhängig vom Standard erfolgen kann, wird die Version der Liste nicht im Standard fest vorgegeben, es ist die jeweils aktuellste veröffentlichte Version zu nutzen.

Tabelle 8: Definition der Datenstruktur Inhaltsdaten

Linke Seite	Rechte Seite
<Inhaltsdaten>	(<Gruppe> <InhaltsdatenBeschreibung>, <Inhalt>), {<Gruppe> <InhaltsdatenBeschreibung>, <Inhalt>}
<Gruppe>	<Label>,[<Beschreibung>],<Inhaltsdaten>
<InhaltsdatenBeschreibung>	<Label>,[<Beschreibung>],[<Typ>],[<Kategorie>]
<Label>	string
<Beschreibung>	string
<Typ>	string
<Kategorie>	string
<Inhalt>	string

Gruppe: Mittels des Konstrukts <Gruppe> werden zusammengehörende Inhaltsdaten (z.B. eine Adresse) als zusammengehörend gekennzeichnet, so dass die Daten, wenn möglich, entsprechend gruppiert dargestellt werden können.

Label: Ein Text, der vor dem Inhalt ausgegeben wird, um die Art des Inhalts zu kennzeichnen (in Softwaresystemen üblicherweise als „Label“ bezeichnet).

Beschreibung: Eine optionale Beschreibung, die als zusätzliche Information zur Erläuterung im Datenschutzcockpit verwendet werden kann.

Typ: Gültige Werte sind in der außerhalb dieses Standards gepflegten Werteliste

Kategorie: Kategorie des Inhalts im Sinne der DSGVO Artikel 15. Die Bezeichnung der Kategorie wird von fachlicher Seite festgelegt, nicht vom Datenschutzcockpit.

Inhalt: Das Feld enthält entweder eine einfache Zeichenkette oder einen Base64 codierten Inhaltswert.

6.3.4. Fehler/Ausnahmen

Zu der gegebenen Identifikationsnummer existiert die angegebene uebermittlungID nicht.

6.3.5. Rahmenbedingungen

- Für das Element „Typ“ gibt es eine eindeutig referenzierbare Werteliste, in der die vom Datenschutzcockpit anzeigbaren Datentypen aufgelistet sind. Diese wird in einem menschen- und maschinenlesbaren Format mit einer eindeutigen Bezeichnung an einer festgelegten Stelle von den Verantwortlichen für das Datenschutzcockpit veröffentlicht und zur Verwendung vorgegeben. Die Register geben im Element „Typ“ nur Einträge aus dieser Liste an und übergeben auf diese Weise abgestimmte Bezeichnungen für Datenformate an das Datenschutzcockpit.

6.3.6. Vorbedingungen

Um den Parameter uebermittlungID angeben zu können, ist diese vom Datenschutzcockpit durch den Aufruf von *abfrageListeProtokolldaten* zu ermitteln.

7 Änderungshistorie

Version	Datum	Autor	Kapitel	Änderungen
1.0.1	06.12.2023	KoSIT/MG	-	Red. Änderungen #41-1,#41-3
1.0.1	10.01.2024	KoSIT/GD	Version, Copyright, Änderungshis- torie	Aktualisiert, Historie auf Ände- rungen zur aktuellen Version re- duziert