Technical Note – Common Audit Trail Exchange Format	**verbindlich** **Common-audittrails** **1.1.0** **Empfehlung**

Kurzbeschreibung	Spezifikation eines einheitlichen Protokollformates für die Übermittlung von Protokollen zur Überprüfung der Zulässigkeit von Anfragen auf Applikationsdaten.	
Autor(en):	Alena Sirka-Bred Hannes Wittmann	Projektteam / Arbeitsgruppe AG-RS: AG-Leiter: Bernhard Karning (BMDW) AG-Leiter-Stv.in: Martina Jacobs (Wien)
Beiträge von:	Ronald Bresich, Hildegard Freidl, Markus Frühwirt, Mirjam Jilka, Bernhard Karning, Harald Stradal	

Version 1.1.0 : **13.03.2019** Abgelehnt von:	Fristablauf: **TT.MM.JJJJ** (Länderangabe bei ablehnender Stellungnahme)
Unter-Version … : **TT.MM.JJJJ**	Fristablauf: **TT.MM.JJJJ** (Länderangabe bei ablehnender Stellungnahme)
Detail-Version … : **19.12.2019**	Freigabe: **17.01.2020** (Detailangaben zur Freigabe)

Inhalt

1. Einleitung 3
1.1 Zweck 3
1.2 Glossar 3
2. Rechtliche Grundlagen 4
2.1 Datenschutz-Grundverordnung DSGVO 4
2.2 Datenschutzgesetz DSG 4
2.2.1. Auswertung von Protokollen 4
2.2.2. Inhalt von Protokollen 5
2.2.3. Übermittlung von Protokollen 5
2.2.4. Aufbewahrungsdauer von Protokolldaten 5
2.3 Bestimmungen der Portalverbundvereinbarung (PVV): 5
3. Aufbau 6
3.1 Encoding und Uhrzeit 6
3.2 Feldtyp 6
3.3 Feldinhalt 6
3.4 Format 7
3.5 Reihenfolge 7
4. Daten 7
4.1 Datenfelder 7
4.2 Beschreibung Datenfelder 8
5. Beispiel einer Protokolldatensatzes 9
6. Referenzen 10
7. Zusammenfassung der Änderungen 10
8. Anhang 11
8.1 Referenzierung 11
8.2 Technische Beschreibung 11

1. Einleitung

1.1 Zweck

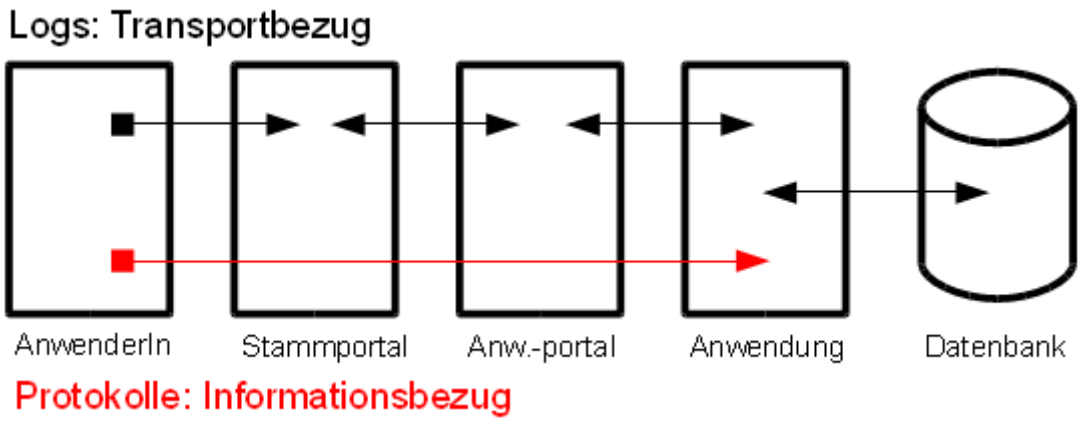
Damit Anwendungsverantwortliche, Stammportalbetreiber und zugriffsberechtigte Stellen ihre Pflichten nach der DSGVO (Wahrnehmung der Rechte Betroffener, Dokumentationspflichten, Festlegung technischer und organisatorischer Sicherheitsmaßnahmen, etc.) und der Portalverbundvereinbarung erfüllen können, ist die Protokollierung von Verarbeitungsvorgängen, die der Nachvollziehbarkeit der tatsächlichen Verwendung der Daten dienen, vorzusehen. Die Pflicht zur Protokollierung trifft in erster Linie den Betreiber bzw. soweit möglich die (Verantwortlichen nach Art.4 Z 7 DSGVO[1]).

Damit Anwendungsverantwortliche (nach Art.4 Z 7 DSGVO) hinsichtlich ihrer Verpflichtungen der DSGVO (z.B. Betroffenenrechte) wahrnehmen können, kann unter anderem die Protokollierung herangezogen werden. Die damit festgehaltenen Protokolldaten können zur Nachvollziehbarkeit der tatsächlichen Verwendung der Daten (Portalverbundvereinbarung) auf Antrag auch an zugriffsberechtigte Stellen übermittelt werden.

Da Anwendungsverantwortliche (i.S. der Portalverbundvereinbarung) Anwendungen der unterschiedlichsten Zwecke und Ausprägungen betreiben können, lässt sich naturgemäß kaum ein einheitliches Format für alle Protokolldaten im Sinne dieses Dokumentes festlegen. Für die Durchführung einer Revision bzw. der Überprüfung der Zulässigkeit von Zugriffen auf eine Anwendung im Einzelfall sind jedoch Mindestanforderungen für ein zu übermittelndes Protokoll für die Prüfzwecke erforderlich. Nur diese werden in der gegenständlichen Spezifikation definiert.

1.2 Glossar

Wichtig ist die Unterscheidung der oftmals verwendeten Begriffe „Protokoll“ und „Log“:



Protokoll:

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32016R0679

Aufzeichnungen der Anwendung, die der Kontrolle, ob personenbezogene Daten Dritter (Betroffener) oder andere „schützenswerte Daten“ ordnungsgemäß verwendet worden sind, dienen. Das Führen derartiger Aufzeichnungen ist notwendig, um den Pflichten gemäß DSGVO nachkommen zu können. Dieses Dokument betrachtet hier Protokolle nur in Bezug auf die Verarbeitung der Daten der protokollierungswürdigen Applikationim Hinblick auf An-/Abfrage, Bearbeitung (Neuanlage, Veränderung, Löschung) und Übermittlung von Verarbeitungsdaten.

Log:

Sammlung technisch relevanter Informationen, um bestimmte Systemkomponenten des Datenverkehrs nachvollziehen zu können. Diese Informationen dienen nicht dem oben beschriebenen Protokollführungszweck, sondern der abstrakten technischen Sicherheit. Die Spezifikationen von Logs im Portalverbund sind im Dokument „common-logs“ [CommLog] beschrieben.

2. Rechtliche Grundlagen

2.1 Datenschutz-Grundverordnung DSGVO

Im Gegensatz zum DSG 2000 kennt die EU Datenschutz-Grundverordnung keine verpflichtende Protokollierung von Verwendungsvorgängen. Diese können allenfalls aus der Verpflichtung zur Umsetzung der Betroffenenrechte gemäß Art. 15 – 22 sowie den Art. 24, 25 und 32 DSGVO abgeleitet werden. Die Entscheidung zur Protokollierung trifft hierbei der Verantwortliche im Sinne der DSGVO.

2.2 Datenschutzgesetz DSG

Das Datenschutzgesetz regelt die offenen Punkte der DSGVO, welche durch die Öffnungsklauseln dem Gesetzgeber zur Regelung überlassen wurde.

Für die Sicherheitsbehörden ist im DSG eine verpflichtende Protokollierung der Verarbeitungsvorgänge vorgesehen.

2.2.1. Auswertung von Protokollen

Protokolle dürfen nur für die im Einklang mit datenschutzrechtlichen Vorgaben nominierten Zwecke ausgewertet werden, wenn nicht einschlägige Bestimmungen zusätzliche Verwendungszwecke erlauben. Unvereinbar ist insbesonders die Weiterverwendung zum Zweck der Kontrolle von Betroffenen, deren Daten im protokollierten Datenbestand enthalten sind, oder zum Zweck der Kontrolle jener Personen, die auf den protokollierten Datenbestand zugegriffen haben, aus einem anderen Grund als jenem der Prüfung ihrer Zugriffsberechtigung, sofern dies nicht durch Materiengesetze geregelt ist.

Die Verantwortung für den Zugriff auf Protokolldaten liegt beim Anwendungsverantwortlichen, der auf Basis eines Rollen- und Rechtemodells eine Regelung für die Auswertung bereitstellen muss.

2.2.2. Inhalt von Protokollen

Welche Daten ein Protokoll beinhalten darf bzw. muss, ergibt sich aus dem Zweck der Protokollierung in Verbindung mit dem Verhältnismäßigkeitsprinzip: In Protokollen dürfen nur jene Daten verwendet werden, die für die Erreichung des Zwecks des Protokolls tatsächlich erforderlich sind.

Bei den für den Zweck der Portalverbund-Revision ausgestellten Abzügen aus dem Protokoll ist demgemäß ebenfalls darauf zu achten, dass darin nur Protokolldaten enthalten sind, die für den jeweiligen Revisionszweck erforderlich sind. Bei den in diesem Dokument definierten MUSS-Feldern ist davon auszugehen, dass sie für die Revision erforderlich sind. Bei den KANN-Feldern muss dies im Anlassfall durch den Verantwortlichen überprüft werden.

2.2.3. Übermittlung von Protokollen

Bei der Übermittlung der Revisionsprotokolle an die anfordernde Stelle sind entsprechende Maßnahmen zu treffen, die eine Einsicht in die Protokolle durch unbefugte Dritte verhindern. Dies soll durch organisatorische und/oder technische Maßnahmen im Sinne des Art. 32 DSGVO geregelt werden.

2.2.4. Aufbewahrungsdauer von Protokolldaten

Die Aufbewahrungsdauer von Protokolldaten ist vom Verantwortlichen hinsichtlich der datenschutzrechtlichen Vorgaben des Zwecks der Verarbeitung unter Beachtung allfälliger materiellrechtlicher Grundlagen, sowie bi- oder multilateraler Vereinbarungen festzulegen. Für die Aufbewahrung von Protokolldaten sind die Datensicherheitsmaßnahmen gemäß Art. 32 DSGVO (Sicherheit der Verarbeitung) anzuwenden.

Sofern daher keine dezitierten Gründe im jeweiligen Anwendungsfall für eine längere bzw. kürzere Aufbewahrungsdauer sprechen, haben die Anwendungs-verantwortlichen eine Aufbewahrungsdauer von drei Jahren einzuhalten. Die Entscheidung darüber trifft die/der Anwendungsverantwortliche als „Verantwortlicher der Datenanwendung“ im Sinne der DSGVO.

Aufbewahrungsdauer beim Empfänger der Protokolle:

Grundsätzlich sind die zur Revision übermittelten Protokolldaten der Applikation mit Abschluss der Revision beim Empfänger der Protokolldaten zu vernichten, sofern nicht eine längere Aufbewahrungsdauer aufgrund besonderer Rechtsgrundlagen vorsehen ist. Auch in diesem Fall sind Datensicherheitsmaßnahmen gemäß Art. 32 DSGVO zu treffen.

2.3 Bestimmungen der Portalverbundvereinbarung (PVV):

Es ist im Rahmen des Portalverbundes für Kontrollzwecke notwendig, erfolgte Zugriffe ex post auf ihre Zulässigkeit hin zu überprüfen. Dazu ist die Möglichkeit der Rückführbarkeit der Abfrage/des Zugriffs auf einen bestimmten Geschäftsfall der zugreifenden Stelle erforderlich.

Verweis auf bezughabende Bestimmungen der PVV:

- Der Stammportalbetreiber hat mindestens einmal jährlich eine **Sicherheitsrevision** durchzuführen oder zu veranlassen. Die Revision muss sich auf Sicherheitsrichtlinien beziehen, in der die im Anhang 2 (*Anm.: Spezifikation Sicherheitsklassen im Portalverbundsystem*) beschriebenen Maßnahmen entsprechend der geforderten Sicherheitsklasse als Mindeststandard gelten (§ 6 Abs. 6 PVV).
- Die zugriffsberechtigte Stelle (§3 Z 10 PVV)[2] kann vom Abwendungs-verantwortlichen **Auswertungen über die erfolgten Zugriffe** durch Benutzer aus ihrem Bereich **für Kontrollzwecke** anfordern (§ 7 Abs. 4 PVV).
- **Entzug der Zugriffsberechtigung**: Der Stammportalbetreiber hat einem Benutzer seine individuelle Zugriffsberechtigung zu entziehen, wenn dem Stammportalbetreiber zur Kenntnis gelangt, dass der Benutzer seine Zugriffsberechtigung nicht ordnungsgemäß gebraucht (§ 11 Abs. 1d PVV).

3. Aufbau

3.1 Encoding und Uhrzeit

Die protokollierten Daten werden nach dem UTF 8 Standard kodiert[3]. Die Uhrzeit ist als lokale Uhrzeit anzugeben.

3.2 Feldtyp

Die protokollierten Datenfelder werden in zwei Bereiche untergliedert:

- **Muss (M)** – die in Pkt 4.1 definierten Datenfelder müssen verpflichtend angeliefert werden.
- **Kann (K)** – weitere Datenfelder sollten angeliefert werden wenn sie in der Applikation vorhanden sind bzw. von der Applikation ermittelt werden können, um zusätzliche Informationen in das Protokoll zu integrieren.

3.3 Feldinhalt

Die protokollierten Daten werden in zwei Bereiche untergliedert:

- **Muss (M)** – für als Mussfeld gekennzeichnete Datenfelder müssen verpflichtend Feldinhalte protokolliert bzw. angeliefert werden.
- **Kann (K)** – wird ein Kannfeld innerhalb der aufgerufenen Applikation nicht verwendet oder ist nicht befüllt, so ist ein leeres Feld anzuliefern.

[2] http://reference.e-government.gv.at/uploads/media/pvv1.0-21112002.pdf

[3] http://de.wikipedia.org/wiki/UTF-8

3.4 Format

Das Format des Protokolls ist so ausgelegt, das es von EDV-Systemen, Betriebssystemen und Applikationen unabhängig verarbeitet werden kann. Das Protokoll muss in computerverarbeitbarer Form (als Datei) bereitgestellt werden. Die Daten werden zeilenweise, durch Trennzeichen getrennt, ausgegeben und müssen mit einer Kopf-Zeile (Feldbezeichnung) versehen werden. Die Bezeichnungen der Feldnamen sind beizubehalten.

Bevorzugt wird das CSV-Format mit Strichpunkt als Trennzeichen und doppelten Hochkomma als Feldbegrenzungszeichen wie im Beispiel angegeben.

3.5 Reihenfolge

Die Reihenfolge der Datenfelder muss eingehalten werden, um die Lesbarkeit der Protokolle zu vereinfachen. Für weitere Datenfelder wird sinngemäß keine Reihenfolge vorgegeben. Es ist jedoch sinnvoll, wichtige Kann-Felder direkt nach den Muss-Feldern zu reihen.

4. Daten

4.1 Datenfelder

Das technische Mapping der einzelnen Feldinhalte wird im Anhang beschrieben.

Nummer	Bezeichnung	Beschreibung	Beispiel	Feldinhalt
1	Anfragedatum	Datum der getätigten Anfrage an die Applikation	20100401	M
2	Anfragezeitpunkt	Uhrzeit der getätigten Anfrage	14:21:00	M
3	Benutzerkennung	Benutzerkennung des anfragenden Users	mmuster	M
4	Name	Name des/der AnwenderIn	Monika Musterfrau	K
5	Organisationseinheit	Organisationseinheit des/der AnwenderIn	Abteilung 11	M
6	Applikationskennung	Name des aufgerufenen Programms	ZMR	M
7	Verarbeitungsart (UseCase)	Beschreibung des UseCases (Verarbeitungsart) der Protokollzeile	Standardanfrage	M
8	Bearbeitungsgrund	Geschäftsfallkennung, oder sonstige Verbalbegründung durch den User selbst vergeben	AKT/123/2010	K

9	Workflow-ID / Transaktions-Kennzeichen	Eine eindeutige Nummer zur Zusammenführung von Anfrage und des Ergebnis innerhalb des Protokolls	493801	K
10	Abfrage/Ergebnis	Wert der Anfrage bzw. an die Applikation	Mustermann	K

4.2 Beschreibung Datenfelder

Anfragedatum:

Das Datum der Anfrage an die Applikation, welches mindestens Jahr, Monat und Tag beinhalten muss. Das Format des Datums ist vorgegeben, zu protokollieren ist ein 8-stelliges Datum in der Form JJJJMMTT.

Beispiel: 20100401 für den 1. April 2010

Anfragezeitpunkt:

Der Zeitpunkt der Anfrage, welcher mindestens Stunde, Minute und Sekunde beinhalten muss. Eine kürzere Zeiteinheit als Sekunden ist nicht sinnvoll.

Beispiel: 14:21:00 für 14 Uhr 21 und 00 Sekunden

Benutzerkennung:

Eine eindeutige Identifikation des anfragenden Benutzers innerhalb des Service-Konsumenten.

Beispiel: mmuster

Beispiel: at:vkz:L9:mmuster

Name:

Der Name der/des abfragenden AnwenderIn. Ist dieser im Protokoll vorhanden, so ist er verpflichtend anzuliefern.

Beispiel: Monika Musterfrau

Organisationseinheit:

Ist innerhalb der Organisation eine Untergliederung vorhanden, so müssen die Organisationseinheiten dargestellt werden um Protokolldatensätze entsprechend aufzuteilen.

Beispiel: Abteilung 11

Applikationskennung:

Werden innerhalb einer Applikation verschiedene Anwendungen (oder Anfragen) angeboten, so sind diese auf die Anfrage bezogen im Protokolldatensatz anzugeben.

Beispiel: ZMR

Verarbeitungsart:

Beschreibt die Verarbeitungsart oder den UseCase der Anfrage (z.B. ob die Protokollzeile eine Anfrage an die Applikation oder eine Antwort darstellt). Das Format ist abhängig von der Applikation.

Beispiel: Standardanfrage

Bearbeitungsgrund:

Die Nummer des Geschäftsfalls ermöglicht die Zuordnung innerhalb der Organisation und erlaubt somit die Revision. Somit kann überprüft werden ob die Daten der Anfrage mit dem Geschäftsfall in Verbindung stehen und kein Missbrauch stattgefunden hat.

Beispiel: AKT/123/2018

Workflow-ID/ Transaktions-Kennzeichen:

Die Workflow-ID bzw. das Transaktions-Kennzeichen erlaubt ein Zusammenführen von Anfrage und Auskunft in den Protokolldaten der Protokolldatei.

Beispiel: 493801

Dieses Feld ist abhängig von der Anwendung. Wenn keine Datensätze zusammengeführt werden sollen, ist auch eine gemeinsame ID nicht notwendig.

Anfrage/Ergebnis:

Der Inhalt der Anfrage innerhalb einer Protokollzeile, die an die Applikation gesendet wurde oder das Ergebnis in einer Protokollzeile pro Treffer. Im Beispiel will der/die AnwenderIn alle Fahrzeuge des Anfragewertes (Mustermann) wissen.

Anfrage: Mustermann

Ergebnis: W-12345

Eine genaue Spezifikation von Anfrage/Ergebnis ist nicht möglich, da diese Felder abhängig von der Applikation bereit gestellt werden müssen. Die protokollierten Inhalte müssen eine Revision unterstützen. Im Revisionsprotokoll sollten diese Daten nur dann aufscheinen, wenn sie für die Prüfung der Zulässigkeit des Zugriffs erforderlich sind.

5. Beispiel einer Protokolldatensatzes

Der Protokolldatensatz besteht aus einer Anfrage an ein Applikation (Anfrage) und der Antwort (Auskunft). Über die gemeinsame Workflow-ID bzw. Transaktionsnummer (493801) können die Datensätze zusammengefasst werden. Über die Nummer des Geschäftsfalles (M26/123/2010) in der Anfrage können die Datensätze dem Anfragegrund zugeordnet und somit revisioniert werden.

```
"Anfragedatum";"Anfragezeitpunkt";"Benutzerkennung";"Name";"Organisat
ionseinheit";"Applikationskennung";"Verarbeitungsart(UseCase)";"Bearb
eitungsgrund";"Transaktions-Kennzeichen";"Abfrage/Ergebnis"

"20010401";"14:21:00";"mmuster";"Monika_Musterfrau";"Abteilung11";"ZM
R";"Standardanfrage";"AKT/123/2010";"493801";"Mustermann"


"20010401"; "14:21:30";"mmuster";"Monika_Musterfrau";"Abteilung11";
"EKA-KZN";"Standardauskunft";"AKT/123/2010";"493081";"Adressedaten"
```

6. Referenzen

[EU-DSGVO]	Feiler L., Forgó N., EU-Datenschutz-Grundverordnung, Verlag Österreich, 2017
[DSG]	Pollirer/Weiss/Knyrim/Haidinger, DSG Datenschutzgesetz[3], Manz Verlag, 2017
[DSG]	Bresich/Dopplinger/Dörnhofer/Kunnert/Riedl, DSG Datenschutz Kommentar, Linde Verlag, 2018

[CommLog] *Müllner, Kremser, Reif*; Technical Note – Common Log File Format zum Austausch im Portalverbund; Version 1.0.7

[PVP] *Hörbe, Pfläging*; Portal Verbund Protokoll; Version 2.1.3

[PVV] *Connert, Grandits, Kotschy, Posch, Siegl*; Portal Verbund Vereinbarung; Version 1.0

7. Zusammenfassung der Änderungen

- 02.12.2010 Version 1.0 Erstellung des Dokumentes
- 13.03.2019 Version 1.1 Anpassungen an die DSGVO

8. Anhang

8.1 Referenzierung

Für die Zwecke der Revision im Portalverbund werden im Anhang die Datenfelder des zu übermittelnden Protokolls den Datenfeldern des Portalverbundprotokolls in der Version 2.1 R-Profil [PVP] gegenübergestellt.

Nummer	Bezeichnung	PVP
1	Anfragedatum	
2	Anfragezeitpunkt	
3	Benutzerkennung	AUTHENTICATE-UserID
4	Name	AUTHENTICATE-cn
5	Organisationseinheit	AUTHENTICATE-gvOuId
		AUTHENTICATE-Ou
		AUTHORIZE-gvOuId
		AUTHORIZE-Ou
6	Applikationskennung	
7	Verarbeitungsart (UseCase)	
8	Bearbeitungsgrund	
9	Transaktions-Kennzeichen	
10	Anfrage/Ergebnis	

8.2 Technische Beschreibung

Alle in Tabelle Datenfelder als Mussfeld (M) gekennzeichneten Felder müssen angeliefert werden. Wird ein Feld innerhalb der aufgerufenen Applikation nicht verwendet, so ist ein leeres Feld anzuliefern.

Anfragedatum:

8-stelliges Datum im Format JJJJMMTT.

Beispiel: 20100401

Anfragezeitpunkt:

8-stellige lokale Uhrzeit im Format HH:MM:SS.

Beispiel: 14:21:00

Benutzerkennung:

Für die Benutzerkennung des/der AnwenderIn ist das Feld **AUTHENTICATE-UserID** aus dem Portalverbundprotokoll zu verwenden.

Name:

Für die Benutzerkennung des/der AnwenderIn ist das Feld **AUTHENTICATE-cn** aus dem Portalverbundprotokoll zu verwenden.

Organisationseinheit des Benutzers:

Es ist mindestens ein gefülltes Datenfeld der Organisationseinheit anzugeben. Folgende Felder aus dem Portalverbundprotokoll können verwendet werden:

- **AUTHENTICATE-gvOuId**
- **AUTHENTICATE-Ou**
- **AUTHORIZE-gvOuId**
- **AUTHORIZE-Ou**

Werden mehrere Felder angegeben, so sind diese entsprechend in mehrere Datenfelder aufzuteilen.

Applikationskennung:

Applikationskennung entsprechend der Anwendung.

Beispiel: ZMR

Verarbeitungsart (UseCase):

Verarbeitungsart oder UseCase der Anfrage bzw. des Ergebnis.

Beispiel: Standardanfrage

Bearbeitungsgrund:

Wird bei der Anfrage durch den/die AnwenderIn eingegeben.

Beispiel: AKT/123/2010

Transaktions-Kennzeichen:

Transaktions-Kennzeichen zur Verknüpfung von Anfrage und Ergebnis. Einer Anfrage können (applikationsabhängig) mehrere Ergebnisse zugeordnet werden.

Beispiel: 493801

Anfrage/Ergebnis:

Der Inhalt der Anfrage bzw. das Ergebnis innerhalb der Protokollzeile wird durch die Applikation vorgegeben und soll eine Revision der Anfrage ermöglichen. Sind innerhalb der Anfrage oder des Ergebnisses mehrere Datenfelder vorhanden, so sind diese in getrennte Felder zu übermitteln.