Richtlinie

Bearbeitung von Auskunftsanfragen (Art. 15 DSGVO)

1 Vorwort und Zweck

Diese Richtlinie beschreibt verbindlich, wie wir Auskunftsanfragen betroffener Personen nach Art. 15 DSGVO

- entgegennehmen,
- prüfen,
- bearbeiten und
- beantworten.

Es dient allen Bereichen als praktische Arbeitsunterlage und enthält neben dem End-to-End-Prozess auch Musterschreiben und Formulare sowie eine fachbereichsspezifische Datenlandkarte. Ziel ist es,

- effizient,
- einheitlich,
- rechtssicher und
- fristgerecht

zu agieren – unabhängig davon, ob eine Anfrage nur einen Fachbereich oder die gesamte Organisation betrifft, und unabhängig davon, ob sich die Anfrage auf Kunden, Interessenten, Lieferantenkontakte, Bewerber, Beschäftigte oder ehemalige Beschäftigte bezieht.

2 Geltungsbereich und Rechtsgrundlagen

Die Richtlinie gilt für alle Konzerngesellschaften, Standorte, Systeme und Prozesse, in denen personenbezogene Daten verarbeitet werden. Rechtsgrundlagen sind insbesondere Art. 12 und 15 DSGVO (Transparenz und Auskunft), flankiert durch Grundsätze aus Art. 5 DSGVO (Rechtmäßigkeit, Zweckbindung, Datenminimierung etc.). Spezielle Schutzanforderungen gelten bei

- besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) sowie
- bei Betriebs-/Geschäftsgeheimnissen und
- Rechten Dritter.

3 Begriffe (Kurzüberblick)

Auskunft ist das Recht der betroffenen Person, eine Bestätigung über die Verarbeitung sowie ggf. eine Kopie ihrer personenbezogenen Daten und Zusatzinformationen aus Art. 15 DSGVO zu erhalten.

Betroffene Personen sind etwa Kunden, Nutzer, Bewerber, Lieferantenkontakte, Beschäftigte oder ehemalige Beschäftigte.

Empfänger sind interne Stellen oder Dritte, denen Daten offengelegt wurden.

Auftragsverarbeiter verarbeiten Daten weisungsgebunden für uns.

Gemeinsame Verantwortliche bestimmen Zwecke und Mittel gemeinsam mit uns.

4 Rollen und Zuständigkeiten

Die Gesamtzuständigkeit liegt bei der Datenschutzkoordindation der involvierten Fachbereiche.

Der **Datenschutzkoordinator unternehmensweit | Zentrale Stelle** eröffnet Tickets, koordiniert die involvierten Fachbereiche, korrespondiert mit der betroffenen Person und überwacht Fristen.

Der **Datenschutzkoordinator des Fachbereichs** überwacht Fristen, initiiert die Klärung des Umfangs und der Datenerhebung und führt den Abschluss herbei.

Juristische Prüffälle, Ablehnungen oder Verlängerungen werden vom **Datenschutzbeauftragten/Recht & Compliance** entschieden und freigegeben.

IT-Abteilung unterstützt bei systemweiten Suchen, Exporten und der sicheren Bereitstellung.

Die **Fachbereiche** sind für das Auffinden und fachliche Einordnen der eigenen Daten verantwortlich.

Die **Informationssicherheit** stellt sichere Transportwege, Zugriffskontrollen und Protokollierung sicher.

Das **Dienstleister-/Lieferantenmanagement** bindet Auftragsverarbeiter ein und überwacht Rückläufe.

4.1 Rollen

4.1.1 Zuständigkeiten je Prozess

Datenschutzbeauftragter			
Funktion	**Name**	**E-Mail**	**Telefonnummer(n)**
Zuständig			
Vertretung			

Datenschutzkoordinator (unternehmensweit) | Zentrale Stelle			
Funktion	**Name**	**E-Mail**	**Telefonnummer(n)**

Zuständig			
Vertretung			

IT-Abteilung			
Funktion	**Name**	**E-Mail**	**Telefonnummer(n)**
Zuständig			
Vertretung			

Informationssicherheitsbeauftragter			
Funktion	**Name**	**E-Mail**	**Telefonnummer(n)**
Zuständig			
Vertretung			

Recht & Compliance			
Funktion	**Name**	**E-Mail**	**Telefonnummer(n)**
Zuständig			
Vertretung			

Dienstleister-/Lieferantenmanagement			
Funktion	**Name**	**E-Mail**	**Telefonnummer(n)**
Zuständig			
Vertretung			

4.1.2 Zuständigkeiten je Fachbereich

Einkauf & Beschaffung			
Datenschutzkoordination			
Funktion	**Name**	**E-Mail**	**Telefonnummer(n)**
Zuständig			
Vertretung			
Fachbereich			
Funktion	**Name**	**E-Mail**	**Telefonnummer(n)**
Zuständig			
Vertretung			

Facility Management & Sicherheit
Datenschutzkoordination

Fachbereich			
Funktion	**Name**	**E-Mail**	**Telefonnummer(n)**
Zuständig			
Vertretung			

Recht & Compliance			
Datenschutzkoordination			
Funktion	**Name**	**E-Mail**	**Telefonnummer(n)**
Zuständig			
Vertretung			
Fachbereich			
Funktion	**Name**	**E-Mail**	**Telefonnummer(n)**
Zuständig			
Vertretung			

Vertrieb			
Datenschutzkoordination			
Funktion	**Name**	**E-Mail**	**Telefonnummer(n)**
Zuständig			
Vertretung			
Fachbereich			
Funktion	**Name**	**E-Mail**	**Telefonnummer(n)**
Zuständig			
Vertretung			

4.2 Zuständigkeiten-Matrix

Die folgende Tabelle zeigt die Zuständigkeiten pro Prozessschritt:

Prozessschritt	Datenschutz-koordination (unternehmensweit)	Datenschutz-beauftragter / Recht & Compliance (falls erforderlich)	IT-Abteilung	Datenschutz-koordinator Fachbereich/Fachbereich	Informations-sicherheitsbeauftragter	Dienstleister-/Lieferanten-management
Eingang & Ersteinstufung	führt durch (operativ verantwortlich)	wird zur Beratung hinzugezogen	wird informiert	wird informiert	wird informiert	wird informiert
Identitätsprüfung	führt durch (operativ verantwortlich)	wird zur Beratung hinzugezogen	wird informiert	wird zur Beratung hinzugezogen	wird informiert	wird informiert
Umfang klären (Scoping)	führt durch (operativ verantwortlich)	wird zur Beratung hinzugezogen	wird zur Beratung hinzugezogen	trägt die Gesamtverantwortung für die	wird informiert	wird informiert

- Ansprechpartner,
- betroffene(n) Fachbereich(e) und
- Frist.

Dieser leitet die Anfrage an die Datenschutzkoordination des Fachbereichs bzw. der Fachbereiche weiter.

Doppelmeldungen werden zusammengeführt. Jeder externe Kontakt erfolgt über die im Kapitel „Musterschreiben“ beschriebenen standardisierten Texte.

4.5 Standardprozess (End-to-End)

Der Gesamtprozess verläuft in neun Schritten. Die Schritte sind unabhängig von der Anzahl der betroffenen Bereiche identisch. Nur die Koordinations- und Konsolidierungsaufwände steigen mit der Anzahl der Datenquellen.

4.5.1 Eingang & Ersteinstufung

Nach Eingang wird das Ticket angelegt, die Frist gesetzt und die Art des Begehrens bestätigt (Auskunft vs. Löschung/Berichtigung/Übertragbarkeit). Bei Mehrfachrechten wird sauber getrennt und ggf. parallel gearbeitet. Offenkundig fachfremde Anträge werden mit der Person abgestimmt, ohne die Bearbeitung zu verzögern.

4.5.2 Identitätsprüfung

Die Prüfung erfolgt risikobasiert und datenminimiert. Bestehende Kunden- oder Mitarbeiterkonten mit starker Authentifizierung genügen regelmäßig. Bei Vertreterinnen und Vertretern wird die Vollmacht geprüft und ggf. nachgefordert. Bei Beschäftigten und ehemaligen unterstützt die Personalabteilung die Verifikation intern, ohne unnötige Dokumente zu erzeugen. Nachweise werden nach Abschluss sicher gelöscht, die Erforderlichkeit wird dokumentiert.

4.5.3 Routing und Datenlandkarte

Anhand der Datenlandkarte werden betroffene Systeme und Daten identifiziert.

Auftragsverarbeiter werden nach AV-Vereinbarung eingebunden. Bei Konzernverbund werden ggf. gemeinsame Verantwortlichkeiten berücksichtigt.

4.5.4 Scoping

Der Umfang wird zweckmäßig eingegrenzt:

- relevante Zeiträume,
- Kommunikationskanäle,
- beteiligte Systeme und
- eindeutige Identifikatoren (z. B. Kundennummer, E-Mail-Adresse, Personalnummer).

Wo Präzisierungen erforderlich oder sinnvoll sind, werden diese mithilfe des Musterschreibens angefragt. Ohne Rückmeldung erfolgt eine angemessene, generalistische Suche.

Datenlandkarte ergänzen sich: Der Prüfstandard stellt die Vorgehensweise sicher, die Datenlandkarte hilft dabei, dass die fachbereichstypischen Systeme und Ablagen berücksichtigt werden. Dabei ist zu beachten, dass die Datenlandkarten lediglich als Hilfsmittel eingesetzt werden dürfen und keine abschließende Prüfung durch den Mitarbeiter ersetzen können. Die Datenlandkarte ist laufend zu aktualisieren und an die tatsächlichen Begebenheiten in dem Fachbereich anzupassen.

5.1 Such- und Identifikationslogik

Bei der Suche nach personenbezogenen Daten arbeiten Sie immer mit mehreren Suchschlüsseln und berücksichtigen Schreibvarianten sowie Altstände. Verlassen Sie sich nie ausschließlich auf

- Name oder E-Mail-Adresse.

Nutzen Sie – je nach Kontext – zusätzlich

- Telefonnummern,
- frühere E-Mail-Adressen,
- frühere Namen,
- Anschrift,
- Kunden- oder Vertragsnummern,
- Ticket- oder Vorgangsnummern,
- Bestell- oder Rechnungsnummern,
- interne Kennungen (zum Beispiel Benutzerkennung)

und weitere Referenzen, die im jeweiligen Prozess verwendet werden. Wenn eine Nummer oder Kennung im Prozess als „führender Schlüssel“ genutzt wird, ist sie auch Ihr primärer Suchschlüssel.

Beziehen Sie außerdem standardmäßig ein, dass Systeme und Datenbestände **mehrfach vorhanden** sein können (zum Beispiel mehrere Gesellschaften, Standorte, Regionen, Mandanten, Workspaces oder getrennte Instanzen). Ein Treffer „nicht gefunden“ gilt erst dann als belastbar, wenn die Suche in allen relevanten Strukturen erfolgt ist.

5.2 Pflicht-Prüfobjekte je Fundstelle

Wenn Sie eine Fundstelle identifiziert haben, prüfen Sie den Datenbestand vollständig und nicht nur die Erstansicht oder eine Listenübersicht. Öffnen Sie Datensätze konsequent bis in die Detailansicht und gehen Sie alle Bereiche durch, die Inhalte zur Person enthalten können – insbesondere Stammdaten, zusätzliche Felder, Historien, Statusinformationen, Verknüpfungen, Dokumente/Anhänge und Freitextfelder.

Achten Sie darauf, dass personenbezogene Informationen häufig nicht im Hauptfeld, sondern in Anlagen liegen. Prüfen Sie daher immer alle Anhänge und Uploads zum Beispiel

- Portable Document Format (PDF),

5.7 Protokoll- und Auditspuren

Prüfen Sie Protokoll- und Auditdaten, soweit sie im System vorhanden und zugänglich sind. Dazu gehören

- Änderungsverläufe,
- Exportereignisse,
- Upload- und Downloadspuren,
- Protokolle zu Freigaben,
- Zugriffs- oder Einsichtsprotokolle sowie
- Rollen- und Berechtigungsänderungen.

Bewerten Sie solche Protokolle nicht als „nur technisch“. Sie enthalten häufig personenbezogene Informationen (wer hat wann was gesehen, geändert, exportiert oder freigegeben) und können außerdem Hinweise geben, wo Kopien entstanden sind oder wohin Daten weitergegeben wurden.

5.8 Zugriffsbeschränkungen und sensible Bereiche

Gehen Sie grundsätzlich davon aus, dass es in nahezu jedem Fachbereich zugriffsbeschränkte Bereiche gibt. „Nicht sichtbar“ bedeutet nicht „nicht vorhanden“. Wenn ein Bereich aufgrund von Need-to-know, Rollenrechten oder Schutzstufen nicht einsehbar ist, binden Sie die zuständige Stelle ein, die Zugriff hat, und lassen Sie die relevanten Daten dort ermitteln.

Behandeln Sie besonders geschützte Systeme und Fallakten (zum Beispiel Hinweisgebersysteme, interne Untersuchungen, besondere Eskalationsakten) nicht als Sonderfall außerhalb des Prüfstandards, sondern als reguläre Prüforte mit erhöhten Zugriffsvorgaben.

5.9 Daten Dritter und Schwärzungsbedarf

Achten Sie frühzeitig darauf, ob in Fundstellen Daten weiterer Personen enthalten sind. Das betrifft insbesondere Anhänge, Freitextfelder, Protokolle und Kommunikationsverläufe, in denen häufig zusätzliche Beteiligte genannt werden (zum Beispiel Zeugen, Hinweisgeber, Bearbeiter, Ansprechpartner, Vertreter oder sonstige Dritte).

Wenn solche Daten auftauchen, ist dies bei der Zusammenstellung der Auskunft zu berücksichtigen (insbesondere zur Abgrenzung und – falls erforderlich – Schwärzung). Prüfen Sie daher Inhalte nicht nur auf „Treffer zur betroffenen Person“, sondern auch auf enthaltene Drittinformationen.

6 Weiterführende Informationen

6.1 Prüfung der Identität

Bestehen Zweifel an der Identität der betroffenen Person, muss vor der Auskunfterteilung sichergestellt werden, dass die anfragende Person wirklich die betroffene Person ist. Ziel ist, eine

Schwärzungen erfolgen somit nur nach konkreter Einzelfallprüfung, soweit die Offenlegung bestimmter Informationen die Rechte und Freiheiten anderer Personen tatsächlich beeinträchtigen würde. Eine pauschale Schwärzung bestimmter Personengruppen, etwa sämtlicher Mitarbeitenamen, erfolgt nicht. Soweit möglich, werden mildere Mittel geprüft, etwa Teilschwärzungen, Zusammenfassungen oder Kontextangaben.

6.5 Fristverlängerung

Die Frist zur Beantwortung einer Betroffenenanfrage beträgt grundsätzlich einen Monat ab Eingang der Anfrage. Eine Verlängerung um bis zu zwei weitere Monate ist nur als Ausnahme zulässig, wenn dies erforderlich ist und zwar unter Berücksichtigung der Komplexität der Anfrage oder der Anzahl der Anträge. Erforderlich bedeutet: Mit den vorhandenen Ressourcen und wegen objektiver Umstände (z. B. sehr umfangreiche Recherchen über mehrere Systeme, viele Verarbeitungsvorgänge, notwendige Abstimmungen mit Fachbereichen, Aufbereitung großer Datenmengen) kann eine sachgerechte und vollständige Antwort innerhalb eines Monats nicht realistisch erstellt werden. Eine Verlängerung darf nicht „vorsorglich“ oder als Standard gesetzt werden, sondern nur, wenn Sie sie im konkreten Fall nachvollziehbar begründen können.

Bitte beachten: Die Verlängerung muss der betroffenen Person innerhalb des ersten Monats nach Eingang der Anfrage mitgeteilt werden, zusammen mit einer kurzen Begründung für die Verzögerung und dem neuen spätesten Antwortdatum.

6.6 Negativauskunft

Eine Negativauskunft wird erteilt, wenn nach sorgfältiger Prüfung der verfügbaren Systeme und Unterlagen zu den von der betroffenen Person angegebenen Identifikationsmerkmalen keine personenbezogenen Daten gefunden werden, die wir unabhängig von der Bearbeitung der Betroffenenanfrage verarbeiten. Vor Versand einer Negativauskunft ist sicherzustellen, dass die Identität ausreichend verifiziert ist, soweit dies im konkreten Fall erforderlich ist, und dass die Suche nachvollziehbar in den relevanten Systemen erfolgt ist. Die Negativauskunft wird klar und verständlich formuliert: Sie teilen mit, dass aktuell keine weiteren personenbezogenen Daten zur Person verarbeitet werden und deshalb keine Auskunft zu weiteren Daten erteilt werden kann.

Wichtig ist, dass auch bei einer Negativauskunft regelmäßig dennoch personenbezogene Daten verarbeitet werden, nämlich die Daten aus der Anfrage selbst und aus der dazugehörigen Kommunikation. Diese Verarbeitung dient der Bearbeitung und Dokumentation der Betroffenenanfrage sowie der Erfüllung der gesetzlichen Pflichten nach der DSGVO und gegebenenfalls der Rechtsverteidigung. Deshalb enthält die Negativauskunft die Pflichtangaben nach Art. 15 DSGVO bezogen auf diese Verarbeitung, insbesondere zu den Verarbeitungszwecken, den Kategorien der verarbeiteten Daten (z. B. Identifikations- und Kontaktdaten, Sachverhaltsdaten, Kommunikations- und Metadaten), den Empfängern bzw. Kategorien von Empfängern, einer möglichen Übermittlung in Drittländer und den dazugehörigen Garantien, der Speicherdauer

6.9.3 Kategorien personenbezogener Daten

Art. 15 Abs. 1 lit. b) DSGVO:
„die Kategorien personenbezogener Daten, die verarbeitet werden“

Bedeutung:

Die betroffene Person muss erfahren, welche Arten von personenbezogenen Daten über sie verarbeitet werden. Gemeint sind Datenkategorien, also Gruppen von Daten. Beispiele sind Stammdaten, Kontaktdaten, Vertragsdaten, Zahlungsdaten, Kommunikationsdaten, Bewerbungsdaten, Nutzungsdaten, Protokolldaten oder Beschwerdedaten.

Diese Information ist für die betroffene Person wichtig, weil sie dadurch einen Überblick darüber erhält, welche Lebens- oder Tätigkeitsbereiche von der Verarbeitung betroffen sind. Es macht einen Unterschied, ob wir nur einfache Kontaktdaten gespeichert haben oder zusätzlich Zahlungsinformationen, Gesundheitsdaten, interne Bewertungen, Kommunikationsverläufe oder Verhaltensdaten.

Die Datenkategorien helfen der betroffenen Person auch dabei einzuschätzen, wie sensibel die Verarbeitung ist. Manche Daten sind für die Privatsphäre weniger kritisch, andere können besonders schutzbedürftig sein. Bewerbungsunterlagen, Gesundheitsinformationen, Kontodaten oder Leistungsbewertungen können für die betroffene Person deutlich empfindlicher sein als eine geschäftliche E-Mail-Adresse.

Die Auskunft muss daher so konkret sein, dass die betroffene Person versteht, welche Daten betroffen sind. Es reicht nicht aus, nur allgemein mitzuteilen, dass „personenbezogene Daten“ verarbeitet werden. Gleichzeitig müssen die Daten sinnvoll strukturiert werden, damit die Auskunft lesbar und verständlich bleibt.

6.9.4 Empfänger oder Kategorien von Empfängern

Art. 15 Abs. 1 lit. c) DSGVO:
„die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen“

Bedeutung:

Die betroffene Person muss erfahren, an wen ihre personenbezogenen Daten weitergegeben wurden oder künftig weitergegeben werden können. Empfänger können sowohl externe Stellen als auch interne Stellen sein, soweit sie Zugriff auf die Daten erhalten oder Daten übermittelt wurden. Beispiele sind IT-Dienstleister, Steuerberater, Zahlungsdienstleister, Versanddienstleister, Hosting-Anbieter, Behörden, Rechtsanwälte, Versicherungen, verbundene Unternehmen oder Geschäftspartner.

Diese Information ist für die betroffene Person wichtig, weil sie wissen muss, wer außer uns Zugang zu ihren Daten hat. Datenschutz betrifft nicht nur die Speicherung bei uns, sondern

Für die betroffene Person bedeutet das: Sie erhält grundsätzlich Auskunft über ihre eigenen personenbezogenen Daten, aber nicht automatisch uneingeschränkten Zugriff auf Informationen über andere Personen. Der Datenschutz schützt also nicht nur die anfragende Person, sondern auch alle anderen Personen, die in den Unterlagen vorkommen.

Für uns ist diese Prüfung besonders wichtig. Eine ungeschwärzte Herausgabe kann dazu führen, dass personenbezogene Daten Dritter offengelegt werden. Das kann selbst einen Datenschutzverstoß darstellen. Deshalb müssen Dokumente, E-Mails und Auszüge vor der Herausgabe sorgfältig geprüft werden.

7 Musterschreiben

Hinweis: Platzhalter sind in eckigen Klammern markiert.

7.1 Eingangsbestätigung

Betreff: Ihre Auskunftsanfrage nach Art. 15 DSGVO – [Vorgangsnummer]

Sehr geehrter/geehrte [Name],

wir bestätigen den Eingang Ihrer Auskunftsanfrage am [Datum]. Wir bearbeiten Ihr Anliegen fristgemäß und planen die Antwort bis spätestens [Fristdatum]. Falls wir für die Bearbeitung einen Identitätsnachweis oder eine Eingrenzung des Umfangs benötigen, melden wir uns bei Ihnen.

Für Rückfragen stehen wir Ihnen jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen

7.5 Erteilung der Auskunft

Betreff: Ihre Auskunft nach Art. 15 DSGVO – [Vorgangsnummer]

Sehr geehrter/geehrte [Name],

wir nehmen Bezug auf Ihre Auskunftsanfrage gemäß Art. 15 DSGVO vom [Datum].

Zur Erledigung Ihrer Anfrage haben wir die gewünschten Informationen [sowie die Kopie Ihrer Daten] in der Anlage beigefügt.

Nach sorgfältiger Prüfung gehen wir davon aus, dass die erteilte Auskunft vollständig ist. Sollten aus Ihrer Sicht dennoch Fragen offen geblieben sein oder weiterer Klärungsbedarf bestehen, können Sie sich selbstverständlich jederzeit an uns wenden.

Mit freundlichen Grüßen

7.6 Negativauskunft

Betreff: Ergebnis Ihrer Auskunftsanfrage – [Vorgangsnummer]

Sehr geehrter/geehrte [Name],

wir nehmen Bezug auf Ihre Auskunftsanfrage gemäß Art. 15 DSGVO vom [Datum] sowie unsere Eingangsbestätigung vom [Datum].

Nach Prüfung unserer Systeme und Unterlagen konnten wir zu den von Ihnen angegebenen Identifikationsmerkmalen keine personenbezogenen Daten finden, die wir außerhalb der Bearbeitung Ihrer Anfrage aktuell verarbeiten. Das bedeutet: Uns liegen derzeit keine weiteren personenbezogenen Daten zu Ihrer Person vor, zu denen wir Ihnen im Rahmen von Art. 15 DSGVO Auskunft erteilen könnten.

Unabhängig davon verarbeiten wir nun personenbezogene Daten aus Ihrer Anfrage und dieser Korrespondenz, um Ihr Auskunftsersuchen zu bearbeiten, [die Identität zu prüfen] und die Bearbeitung zu dokumentieren. Hierzu erhalten Sie in der Anlage die Informationen nach Art. 15 DSGVO bezogen auf diese Verarbeitung.

Falls Sie davon ausgehen, dass wir dennoch weitere Daten zu Ihrer Person verarbeiten, kann es helfen, wenn Sie uns zusätzliche Angaben zur eindeutigen Zuordnung nennen (z. B. weitere E-Mail-Adresse, frühere Anschrift, Kundennummer, Bestellnummer, Zeitraum). Dann prüfen wir dies gerne erneut.

Für weitere Rückfragen stehen wir Ihnen jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen

8 Versionierung und Pflege

8.1 Handbuch

Das Handbuch wird jährlich durch den unternehmensweiten Datenschutzkoordinator überprüft. Änderungen in der Organisationsstruktur oder der Rechtslage werden zeitnah eingearbeitet.

Für jede Fassung gibt es eine Versionsnummer, ein Änderungsprotokoll und eine Freigabe durch den Datenschutzbeauftragten. Veraltete Fassungen werden archiviert und sind als solche kenntlich.

8.2 Datenlandkarten

Der Datenschutzkoordinator des Fachbereichs ist für die laufende Aktualisierung der Datenlandkarte zuständig. Für jede Fassung gibt es eine Versionsnummer, ein Änderungsprotokoll und eine Freigabe durch den Fachbereichsleiter. Veraltete Fassungen werden archiviert und sind als solche kenntlich.

Dokumenteneigenschaften

Erstellt von…	Datum

Freigegeben von…	Datum

Geändert von…	Datum	Änderung	Version