Ordivis

MODUL · DATENSCHUTZ

Modul Datenschutz (Verarbeitungsverzeichnis)

Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO), Meldewesen und behördenkonformer Export

Produktversion 2026.08.19 · Handbuch-Revision 1.0
Stand 19.08.2026 · Plattform .NET 10 / Windows Server

ID-32 Datenschutz

Modul Datenschutz (Verarbeitungsverzeichnis)

Wer personenbezogene Daten verarbeitet, muss darüber ein **Verzeichnis von Verarbeitungstätigkeiten** führen – so verlangt es Artikel 30 der Datenschutz-Grundverordnung. Die Aufsichtsbehörde kann es jederzeit anfordern. In der Praxis liegt dieses Verzeichnis oft in einer Tabelle: Niemand weiß, wer sie zuletzt geändert hat, die Fachbereiche melden nichts nach, und in der Prüfung fehlt die Hälfte der Pflichtangaben.

Das Modul **Datenschutz** führt dieses Verzeichnis im Produkt – mit drei Eigenschaften, die eine Tabelle nicht hat: Jede Änderung ist **nachweisbar**, **Lücken werden sichtbar** statt erst in der Prüfung, und die Fachbereiche können ihre Verarbeitungen **selbst melden**, ohne Datenschutz-Vorwissen.

> **Abgrenzung:** Nicht zu verwechseln mit der Selbstauskunft *„Was verarbeitet Ordivis Platform selbst?"* – die steht unverändert unter *Datenschutz → Verarbeitungsverzeichnis (Produkt)* und beschreibt die Software. Dieses Modul führt **Ihr eigenes** Verzeichnis über **Ihre** Verarbeitungen.

INHALT

1 Zweck & Nutzen

- Verzeichnis nach Art. 30 DSGVO im Produkt führen, statt in einer Tabelle.
- **Revisionssicherer Nachweis** je Verfahren: wer, wann, welches Feld, von welchem Wert auf welchen.
- **Unvollständige Verfahren werden angezeigt** – nicht erst von der Aufsichtsbehörde gefunden.
- Meldewesen für Datenschutzverletzungen mit **72-Stunden-Frist** (Art. 33/34).
- **Behördenkonformer Export** auf Knopfdruck (PDF, CSV, JSON).
- Dezentrale Meldung durch Fachbereiche über das Portal.

2 Rollen und Rechte

Rolle	Recht	Sieht / darf
Fachbereich	`datenschutz.vvt.read` + `datenschutz.vvt.edit`	**nur die eigenen** Verfahren; anlegen, ändern, zur Prüfung geben
Betriebsrat / Leserecht	`datenschutz.vvt.read` + `datenschutz.vvt.read.all`	das **gesamte** Verzeichnis, nur lesend
Datenschutzbeauftragte(r)	zusätzlich `datenschutz.vvt.approve`, `datenschutz.catalog.manage`, `datenschutz.vvt.export`, `datenschutz.breach.*`	alles: freigeben, Kataloge pflegen, exportieren, Verletzungen bearbeiten

Die Einschränkung auf „eigene Verfahren" wirkt **serverseitig**: Ohne `datenschutz.vvt.read.all` sind fremde Verfahren weder in der Liste noch über einen Direktaufruf erreichbar. Wer Verfahren erfasst, kann sie **nicht selbst freigeben** – dafür braucht es das eigene Recht `datenschutz.vvt.approve` (Vier-Augen-Prinzip).

> Das Modul lässt sich vom Plattform-Administrator ein- und ausschalten (*Modul-Schalter*: `datenschutz`). Ist es aus, erscheint der Menüpunkt nicht.

3 Die DSB-Zentrale (Client)

Datenschutz → Verarbeitungsverzeichnis zeigt alle Verfahren mit Zweck, Fachbereich, Status und der nächsten Wiedervorlage – filter-, sortier- und exportierbar wie alle Tabellen im Client.

Zwei Dinge hebt die Liste bewusst hervor:

- **Spalte „Befunde"** – was einem Verfahren zu Art. 30 Abs. 1 fehlt: keine Rechtsgrundlage, keine Betroffenen-/Datenkategorien, keine Empfängerkategorien, keine Aufbewahrungsfrist, oder ein Empfänger im Drittland ohne belegte Garantie. Der Filter **„Nur mit Befunden"** macht daraus die Arbeitsliste. Die Banner oben zählen über den **gesamten** Bestand – sie verschwinden nicht, wenn Sie filtern.
- **Wiedervorlage** – ein freigegebenes Verfahren wird nach dem eingestellten Turnus fällig. Das Verzeichnis soll den *aktuellen* Stand abbilden, nicht den von vor drei Jahren.

4 Ein Verfahren bearbeiten (360°-Profil)

Ein Doppelklick öffnet das Verfahren als **360°-Profil** mit den Registern **Stammdaten**, **DSGVO-Metadaten**, **Systeme**, **DSFA**, **Freigabe** und **Nachweis**:

Stammdaten – Bezeichnung, Zweck (beides Pflicht nach Art. 30 Abs. 1 lit. b), Beschreibung, Fachbereich, Zielgruppenprofil (KMU / Enterprise / Öffentliche Verwaltung) und der Überprüfungsturnus. Es gibt **genau**

eine Schaltfläche *Speichern*, und sie schreibt ausschließlich diese Stammdaten.

Das **Zielgruppenprofil** steuert dabei mehr als eine Bezeichnung: Es legt fest, wie viele **Freigabe-Stufen** ein Verfahren durchläuft (Abschnitt 4.7), welche Spezialgesetze angeboten werden und ob der Betriebsrat mitbestimmt. Ein Panel unter dem Feld zeigt an, was das gewählte Profil konkret vorsieht.

DSGVO-Metadaten – die Pflichtangaben:

- **Rechtsgrundlagen (Art. 6 Abs. 1)** – die Buchstaben stehen im Klartext dabei (lit. a Einwilligung, lit. b Vertrag, …), damit die Zuordnung ohne Übersetzungstabelle prüfbar ist. Optional ergänzt um ein Spezialgesetz (BDSG, LDSG, Betriebs- oder Konzernvereinbarung) mit Fundstelle. Bei **berechtigtem Interesse (lit. f)** verlangt das Modul die **Interessenabwägung** – ohne sie ist die Grundlage nicht belastbar, und das Verfahren wird als Befund ausgewiesen.
- **Betroffene & Datenkategorien (Art. 30 Abs. 1 lit. c)** – hier wird verknüpft, *welche* Daten über *welche* Personengruppe verarbeitet werden. Diese Verbindung ist die eigentliche Aussage: „Wir verarbeiten Gesundheitsdaten" und „wir verarbeiten Daten von Bewerbern" ergibt zusammen noch nicht „Gesundheitsdaten **von Bewerbern**".
- **Aufbewahrung & Löschung (Art. 30 Abs. 1 lit. f)** – eine Frist besteht aus **Dauer + Auslöser**, nicht aus einem Datum: „6 Jahre" ist ohne „ab wann" wertlos. Wählbar sind ab Erhebung, ab Vertragsende, ab Jahresende, ab Zweckfortfall oder ab Widerruf; danach löschen, anonymisieren oder sperren. Fristen lassen sich je Datenkategorie festlegen – Bewerbungsunterlagen sechs Monate, die Buchungsbelege dazu zehn Jahre.
- **Empfänger & Drittland (Art. 30 Abs. 1 lit. d/e)** – siehe Abschnitt 4.4.

4.4 Empfänger & Drittland

> 💻 **Client:** *Datenschutz* ▸ *Verarbeitungsverzeichnis*, Verfahren öffnen · 🌐 **Portal:** *Mein Arbeitsplatz* ▸ *Datenschutz-Zentrale* · 🔑 `datenschutz.vvt.edit`

🔒 **Pflichtreihenfolge** — die **Rolle** des Empfängers entscheidet über die Pflichten, das **Sitzland** über die Garantie. Tragen Sie beide ein, bevor Sie die Fundstelle suchen: Bei einem Empfänger in der EU/im EWR brauchen Sie gar keine.

1. Öffnen Sie das Verfahren und wechseln Sie zu den Empfängern.
2. Tragen Sie die **Kategorie** ein (z. B. „Steuerberater“). Sie ist Pflicht.
3. Ergänzen Sie bei Bedarf den **Namen** des Empfängers – die Aufsicht fragt gern danach.
4. Wählen Sie die **Rolle**: *Auftragsverarbeiter* (Art. 28) oder *eigenverantwortlicher Dritter*.
5. Tragen Sie das **Sitzland** ein.
6. Liegt der Empfänger im **Drittland**, hinterlegen Sie die **Garantie** samt Fundstelle.

✅ **Ergebnis:** Der Befund *„Keine Empfängerkategorien erfasst"* verschwindet, und der behördenkonforme Export (Abschnitt 7) weist die Übermittlung vollständig aus.

Artikel 30 verlangt die **Kategorien von Empfängern** – nicht zwingend die Namen. „Steuerberater" genügt; „Musterkanzlei GmbH" dürfen Sie zusätzlich hinterlegen und die Aufsicht fragt gern danach. **Die Kategorie**

ist Pflicht. Auch „Wir geben nichts weiter" ist eine Angabe – ein leeres Feld ist dagegen keine, und das Verfahren trägt dann den Befund *„Keine Empfängerkategorien erfasst"*.

Zu jedem Empfänger gehört die **Rolle**, denn sie entscheidet über die Pflichten: Ein *Auftragsverarbeiter* (Art. 28) handelt weisungsgebunden und braucht einen Vertrag; ein *eigenverantwortlicher Dritter* – etwa Ihr Steuerberater – braucht eine **eigene** Rechtsgrundlage. Eine Schwesterfirma ist datenschutzrechtlich ebenfalls ein Dritter: Ein Konzernprivileg kennt die DSGVO nicht.

Sitzland und Garantie. Ordivis Platform entscheidet automatisch nur eine Frage: EU/EWR oder Drittland. Das folgt aus den Verträgen und ändert sich nicht. Liegt der Empfänger außerhalb, verlangt Kapitel V eine Garantie – Angemessenheitsbeschluss (Art. 45), Standardvertragsklauseln (Art. 46), Binding Corporate Rules (Art. 47) oder eine Ausnahme im Einzelfall (Art. 49). Fehlt sie, ist die Übermittlung unzulässig, und das Verfahren wird als Befund ausgewiesen. Tragen Sie die **Fundstelle** ein (SCC-Modul mit Datum, Zertifikatsnummer) – eine Garantie ohne Beleg ist eine Behauptung.

> **Vereinigte Staaten:** „Angemessenheitsbeschluss" allein reicht nicht. Der Beschluss gilt nicht dem Land, sondern nur Empfängern, die unter dem **Data Privacy Framework zertifiziert** sind. Ordivis Platform verlangt deshalb den Zertifizierungsnachweis; ohne ihn brauchen Sie Standardvertragsklauseln.

Warum Ordivis Ihnen nicht widerspricht: Angemessenheitsbeschlüsse werden erlassen – und wieder gekippt (das Privacy Shield fiel 2020). Eine im Programm hinterlegte Länderliste ist ab dem Tag ihrer Auslieferung möglicherweise veraltet, und eine veraltete Liste, die stillschweigend „zulässig" sagt, wäre gefährlicher als gar keine. Geben Sie einen Angemessenheitsbeschluss für ein Land an, das unser Stand nicht kennt, erhalten Sie deshalb einen **Hinweis mit Datum** – keinen Widerspruch. Die Entscheidung bleibt bei Ihnen.

4.5 Verarbeitende Systeme (Register „Systeme")

Welche IT-Systeme verarbeiten in diesem Verfahren personenbezogene Daten? Das Register **Systeme** verknüpft das Verfahren mit den zugehörigen **CI aus der CMDB** – der Name wird stets aktuell aufgelöst, nie abgeschrieben. Zu jedem System zeigt Ordivis Platform den **Schutzbedarf aus dem Informationssicherheits-Modul** (read-only), sodass Datenschutz und Informationssicherheit dieselbe Wahrheit sehen.

Werden **besonders schutzwürdige Daten** (Art. 9/10) in einem Verfahren auf einem System verarbeitet, für das **kein hoher Schutzbedarf** festgestellt ist, warnt das Register vor dem **„ungeschützten Datenstrom"**. Das ist kein Fehler des Verfahrens, sondern ein Prüfhinweis: Entweder ist der Schutzbedarf im ISMS zu niedrig angesetzt, oder das System ist für diese Daten nicht geeignet.

4.6 Datenschutz-Folgenabschätzung (Register „DSFA")

Artikel 35 verlangt eine **Datenschutz-Folgenabschätzung**, wenn eine Verarbeitung *voraussichtlich ein hohes Risiko* birgt. Das Register **DSFA** führt die **Schwellenwertanalyse** anhand der Muss-Kriterien (Art. 35 Abs. 3 und der Liste der Aufsichtsbehörden – Profiling, umfangreiche besondere Kategorien, systematische Überwachung, neue Technologien, Datenabgleich, schutzbedürftige Betroffene) und lässt Sie das **Restrisiko** aus Eintrittswahrscheinlichkeit × Schadensausmaß (je 1–3) einschätzen.

Das Ergebnis ist eine **Ampel**: „nicht bewertet" (grau), grün, gelb (Prüfung ratsam) oder rot (DSFA-Pflicht). **Ein nicht bewertetes Verfahren bleibt bewusst grau** – die Ampel darf nie fälschlich „unbedenklich" suggerieren, nur weil noch niemand hingesehen hat. Die DSFA-Pflicht ist ein **Prüfhinweis, keine Rechtsberatung**: eine konservative Heuristik (≥ 2 Muss-Kriterien oder hohes Restrisiko).

4.7 Mehrstufige Freigabe (Register „Freigabe")

Der Freigabe-Workflow richtet sich nach dem **Zielgruppenprofil** des Verfahrens:

Profil	Freigabe-Stufen
KMU	direkt der/die Datenschutzbeauftragte
Unternehmen	Fachbereich → Risikomanagement → Datenschutzbeauftragte(r)
Öffentliche Verwaltung	Fachbereich → Betriebsrat → Datenschutzbeauftragte(r)

Beim *Zur Prüfung geben* werden die Stufen erzeugt und der Reihe nach entschieden. **Jede Freigabe oder Ablehnung trägt eine elektronische Signatur** – einen manipulationssicheren Hash aus Entscheider, Zeitpunkt und Votum, der zusammen mit dem Vorgang im revisionssicheren Nachweis landet. Die **letzte** Stufe gibt das Verfahren frei; eine Ablehnung wirft es auf *Entwurf* zurück. Die Stufen bleiben als Nachweis stehen.

Nachweis – jede Änderung als Gegenüberstellung *alt* → *neu*, mit Benutzer und Zeitpunkt. Die Einträge sind unveränderbar und lassen sich nicht löschen; sie überleben sogar das Löschen des Verfahrens. Wer ein Verfahren entfernt, tilgt damit nicht den Nachweis, dass es existierte (Art. 5 Abs. 2).

4.8 Technisch-organisatorische Maßnahmen (Register „TOM")

Nach **Art. 30 Abs. 1 lit. g DSGVO** gehört eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (TOM) in das Verzeichnis. Im Register **„TOM"** verknüpfen Sie die für das Verfahren getroffenen Maßnahmen aus einem **Katalog** (z. B. Zutritts-, Zugangs- und Zugriffskontrolle, Verschlüsselung, Pseudonymisierung, Verfügbarkeit, Auftrags- und Trennungskontrolle). Der Katalog wird mit Standard-TOMs ausgeliefert und lässt sich je Mandant erweitern. Die verknüpften Maßnahmen erscheinen im behördenkonformen Export (Abschnitt 7).

Lebenszyklus

Entwurf → *Zur Prüfung* → *Freigegeben*. Die Freigabe setzt zugleich die nächste Wiedervorlage. **Eine inhaltliche Änderung an einem freigegebenen Verfahren setzt die Freigabe zurück** – sonst zeigte das Verzeichnis einen freigegebenen Stand, den nie jemand freigegeben hat.

5 Kataloge (Betroffene und Datenkategorien)

Kategorien werden **zentral gepflegt** statt je Verfahren frei eingetippt – sonst stünden „Beschäftigte", „Mitarbeiter" und „Angestellte" nebeneinander, und der Export zeigte drei Gruppen, wo es eine gibt.

Ordivis Platform liefert den **gesetzlichen Grundkatalog** mit, weil er Gesetzestext und keine Konfiguration ist: die **besonderen Kategorien nach Art. 9 Abs. 1** vollständig (Gesundheit, Religion, Gewerkschaft,

Biometrie, …), die **strafrechtlichen Daten nach Art. 10** getrennt davon, dazu die gängigen Betroffenengruppen. Diese Einträge sind änderbar, aber **nicht löschbar**; ebenso wenig lassen sich Kategorien löschen, die noch in einem Verfahren verwendet werden.

> **Art.-9-Daten** brauchen **zusätzlich** zur Art.-6-Grundlage einen Erlaubnistatbestand nach Art. 9 Abs. 2. Ordivis Platform trägt ihn bewusst **nicht** vor: Er hängt am Verfahren, nicht an der Kategorie – eine Vorbelegung wäre eine Rechtsbehauptung. Solange er fehlt, weist der Export ihn als Befund aus.

6 Meldewesen: Datenschutzverletzungen (Art. 33/34)

Datenschutz → Datenpannen. Die Liste zeigt als Erstes die **Restzeit** – denn Artikel 33 gibt Ihnen **72 Stunden**.

Die Frist läuft ab dem Bekanntwerden beim Verantwortlichen – nicht ab dem Vorfall und nicht ab der Erfassung im System. Ein Vorfall von vor zehn Tagen, der Ihnen vor einer Stunde bekannt wurde, hat noch 71 Stunden. Das Erfassungsformular führt diese drei Zeitpunkte deshalb getrennt.

Der Ablauf: **erfassen** (das darf jeder mit dem Melderecht – eine Meldepflicht, die am Recht scheitert, ist keine) → **bewerten** → **melden** → **abschließen**.

- **Bewertung**: kein Risiko / Risiko (Meldung an die Aufsichtsbehörde) / hohes Risiko (zusätzlich Benachrichtigung der Betroffenen nach Art. 34).
- **„Nicht meldepflichtig" verlangt eine Begründung.** Artikel 33 Abs. 5 verlangt die Dokumentation **aller** Verletzungen, auch der nicht gemeldeten – ohne Begründung ist die Entscheidung gegenüber der Behörde nicht haltbar.
- **Abschließen ist gesperrt**, solange eine Pflicht offen ist: meldepflichtig und nicht gemeldet, oder hohes Risiko ohne Benachrichtigung der Betroffenen. Eine offene Pflicht verschwindet nicht durch einen Klick.
- Die Überfällig-Markierung verschwindet **nicht durch Zeitablauf**, sondern erst durch die Meldung – eine verspätete Meldung ist weiterhin zu erstatten.

Jede Verletzung erhält ein fortlaufendes Aktenzeichen (`DSV-JJJJ-NNNN`), auf das die Aufsichtsbehörde sich beziehen kann.

7 Behördenkonformer Export (Art. 30 Abs. 4)

> 🌐 **Nur im Portal:** *Mein Arbeitsplatz ▸ Datenschutz-Zentrale ▸ Behördenkonformer Export* · 🔑 `datenschutz.vvt.approve` — Im Client führen Sie das Verzeichnis unter *Datenschutz ▸ Verarbeitungsverzeichnis*; der behördenkonforme Export liegt in der Zentrale des Portals.

1. Öffnen Sie *Mein Arbeitsplatz ▸ Datenschutz-Zentrale*.
2. Klicken Sie auf *Behördenkonformer Export*.
3. Wählen Sie das Format: **PDF** (Prüfunterlage), **CSV** (Weiterverarbeitung) oder **JSON** (maschinenlesbar).
4. Erzeugen Sie den Export und speichern Sie ihn ab.

✅ **Ergebnis:** Sie erhalten das Verzeichnis mit Ihrem Mandanten als Verantwortlichem im Briefkopf – und mit den offenen Befunden ausgewiesen.

Der Export weist die Befunde mit aus. Das ist Absicht: Ein Export, der Lücken kaschiert, hilft in der Prüfung niemandem – die Behörde findet sie ohnehin, nur später und schlechter erklärt. Ausgewiesen werden unter anderem berechtigtes Interesse ohne Abwägung, Art.-9-Kategorien ohne Erlaubnistatbestand, Empfänger im Drittland ohne belegte Garantie sowie Verfahren ohne Rechtsgrundlage, ohne Empfängerkategorien, ohne Frist oder ohne Freigabe.

> **Was der Export abdeckt:** Artikel 30 Absatz 1 Buchstabe a bis f. Die allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Buchstabe g) ist noch nicht enthalten; das Gesetz formuliert sie mit „wenn möglich", die Vorlage scheitert daran nicht. Ergänzen Sie sie bis dahin im Anschreiben.

8 Fachbereiche melden selbst (Portal)

> 🌐 **Nur im Portal:** *Mein Arbeitsplatz ▸ Verarbeitung melden* · 🔑 `datenschutz.vvt.edit` — Der Client hat keinen Melde-Assistenten; dort führt der DSB das Verzeichnis unmittelbar.

Ein Datenschutzbeauftragter kann nicht alle Verarbeitungen eines Hauses allein kennen. Ein **Assistent** führt die Fachbereiche in fünf Schritten durch die Meldung – in Alltagssprache, ohne Datenschutz-Vorwissen:

🔒 **Pflichtreihenfolge** — der Assistent lässt Sie nicht weiter, solange eine Angabe fehlt, die er selbst abfragt. Das ist Absicht: Er soll keine halben Meldungen erzeugen.

1. **Worum geht es?** (Bezeichnung, Zweck in eigenen Worten)
2. **Wessen Daten verarbeiten Sie?**
3. **Welche Daten verarbeiten Sie?** – besonders schutzwürdige Daten sind gekennzeichnet
4. **Warum dürfen Sie das?** – bei „berechtigtem Interesse" wird direkt nach der Abwägung gefragt
5. **Wie lange behalten Sie die Daten?**

✅ **Ergebnis:** Die Meldung geht als **Entwurf zur Prüfung an den Datenschutzbeauftragten**; der Fachbereich gibt **nicht** selbst frei. Den eigenen Stand sehen die Meldenden danach unter *Mein Arbeitsplatz ▸ Meine Verfahren*.

> **Was der Assistent bewusst nicht fragt:** die **Empfänger** (Abschnitt 4.4). Ob eine Weitergabe an einen Auftragsverarbeiter, einen eigenverantwortlichen Dritten oder eine Behörde geht – und welche Garantie ein Drittland trägt – ist eine rechtliche Einordnung, keine Frage an den Fachbereich. Der DSB ergänzt sie bei der Prüfung; bis dahin trägt das Verfahren den Befund „keine Empfängerkategorien". Das ist gewollt: Der Entwurf sieht dann unfertig aus, weil er es ist.

Der Stand der eigenen Meldungen ist im Portal unter *Compliance & Sicherheit → Meine Verfahren* einsehbar: Der Fachbereich sieht seine gemeldeten Verarbeitungen mit Status (in Prüfung, freigegeben)

und dem Hinweis „Angaben unvollständig", solange eine Pflichtangabe fehlt – aber **nur die eigenen**, nie fremde Verfahren, und ohne die Möglichkeit zur Freigabe (die bleibt der DSB-Zentrale vorbehalten).

9 Grenzen (Stand dieser Fassung)

Neu in dieser Fassung enthalten: die **Schwellenwertanalyse und Datenschutz-Folgenabschätzung** (Art. 35, Abschnitt 4.6), die **Verknüpfung mit CMDB-Systemen** samt Schutzbedarf (Abschnitt 4.5), der **mehrstufige, elektronisch signierte Freigabe-Workflow** (Abschnitt 4.7), der **Katalog technischer und organisatorischer Maßnahmen** (Art. 30 Abs. 1 lit. g, Abschnitt 4.8) sowie das **DSB-Lagebild** mit Kennzahl-Kacheln in der Zentrale.

Bewusst noch **nicht** vollständig im Produkt und für spätere Fassungen vorgesehen: Verträge zur Auftragsverarbeitung (Art. 28) sind auf API-Ebene angelegt, aber noch ohne eigene Oberfläche; die Verknüpfung der Verfahren mit **Geschäftsprozessen** fehlt noch.

> Das Modul ersetzt keine datenschutzrechtliche Beratung. Es führt das Verzeichnis, weist Lücken aus und belegt Änderungen – die fachliche Bewertung bleibt bei Ihrem Datenschutzbeauftragten.

Verwandte Themen

- **ID-28 – Modul Informationssicherheit (ISMS)** – technische und organisatorische Maßnahmen im ISMS
- **ID-21 – Modul CMDB** – die Systeme hinter einer Verarbeitungstätigkeit
- **ID-10 – Benutzerhandbuch – Self-Service-Portal** – Betroffenenrechte aus Sicht der Benutzer
- **ID-44 – Rollen- & Rechte-Matrix** – Rechte für Einsicht und Pflege