



audatis MANAGER

Compliance + ISMS-Erweiterung

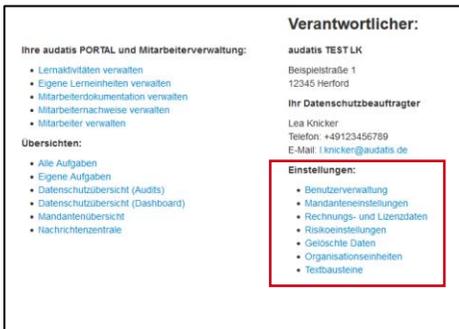
Agenda

1. **Allgemeine Änderungen im audatis MANAGER**
2. **Vorbereitungen**
3. **Compliance-Register**
4. **KI-Compliance**
5. **Geschäftsprozesse**
6. **Ereignisse und Sicherheitsvorfälle**
7. **Risikomanagement**
8. **ISMS-Compliance**

Allgemeine Änderungen im audatis MANAGER

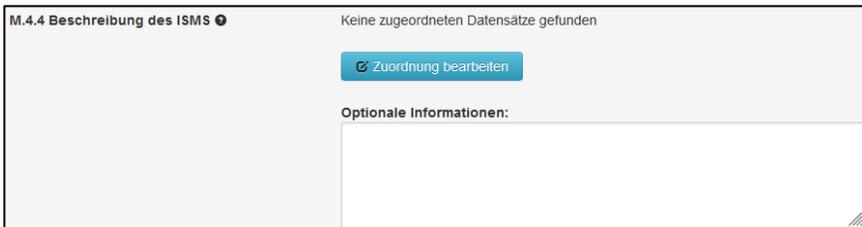
Änderungen vorab

- Das bisher bekannte Risikomanagement-Modul, in welchem bisher die Risikomatrix für eine DSFA und eine Verarbeitungstätigkeit angelegt wird, heißt nun „Risikoeinstellungen“.
- Die Einstellungen befinden sich nun rechts unter den Informationen des Datenschutzbeauftragten:



The screenshot shows a user interface with two columns. The left column contains navigation links under 'Ihre audatis PORTAL und Mitarbeiterverwaltung:' and 'Übersichten:'. The right column contains contact information for the 'Verantwortlicher:' and 'Ihr Datenschutzbeauftragter:'. A red box highlights the 'Einstellungen:' menu in the right column, which includes: Benutzerverwaltung, Mandanteneinstellungen, Rechnungs- und Lizenzdaten, Risikoeinstellungen, Gelöschte Daten, Organisationseinheiten, and Textbausteine.

- Sofern das Paket erworben wurde, gibt es in den technischen und organisatorischen Maßnahmen nun ein zusätzliches Feld:



The screenshot shows a form field titled 'M.4.4 Beschreibung des ISMS'. The field is currently empty and contains the text 'Keine zugeordneten Datensätze gefunden'. Below the field is a blue button labeled 'Zuordnung bearbeiten' and a section for 'Optionale Informationen:' with an empty text area.

Vorbereitungen

1. Bestellung auslösen

Der Systemadministrator eines Mandanten kann entweder in den „Rechnungs- und Lizenzdaten“ im Hauptmandanten über den Reiter „Umfang erweitern“ oder in den „Lizenzdaten“ eines Untermantanten die Bestellung des Compliance + ISMS Erweiterungs-Pakets durchführen:

Compliance + ISMS Erweiterung bestellen: Ja, hiermit bestätige ich die kostenpflichtige Bestellung der Compliance + ISMS Erweiterung für monatlich 29,00 EUR (netto) für diesen Mandanten.

Compliance + ISMS Erweiterung kostenpflichtig bestellen

Das Paket beinhaltet 10 zusätzliche Benutzer und 6 neue Module.

2. Risikoeinstellung für ISMS und KI anlegen

Es muss je eine Risikoeinstellung für ISMS und KI existieren und aktiviert sein, um in den neuen Modulen damit arbeiten zu können. Dies kann in den „Risikoeinstellungen“ erfolgen, in welcher die Einträge für beide Typen angelegt werden müssen:

- Einstellungen:**
- Benutzerverwaltung
 - Mandanteneinstellungen
 - Rechnungs- und Lizenzdaten
 - Risikoeinstellungen
 - Gelöschte Daten
 - Organisationseinheiten
 - Textbausteine

Bezeichnung	Typ	Aktiv
Risikomanagement (KI)	Risikomanagement (KI)	Ja
Risikomanagement (ISMS)	Risikomanagement (ISMS)	Ja

Compliance-Register

Compliance-Register

Dieses neue Modul dient als internes „Rechtskataster“, um alle Gesetze und anderen Compliance-Anforderungen, welche für Ihr Unternehmen gelten, zu dokumentieren, im Blick zu behalten und entsprechend umsetzen zu können. Bisher haben Sie dies vielleicht in einer Word-Datei oder Excel-Liste dokumentiert und können nun stattdessen dieses Modul mit Erinnerungsfunktion nutzen.

1. Neuen Eintrag anlegen

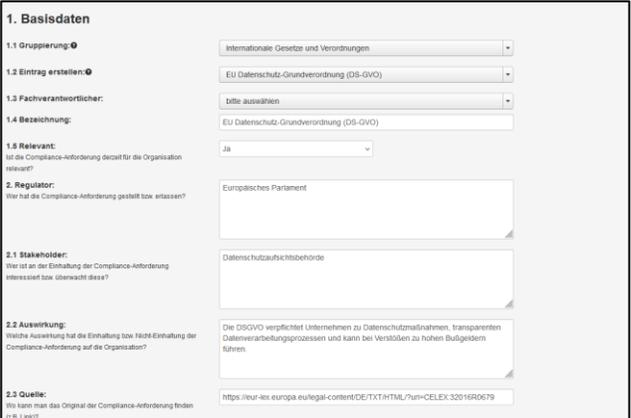
Als erstes muss eine Gruppierung ausgewählt werden. Anschließend kann ein eigener Eintrag erstellt oder eine „Vorlage“ ausgewählt werden (bspw. DS-GVO). Im Falle einer Vorlage werden die Felder automatisch ausgefüllt.

2. Alle Punkte (falls gewünscht) anpassen

3. Prüfung

Sobald ein Datensatz Ihren Anforderungen entspricht, kann dieser wie bisher zur Prüfung freigegeben werden. Die Prüfung bedeutet in diesem Fall die Überprüfung des Gesetzes auf die Relevanz oder schon berücksichtigten Anforderungen. Dabei muss womöglich die Quelle überprüft werden. Hier kann auch eine erneute Prüfung festgelegt werden (bspw. nach einem Jahr), um zu kontrollieren, ob der angelegte Datensatz noch aktuell ist.

4. Export → CSV-Datei



1. Basisdaten

1.1 Gruppierung: Internationale Gesetze und Verordnungen

1.2 Eintrag erstellen: EU Datenschutz-Grundverordnung (DS-GVO)

1.3 Fachverantwortlicher: bitte auswählen

1.4 Bezeichnung: EU Datenschutz-Grundverordnung (DS-GVO)

1.9 Relevant: Ist die Compliance-Anforderung relevant für die Organisation relevant? Ja

2. Regulator: Wie hat die Compliance-Anforderung gestellt bzw. erlassen? Europäisches Parlament

2.1 Stakeholder: Wem ist die Einhaltung der Compliance-Anforderung interessiert bzw. überwacht diese? Datenschutzaufsichtsbehörde

2.2 Auswirkung: Welche Auswirkung hat die Einhaltung bzw. Nicht-Einhaltung der Compliance-Anforderung auf die Organisation? Die DSGVO verpflichtet Unternehmen zu Datenschutzmaßnahmen, transparenten Datenverarbeitungsprozessen und kann bei Verstößen zu hohen Bußgeldern führen.

2.3 Quelle: Wo kann man das Original der Compliance-Anforderung finden (z.B. Link)? <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679>

KI-Compliance

KI-Compliance

Dieses neue Modul dient dazu die Anforderungen und Pflichten aus der EU KI-Verordnung an KI-Systeme zu ermitteln und deren Umsetzung zu dokumentieren.

1. Anwendung anlegen

Im Modul „Daten- und IT-Inventarisierung“ können nun Anwendungen als „KI-System“ angelegt bzw. markiert werden. Dies muss als erster Schritt erfolgen.

Durch das Setzen des Hakens wird an dieser Stelle nach den KI-Systemen gefiltert.



2. Neue KI-Compliance anlegen

Dabei gilt herauszufinden: wie konform sind meine KI-Anwendungen? Sie können pro Datensatz eine Risikoklasse auswählen, die Rolle(n) Ihrer Organisation in Bezug auf die KI-Systeme auswählen und verschiedene IT-Anwendungen mit einbeziehen.



Bezeichnung	Beschreibung	Mandantenübergreifend	KI-System	Verknüpft	Aktion
<input type="checkbox"/> ChatGPT		<input type="checkbox"/>	<input checked="" type="checkbox"/> Minimales Risiko		   

3. Beschreibung und Pflichten ausfüllen

4. Datensatz zur Prüfung einreichen

Geschäftsprozesse

Dieses Modul gleicht dem bereits existierenden „Verzeichnis der Verarbeitungstätigkeiten“ und ist mit diesem auch verknüpft. So wird jede angelegte Verarbeitungstätigkeit auch automatisch im Modul „Geschäftsprozesse“ als Datensatz angelegt. Dieser Datensatz wird in beiden Modulen angezeigt, solange dieser als Prozess mit personenbezogenen Daten definiert ist. Ohne personenbezogene Daten verschwindet der Datensatz aus dem „Verzeichnis der Verarbeitungstätigkeiten“.

Somit können jetzt auch Geschäftsprozesse ohne Personenbezug verwaltet werden bspw. Produktionsprozess mit vertraulichen Informationen, welche für das ISMS relevant sind.

1. Neuen Geschäftsprozess anlegen und Typ bestimmen

2. Ausfüllen des Datensatzes

Bei einem Datensatz ohne personenbezogenen Daten sind beim Ausfüllen des Geschäftsprozesses weniger Felder auszufüllen als bei den Verarbeitungstätigkeiten, da in einem Geschäftsprozess nicht alle aus der DS-GVO relevanten Angaben abgefragt werden müssen. Dabei werden die identischen Felder jedoch in beiden Modulen synchronisiert.

3. Prüfung

Ereignisse und Sicherheitsvorfälle

Ereignisse und Sicherheitsvorfälle

Dieses neue Modul ist eine Vorstufe für das bereits bekannte Modul „Datenschutz- und Sicherheitsvorfälle“. Hier werden also erst einmal Ereignisse gemeldet, welche dann nach einer Evaluation eventuell als Datenschutz- und Sicherheitsvorfall weiterbearbeitet werden.

1. Ereignis wird gemeldet

2. Bearbeitung des Datensatzes

3. Prüfung

Bei der Prüfung können betroffene Anwendung aus den Geschäftsprozessen ausgewählt werden. In der Prüfung muss ansonsten eine Risikobewertung durchgeführt werden und am Ende entschieden werden, ob es sich um einen Datenschutz- und Sicherheitsvorfall handelt und dieser weiterbehandelt werden muss.

Übergabe für weitere Schritte

Es liegt vermutlich ein Datenschutz- und Sicherheitsvorfall vor, welcher weiter behandelt und geprüft werden muss.

→ In diesem Fall wird automatisch ein Datensatz im Modul „Datenschutz- und Sicherheitsvorfälle“ angelegt. Anschließend müssen beide Datensätze in den beiden Modulen separat behandelt werden. (Bspw. Kann der Datensatz in „Ereignisse und Sicherheitsvorfälle“ auf „abgeschlossen“ gesetzt werden, da alles Notwendige in diesem Modul getan wurde.)

Risikomanagement

Risikomanagement

Das neue „Risikomanagement“ und das Modul „Datenschutz-Folgenabschätzung“ sind sich sehr ähnlich. Dieses Modul soll zur Risikobeurteilung und Risikobehandlung im ISMS genutzt werden (bspw. Ereignis und Sicherheitsvorfälle oder auch Ergebnisse aus Audits und anderen Risikoeingaben).

1. Risikomanagement anlegen

2. Ursprung festlegen und mit Datensatz verknüpfen

Es können bestehende Datensätze verknüpft werden (aus den Geschäftsprozessen oder den Ereignissen), oder auch eigene Ursprünge (bspw. Audits) hinzugefügt werden.

3. Risiken definieren

Hier müssen eventuell eintretende Risiken genannt und beurteilt werden. Dazu können unter dem Reiter „Risiko“ Risikobeurteilungen angelegt und ausgefüllt werden. Hier wird die Risikomatrix, welche zu Beginn in den Risikoeinstellungen angelegt wurde, verwendet.

4. Risikobehandlung

Hier können die zuvor festgelegten Risiken behandelt werden, wobei nach eventuell eingeführten Maßnahmen eine Risikoanalyse erneut durchgeführt werden kann. Dadurch lässt sich in der Risikobeurteilung das Risiko reduzieren.

5. Prüfung

Bei der Prüfung in diesem Modul handelt es sich um eine Akzeptanzbewertung des Risikos.

ISMS-Compliance

ISMS-Compliance

Das Modul „ISMS-Compliance“ dient, ähnlich wie die „Datenschutzgrundsätze“, als Dokumentation und Nachweis, dass ein Unternehmen ein ISMS führt und stellt die Umsetzung von Anforderungskatalogen (z.B. dem Standard des VDA ISA) dar.

1. Neuen Anforderungskatalog erfassen

2. Datensätze verknüpfen

Es können im Reiter „Compliance“ in den verschiedenen Abschnitten auch technische und organisatorische Maßnahmen verknüpft werden, womit ausgewählt wird mithilfe welcher Maßnahmen jener Abschnitt umgesetzt wird.

3. Umsetzungsstand anpassen (Prozentzahl)

4. Kapitel hinzufügen, wenn gewünscht

5. Prozentzahl in der Übersicht passt sich entsprechend aus allen Abschnitten an

Vielen Dank

www.audatis.de



audatis Group auf XING



audatis Group auf LinkedIn



audatis Dialog auf YouTube



audatis Group auf Facebook

