

DIN EN 17926

ICS 35.030

Einsprüche bis 2023-03-06

Entwurf**Datenschutz-Informationssystem per ISO/IEC 27701 –
Verfeinerungen im europäischen Kontext;
Deutsche und Englische Fassung prEN 17926:2022**

Privacy Information Management System per ISO/IEC 27701 –
Refinements in European context;
German and English version prEN 17926:2022

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2023-01-06 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin oder Am DIN-Platz, Burggrafenstr. 6, 10787 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 77 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (prEN 17926:2022) wurde vom Technischen Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ erarbeitet, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige nationale Normungsgremium ist der Gemeinschaftsarbeitsausschuss NA 043-04-13 GA „DIN/DKE Gemeinschaftsgremium Cybersecurity“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

Für die in diesem Dokument zitierten Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO/IEC 17021 (alle Teile)	siehe	DIN EN ISO/IEC 17021 (alle Teile)
ISO/IEC 17065	siehe	DIN EN ISO/IEC 17065

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO/IEC 17065, *Konformitätsbewertung — Anforderungen an Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren*

DIN EN ISO/IEC 17021 (alle Teile), *Konformitätsbewertung — Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren*

– *Entwurf* –

E DIN EN 17926:2023-02

– Leerseite –

November 2022

prEN 17926

**Datenschutz-Informationssystem per ISO/IEC 27701 – Verfeinerungen
im europäischen Kontext**

Privacy Information Management System per ISO/IEC 27701 – Refinements in European context

Inhalt

	Seite
Europäisches Vorwort	3
Einleitung	4
1 Anwendungsbereich	5
2 Normative Verweisungen	5
3 Begriffe	5
4 Aufbau dieses Dokuments	5
5 Datenschutz-Informationsmanagementsystem für Verarbeitungsvorgänge von personenbezogenen Daten	6
6 Anforderung für Verarbeitungsvorgänge personenbezogener Daten	6
Anhang A (normativ) Informationssicherheit und Steuerungsmaßnahmen für den <i>Datenschutz</i> .	7
Anhang B (normativ) PIMS-spezifische Referenzmaßnahmenziele und -Maßnahmen (verantwortliche Stellen)	19
Anhang C (normativ) PIMS-spezifische Referenzmaßnahmenziele und -Maßnahmen (Auftragsdatenverarbeiter)	26
Anhang D (informativ) Modell für die Kombination einer Managementsystemzertifizierung nach den Zertifizierungsanforderungen in ISO/IEC 17021 mit einer immateriellen produktbezogenen Zertifizierung nach den Zertifizierungsanforderungen in ISO/IEC 17065	29
D.1 Einleitung	29
D.2 Zusammenhang zwischen ISO/IEC 17021 und ISO/IEC 17065	29
D.3 Möglichkeit von Zertifizierungsprogrammen nach ISO/IEC 17067 für immaterielle Produkte, Prozesse und Dienstleistungen, die den Betrieb eines Managementsystems erfordern	29
Anhang E (informativ) Zusammenhang zwischen dieser Europäischen Norm und der Datenschutz-Grundverordnung	31
Literaturhinweise	36

Bilder

Bild D.1 — Gemeinsames Zertifizierungsmodell nach den Anforderungen von ISO/IEC 17065 und ISO/IEC 17021	30
--	----

Tabellen

Tabelle A.1 — Maßnahmenziele und Maßnahmen	7
Tabelle B.1 — Maßnahmenziele und Maßnahmen	19
Tabelle C.1 — Maßnahmenziele und Maßnahmen	26
Tabelle E.1 — Zuordnung der DSGVO-Artikel zu diesem Dokument	31

Europäisches Vorwort

Dieses Dokument (prEN 17926:2022) wurde vom Technischen Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ erarbeitet, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Einleitung

EN ISO/IEC 27701 legt Anforderungen fest und bietet Leitlinien für die Einführung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines Datenschutz-Informationsmanagementsystems (PIMS, en: Privacy Information Management System), das in jedem Rechtssystem implementiert werden kann. Da es sich um ein Managementsystem für den internationalen Gebrauch handelt, sind die Anforderungen allgemein gehalten, und die Leitlinien können von den Organisationen je nach ihrem Kontext und ihren geltenden Verpflichtungen angepasst werden.

Obwohl EN ISO/IEC 27701 mit der Absicht geschrieben wurde, in jedem Rechtssystem anwendbar zu sein, einschließlich der EU-Datenschutz-Grundverordnung (DSGVO) (ISO/IEC 27701, Anhang D, enthält eine Zuordnung zwischen den Abschnitten der Norm und der DSGVO), liegt es in der Verantwortung der Organisation, zu bestimmen, wie die Anforderungen und Maßnahmen von EN ISO/IEC 27701 im Kontext der DSGVO implementiert werden sollen.

Dieses Dokument enthält Verfeinerungen von EN ISO/IEC 27701 bei der Anwendung von Maßnahmen und Leitlinien in EN ISO/IEC 27701 speziell für die DSGVO, wo dies erforderlich ist. Dieses Dokument ist für dieselben Entitäten wie in ISO/IEC 27701 anwendbar: alle Arten und Größen von Organisationen, einschließlich öffentlicher und privater Unternehmen, öffentlicher Stellen und gemeinnütziger Organisationen, die verantwortlichen Stellen und/oder Auftragsdatenverarbeiter im Rahmen eines ISMS (Informationssicherheitsmanagementsystem) sind. Dies soll von Organisationen im Zusammenhang mit der DSGVO verwendet werden, um die Einhaltung ihrer Verpflichtungen nachzuweisen. EN ISO/IEC 27701 in Verbindung mit den Verfeinerungen dieses Dokuments stellt eine Reihe von Anforderungen dar, die spezifischer gestaltet und besser für den Kontext der DSGVO geeignet sind als die allgemeinen Anforderungen von EN ISO/IEC 27701 allein.

Somit kann EN ISO/IEC 27701 als internationales Rahmenwerk betrachtet werden, das für einen bestimmten regionalen Kontext (im Fall dieses Dokuments die Datenschutz-Grundverordnung) verfeinert und sogar um Anforderungen ergänzt werden kann, die für ein bestimmtes Rechtssystem/Land oder eine bestimmte Branche geeignet sind (fällt nicht in den Anwendungsbereich dieses Dokuments).

Die in diesem Dokument festgelegten Verfeinerungen von EN ISO/IEC 27701 für Verarbeitungsvorgänge als Teil von Produkten, Prozessen und Dienstleistungen können für die Konformitätsbewertung verwendet werden, die entweder von Erst-, Zweit- oder Drittparteien durchgeführt werden kann. Insbesondere können Zertifizierungsstellen diese Anforderungen und Verfeinerungen nutzen, um die Konformität sowohl eines Datenschutz-Informationsmanagementsystems nach ISO/IEC 17021 als auch der Verarbeitungsvorgänge eines Produkts, Prozesses oder einer Dienstleistung nach ISO/IEC 17065 zu beurteilen. Zertifizierungsprogramme für Produkte, die personenbezogene Daten verarbeiten, können auf dieses Dokument verweisen, wie in ISO/IEC 17067 für Programmtyp 6 beschrieben.

ANMERKUNG „Produkt“ kann als „Prozess“ oder „Dienstleistung“ verstanden werden (ISO/IEC 17065, Abschnitt 1 und Anhang B).

Die Anforderungen in diesem Dokument können Teil eines Programms sein, das sowohl unter ISO/IEC 17065 für die Anforderungen an Produkte, die Auftragsdatenverarbeitungsaufgaben beinhalten („Produktanforderungen“ nach ISO/IEC 17065, 3.8) als auch unter ISO/IEC 17021 für die Anforderungen an das Managementsystem (ISO/IEC 17067 Programmtyp 6) geregelt ist.

Artikel 42 der DSGVO fördert die Einführung von datenschutzspezifischen Zertifizierungsverfahren. Die Bestimmungen dieses Dokuments können von den zuständigen Stellen zur Festlegung von datenschutzspezifischen Zertifizierungsmechanismen gemäß Artikel 42 der DSGVO verwendet werden, um die Konformität der Verarbeitungsvorgänge im PIMS nach ISO/IEC 17065 zu beurteilen, einschließlich der Beurteilung der systematischen Elemente des Datenschutz-Informationsmanagementsystems nach ISO/IEC 17067, Abschnitt 6.

1 Anwendungsbereich

Dieses Dokument legt Verfeinerungen für eine Anwendung von EN ISO/IEC 27701 in einem europäischen Kontext fest.

Dieses Dokument ist für dieselben Entitäten wie in ISO/IEC 27701 anwendbar: alle Arten und Größen von Organisationen, einschließlich öffentlicher und privater Unternehmen, öffentlicher Stellen und gemeinnütziger Organisationen, die verantwortliche Stellen und/oder Auftragsdatenverarbeiter im Rahmen eines ISMS (Informationssicherheitsmanagementsystem) sind.

Eine Organisation kann dieses Dokument für die Umsetzung der allgemeinen Anforderungen und Maßnahmen von EN ISO/IEC 27701 je nach ihrem Kontext und ihren geltenden Verpflichtungen verwenden.

Zertifizierungskriterien, die auf diesen Verfeinerungen basieren, können ein Zertifizierungsmodell nach ISO/IEC 17065 für Verarbeitungsvorgänge bereitstellen, die im Rahmen eines Datenschutz-Informationssicherheitsmanagementsystems nach EN ISO/IEC 27701 durchgeführt werden, das mit Zertifizierungsanforderungen für EN ISO/IEC 27701 nach ISO/IEC 17021 kombiniert werden kann.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

EN ISO/IEC 27701:2021, *Sicherheitstechniken — Erweiterung zu ISO/IEC 27001 und ISO/IEC 27002 für das Management von Informationen zum Datenschutz — Anforderungen und Leitlinien*

EN ISO/IEC 27001:2017, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Anforderungen (ISO/IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2:2015)*

3 Begriffe

In diesem Dokument werden keine Begriffe aufgeführt.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: verfügbar unter <https://www.electropedia.org/>
- ISO Online Browsing Platform: verfügbar unter <https://www.iso.org/obp>

4 Aufbau dieses Dokuments

Abschnitt 5 bezieht sich auf das in EN ISO/IEC 27701 definierte Datenschutz-Informationssicherheitsmanagementsystem und legt zusätzliche Anforderungen und Verfeinerungen der Anforderungen fest.

Abschnitt 6 legt die Anforderungen für die Verarbeitungsvorgänge von personenbezogenen Daten als Teil von Produkten, Prozessen oder Dienstleistungen fest; dabei handelt es sich um Anforderungen an die Organisation zur Durchführung spezifischer Maßnahmen aus Anhang A, Anhang B, Anhang C und den zugehörigen Leitlinien.

Anhang A bezieht sich auf die in ISO/IEC 27001, Anhang A, festgelegten Maßnahmen.

Anhang B bezieht sich auf die in EN ISO/IEC 27701, Anhang A, festgelegten Maßnahmen für verantwortliche Stellen.

Anhang C bezieht sich auf die in EN ISO/IEC 27701, Anhang B, festgelegten Maßnahmen für Auftragsdatenverarbeiter.

Der informative Anhang D enthält ein Modell für die Kombination von Zertifizierungen nach ISO/IEC 17021 und ISO/IEC 17065. Schließlich wird in Anhang E der Zusammenhang zwischen diesem Dokument und der Datenschutz-Grundverordnung (EU 2016/679) dargestellt.

5 Datenschutz-Informationssystem für Verarbeitungsvorgänge von personenbezogenen Daten

Die Organisation muss ein PIMS nach EN ISO/IEC 27701 einführen, umsetzen, aufrechterhalten und fortlaufend verbessern.

Die Organisation muss die Verarbeitungsvorgänge von personenbezogenen Daten im Rahmen des Managementsystems festlegen (EN ISO/IEC 27701, 5.2.3).

EN ISO/IEC 27701:2021, 5.2.3, wird wie folgt verfeinert:

Bei der Festlegung dieses Anwendungsbereichs muss die Organisation Schnittstellen und Abhängigkeiten zwischen Auftragsdatenverarbeitungsaufgaben innerhalb und außerhalb der Organisation berücksichtigen.

EN ISO/IEC 27001:2013, 6.1.3 c), wird wie folgt verfeinert:

Die in ISO/IEC 27001:2013, 6.1.3 b) festgelegten Maßnahmen müssen mit den Maßnahmen in Anhang A, Anhang B und/oder Anhang C verglichen werden, um zu überprüfen, dass keine notwendigen Maßnahmen ausgelassen wurden.

Bei der Beurteilung der Anwendbarkeit der Maßnahmenziele und Maßnahmen aus Anhang A für die Behandlung von Risiken müssen die Maßnahmenziele und Maßnahmen sowohl im Zusammenhang mit Risiken für die Informationssicherheit als auch mit Risiken im Zusammenhang mit der Verarbeitung personenbezogener Daten, einschließlich Risiken für betroffene Personen, berücksichtigt werden.

EN ISO/IEC 27001:2013, 6.1.3 d), wird wie folgt verfeinert:

Erstellung einer Erklärung zur Anwendbarkeit, die Folgendes enthält:

- die notwendigen Maßnahmen [siehe ISO/IEC 27001:2013, 6.1.3 b) und c) als Verfeinerung von Cove];
- Begründung für ihre Aufnahme;
- ob die notwendigen Maßnahmen umgesetzt sind oder nicht; und
- die Begründung für den Ausschluss einer der Maßnahmen in Anhang A und in Anhang B und/oder Anhang C entsprechend der Bestimmung der Rolle der Organisation (siehe EN ISO/IEC 27701, 5.2.1).

In Anhang A, Anhang B und Anhang C wird festgelegt, welche Maßnahmen die Organisation in Abhängigkeit ihrer Rolle durchführen muss. Daher können diese Maßnahmen nicht ausgeschlossen werden.

6 Anforderung für Verarbeitungsvorgänge personenbezogener Daten

Für alle Verarbeitungsvorgänge personenbezogener Daten nach Abschnitt 5 muss die Organisation die in Anhang A, Anhang B oder Anhang C geforderten Maßnahmen durchführen, je nach Rolle der Organisation (siehe ISO/IEC 27701, 5.2.1).

Anhang A (normativ)

Informationssicherheit und Steuerungsmaßnahmen für den *Datenschutz*

Dieser Anhang ist zur Verwendung durch alle Organisationen bestimmt, unabhängig von ihrer Rolle (als verantwortliche Stelle, als Auftragsdatenverarbeiter oder beides). Dieser Anhang listet alle Maßnahmen aus ISO/IEC 27001:2013, Anhang A, auf und gibt an, wo Erweiterungen zu diesen Maßnahmen in ISO/IEC 27701 enthalten sind und wo Verfeinerungen im europäischen Kontext anwendbar sind.

In Tabelle A.1 gibt es zwei Arten von Verweisungen auf Maßnahmen nach ISO/IEC 27001:2013:

- Verweisungen auf Maßnahmen nach ISO/IEC 27001:2013 in der Form „Die Maßnahme ISO/IEC 27001:2013 [Maßnahmennummer A.x.y.z] gilt.“ bedeuten, dass die Organisation die Anwendbarkeit der Maßnahme entsprechend ihrer Risikobewertung (EN ISO/IEC 27701, 5.4.1.2) und Risikobehandlung (EN ISO/IEC 27701, 5.4.1.3) berücksichtigen muss;
- Anforderungen in der Form „Die Organisation muss die Maßnahme ISO/IEC 27001:2013 [Maßnahmennummer A.x.y.z] unter Beachtung der zusätzlichen Leitlinien in ... umsetzen“ bedeuten, dass die Organisation alle diese Maßnahmen unter Beachtung der entsprechenden Leitlinien umsetzen muss, um die allgemeinen Anforderungen in Abschnitt 6 zu erfüllen (in allen Fällen, unabhängig von der Risikobewertung und der Risikobehandlung im Managementsystem). Einige Maßnahmen dieser Art umfassen zusätzliche Verfeinerungen der Leitlinien von EN ISO/IEC 27701 in Übereinstimmung mit dem Anwendungsbereich dieses Dokuments.

ANMERKUNG Die Abschnittsnummern in diesem Anhang beziehen sich auf die Unterabschnittsnummern in ISO/IEC 27001:2013, Anhang A.

Tabelle A.1 — Maßnahmenziele und Maßnahmen

A.5 Informationssicherheitsrichtlinien		
A.5.1 Vorgaben der Leitung für Informationssicherheit		
Ziel: Bereitstellung von Vorgaben der Leitung und Unterstützung für die Informationssicherheit und den Datenschutz in Übereinstimmung mit den geschäftlichen Anforderungen und den einschlägigen Gesetzen und Vorschriften.		
A.5.1.1	Richtlinien für die Informationssicherheit	Die Organisation muss die Maßnahme ISO/IEC 27001 A.5.1.1 umsetzen und dabei die zusätzlichen Leitlinien in EN ISO/IEC 27701, 6.2.1.1, beachten.
A.5.1.2	Überprüfung der Informationssicherheitsrichtlinien	Die Maßnahme ISO/IEC 27001 A.5.1.2 gilt.
A.6 Organisation der Informationssicherheit		
A.6.1 Interne Organisation		
Ziel: Einführung eines Managementrahmenwerks, um die Umsetzung und den Betrieb von Informationssicherheit und Datenschutz innerhalb der Organisation zu initiieren und zu steuern.		

Tabelle A.1 (fortgesetzt)

A.6.1.1	Informationssicherheitsrollen und -verantwortlichkeiten	Die Organisation muss die ISO/IEC 27001 A.6.1.1 umsetzen und dabei die zusätzlichen Leitlinien in EN ISO/IEC 27701, 6.3.1.1, und diese zusätzlichen Verfeinerungen beachten: — Die Organisation muss einen Datenschutzbeauftragten (DSB) als Verantwortlichen entsprechend EN ISO/IEC 27701:2021, 6.3.1.1 benennen, wenn die Art, der Anwendungsbereich und die Zwecke der Verarbeitung dies nach den geltenden Verpflichtungen erfordern. — Die Organisation muss sicherstellen, dass der DSB über ausreichende Ressourcen zur Erfüllung seiner Aufgaben verfügt, der höchsten Führungsebene unterstellt ist, in alle Fragen des Schutzes personenbezogener Daten einbezogen wird und dass die Kontaktdaten des DSB veröffentlicht und der Aufsichtsbehörde und den betroffenen Personen mitgeteilt werden. — Die Organisation muss sicherstellen, dass der Datenschutzbeauftragte keine Anweisungen für die Ausübung dieser Aufgaben erhält.
A.6.1.2	Aufgabentrennung	Die Organisation muss die Maßnahme ISO/IEC 27001 A.6.1.2 umsetzen.
A.6.1.3	Kontakt zu Behörden	Die Maßnahme ISO/IEC 27001 A.6.1.3 gilt.
A.6.1.4	Kontakt zu speziellen Interessengruppen	Die Maßnahme ISO/IEC 27001 A.6.1.4 gilt.
A.6.1.5	Informationssicherheit im Projektmanagement	Die Maßnahme ISO/IEC 27001 A.6.1.5 gilt.
A.6.2 Mobilgeräte und Telearbeit		
Ziel: Sicherstellung der Sicherheit und des Datenschutzes bei der Telearbeit und der Nutzung von Mobilgeräten		
A.6.2.1	Richtlinie zu Mobilgeräten	Die Organisation muss die Maßnahme ISO/IEC 27001 A.6.2.1 umsetzen und dabei die zusätzlichen Leitlinien in EN ISO/IEC 27701, 6.3.2.1, beachten.
A.6.2.2	Telearbeit	Die Maßnahme ISO/IEC 27001 A.6.2.2 gilt.
A.7 Personalsicherheit		
A.7.1 Vor Beginn eines Anstellungsverhältnisses		
Ziel: Sicherstellung, dass Mitarbeiter und Auftragnehmer ihre Verantwortung verstehen und für die Aufgaben, für die sie in Frage kommen, geeignet sind.		
A.7.1.1	Sicherheitsüberprüfung	Die Maßnahme ISO/IEC 27001 A.7.1.1 gilt.
A.7.1.2	Beschäftigungs- und Vertragsbedingungen	Die Maßnahme ISO/IEC 27001 A.7.1.2 gilt.
A.7.2 Während des Anstellungsverhältnisses		

Tabelle A.1 (fortgesetzt)

Ziel: Sicherstellung, dass sich Mitarbeiter und Auftragnehmer ihrer Verantwortung für die Informationssicherheit und den Datenschutz bewusst sind und diese erfüllen.		
A.7.2.1	Verantwortlichkeiten des Managements	Die Maßnahme ISO/IEC 27001 A.7.2.1 gilt.
A.7.2.2	Informationssicherheitsbewusstsein, -ausbildung und -schulung	Die Organisation muss die Maßnahme ISO/IEC 27001 A.7.2.2 umsetzen und dabei die zusätzlichen Leitlinien in EN ISO/IEC 27701, 6.4.2.2 beachten.
A.7.2.3	Maßregelungsprozess	Die Maßnahme ISO/IEC 27001 A.7.2.3 gilt.
A.7.3 Beendigung und Änderung des Anstellungsverhältnisses		
Ziel: Schutz der Interessen der Organisation als Teil des Prozesses der Änderung oder Beendigung einer Beschäftigung.		
A.7.3.1	Verantwortlichkeiten bei Beendigung oder Änderung des Anstellungsverhältnisses	Die Maßnahme ISO/IEC 27001 A.7.3.1 gilt.
A.8 Verwaltung der Werte		
A.8.1 Verantwortlichkeit für Werte		
Ziel: Identifizierung von Unternehmensressourcen und Festlegung entsprechender Schutzverantwortlichkeiten.		
A.8.1.1	Inventarisierung der Werte	Die Maßnahme ISO/IEC 27001 A.8.1.1 gilt.
A.8.1.2	Zuständigkeit für Werte	Die Maßnahme ISO/IEC 27001 A.8.1.2 gilt.
A.8.1.3	Zulässiger Gebrauch von Werten	Die Maßnahme ISO/IEC 27001 A.8.1.3 gilt.
A.8.1.4	Rückgabe von Werten	Die Maßnahme ISO/IEC 27001 A.8.1.4 gilt.
A.8.2 Informationsklassifizierung		
Ziel: Sicherstellung, dass die Informationen entsprechend ihrer Bedeutung für die Organisation angemessen geschützt werden.		
A.8.2.1	Klassifizierung von Informationen	Die Organisation muss die Maßnahme ISO/IEC 27001 A.8.2.1 umsetzen und dabei die zusätzlichen Leitlinien in EN ISO/IEC 27701, 6.5.2.1, beachten.
A.8.2.2	Kennzeichnung von Informationen	Die Organisation muss die Maßnahme ISO/IEC 27001 A.8.2.2 umsetzen und dabei die zusätzlichen Leitlinien in EN ISO/IEC 27701, 6.5.2.2, beachten.
A.8.2.3	Handhabung von Werten	Die Maßnahme ISO/IEC 27001 A.8.2.3 gilt.
A.8.3 Handhabung von Datenträgern		
Ziel: Verhinderung der unbefugten Offenlegung, Änderung, Entfernung oder Zerstörung von auf Datenträgern gespeicherten Informationen.		
A.8.3.1	Handhabung von Wechseldatenträgern	Die Organisation muss die Maßnahme ISO/IEC 27001 A.8.3.1 und dabei die zusätzlichen Leitlinien in EN ISO/IEC 27701, 6.5.3.1, umsetzen.

Tabelle A.1 (fortgesetzt)

A.8.3.2	Entsorgung von Datenträgern	Die Organisation muss die Maßnahme ISO/IEC 27001 A.8.3.2 umsetzen und dabei die zusätzlichen Leitlinien in EN ISO/IEC 27701, 6.5.3.2, beachten.
A.8.3.3	Übertragung von physischen Datenträgern	Die Organisation muss die Maßnahme ISO/IEC 27001 A.8.3.3 und dabei die zusätzlichen Leitlinien in EN ISO/IEC 27701, 6.5.3.3, umsetzen.
A.9 Zugangssteuerung		
A.9.1 Geschäftsanforderungen an die Zugangsteuerung		
Ziel: Begrenzung des Zugangs zu Informationen und informationsverarbeitenden Einrichtungen.		
A.9.1.1	Zugangssteuerungsrichtlinie	Die Organisation muss die Maßnahme ISO/IEC 27001 A.9.1.1 umsetzen.
A.9.1.2	Zugang zu Netzwerken und Netzwerkdiensten	Die Maßnahme ISO/IEC 27001 A.9.1.2 gilt.
A.9.2 Benutzerzugangsverwaltung		
Ziel: Sicherstellung des befugten Benutzerzugangs und Verhinderung des unbefugten Zugangs auf Systeme und Dienste.		
A.9.2.1	Registrierung und Registrierungsaufhebung von Benutzern	Die Organisation muss die Maßnahme ISO/IEC 27001 A.9.2.1 umsetzen und dabei die zusätzlichen Leitlinien in EN ISO/IEC 27701, 6.6.2.1, beachten.
A.9.2.2	Zuteilung von Benutzerzugängen	Die Organisation muss die Maßnahme ISO/IEC 27001 A.9.2.2 umsetzen und dabei die zusätzlichen Leitlinien in EN ISO/IEC 27701, 6.6.2.2, beachten.
A.9.2.3	Verwaltung privilegierter Zugangsrechte	Die Organisation muss die Maßnahme ISO/IEC 27001 A.9.2.3 umsetzen.
A.9.2.4	Verwaltung geheimer Authentisierungsinformationen von Benutzern	Die Maßnahme ISO/IEC 27001 A.9.2.4 gilt.
A.9.2.5	Überprüfung von Benutzerzugangsrechten	Die Organisation muss die Maßnahme ISO/IEC 27001 A.9.2.5 umsetzen.
A.9.2.6	Entzug oder Anpassung von Zugangsrechten	Die Organisation muss die Maßnahme ISO/IEC 27001 A.9.2.6 umsetzen.
A.9.3 Benutzerverantwortlichkeiten		
Ziel: Die Benutzer sollen für den Schutz ihrer Authentifizierungsdaten verantwortlich sein.		
A.9.3.1	Gebrauch geheimer Authentisierungsinformationen	Die Maßnahme ISO/IEC 27001 A.9.3.1 gilt.
A.9.4 System- und Anwendungsmaßnahme		
Ziel: Verhinderung des unbefugten Zugangs auf Systeme und Anwendungen.		
A.9.4.1	Informationszugangsbeschränkung	Die Organisation muss die Maßnahme ISO/IEC 27001 A.9.4.1 umsetzen.

Tabelle A.1 (fortgesetzt)

A.9.4.2	Sichere Anmeldeverfahren	Die Organisation muss die Maßnahme ISO/IEC 27001 A.9.4.2 umsetzen und dabei die zusätzlichen Leitlinien in EN ISO/IEC 27701, 6.6.2.2., beachten.
A.9.4.3	System zur Verwaltung von Kennwörtern	Die Maßnahme ISO/IEC 27001 A.9.4.3 gilt.
A.9.4.4	Gebrauch von Hilfsprogrammen mit privilegierten Rechten	Die Maßnahme ISO/IEC 27001 A.9.4.4 gilt.
A.9.4.5	Zugangssteuerung für Quellcode von Programmen	Die Maßnahme ISO/IEC 27001 A.9.4.5 gilt.
A.10 Kryptographie		
A.10.1 Kryptographische Maßnahmen		
Ziel: Sicherstellung des angemessenen und wirksamen Gebrauchs von Kryptographie zum Schutz der Vertraulichkeit, Authentizität und/oder Integrität von Informationen.		
A.10.1.1	Richtlinie zum Gebrauch von kryptographischen Maßnahmen	Die Organisation muss die Maßnahme ISO/IEC 27001 A.10.1.1 umsetzen und dabei die zusätzlichen Leitlinien in EN ISO/IEC 27701, 6.7.1.1, beachten.
A.10.1.2	Schlüsselverwaltung	Die Maßnahme ISO/IEC 27001 A.10.1.2 gilt.
A.11 Physische und umgebungsbezogene Sicherheit		
A.11.1 Sicherheitsbereiche		
Ziel: Verhinderung des unbefugten physischen Zugriffs, der Beschädigung und des Eingriffs in die Informationen der Organisation und informationsverarbeitenden Einrichtungen.		
A.11.1.1	Physische Sicherheitsperimeter	Die Maßnahme ISO/IEC 27001 A.11.1.1 gilt.
A.11.1.2	Physische Zutrittssteuerung	Die Maßnahme ISO/IEC 27001 A.11.1.2 gilt.
A.11.1.3	Sichern von Büros, Räumen und Einrichtungen	Die Maßnahme ISO/IEC 27001 A.11.1.3 gilt.
A.11.1.4	Schutz vor externen und umweltbedingten Bedrohungen	Die Maßnahme ISO/IEC 27001 A.11.1.4 gilt.
A.11.1.5	Arbeiten in Sicherheitsbereichen	Die Maßnahme ISO/IEC 27001 A.11.1.5 gilt.
A.11.1.6	Anlieferungs- und Ladebereiche	Die Maßnahme ISO/IEC 27001 A.11.1.6 gilt.
A.11.2 Einrichtung		
Ziel: Verlust, Beschädigung, Diebstahl oder Gefährdung von Vermögenswerten und die Unterbrechung von Organisationstätigkeiten sind unterbunden.		
A.11.2.1	Platzierung und Schutz der Einrichtung	Die Maßnahme ISO/IEC 27001 A.11.2.1 gilt.
A.11.2.2	Versorgungseinrichtungen	Die Maßnahme ISO/IEC 27001 A.11.2.2 gilt.

Tabelle A.1 (fortgesetzt)

A.11.2.3	Sicherheit der Verkabelung	Die Maßnahme ISO/IEC 27001 A.11.2.3 gilt.
A.11.2.4	Instandhaltung von Geräten und Betriebsmitteln	Die Maßnahme ISO/IEC 27001 A.11.2.4 gilt.
A.11.2.5	Entfernen von Werten	Die Maßnahme ISO/IEC 27001 A.11.2.5 gilt.
A.11.2.6	Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten	Die Maßnahme ISO/IEC 27001 A.11.2.6 gilt.
A.11.2.7	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln	Die Organisation muss die Maßnahme ISO/IEC 27001 A.11.2.7 umsetzen und dabei die zusätzlichen Leitlinien in EN ISO/IEC 27701, 6.8.2.7, beachten.
A.11.2.8	Unbeaufsichtigte Benutzergeräte	Die Maßnahme ISO/IEC 27001 A.11.2.8 gilt.
A.11.2.9	Richtlinie für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren	Die Organisation muss die Maßnahme ISO/IEC 27001 A.11.2.9 umsetzen und dabei die zusätzlichen Leitlinien in EN ISO/IEC 27701, 6.8.2.9, beachten.
A.12 Betriebssicherheit		
A.12.1 Betriebsabläufe und -verantwortlichkeiten		
Ziel: Der ordnungsgemäße und sichere Betrieb von informationsverarbeitenden Einrichtungen ist sichergestellt.		
A.12.1.1	Dokumentierte Betriebsabläufe	Die Maßnahme ISO/IEC 27001 A.12.1.1 gilt.
A.12.1.2	Änderungsmanagement	Die Maßnahme ISO/IEC 27001 A.12.1.2 gilt.
A.12.1.3	Kapazitätssteuerung	Die Maßnahme ISO/IEC 27001 A.12.1.3 gilt.
A.12.1.4	Trennung von Entwicklungs-, Prüf- und Betriebsumgebungen	Die Organisation muss die Maßnahme ISO/IEC 27001 A.12.1.4 umsetzen.
A.12.2 Schutz vor Schadsoftware		
Ziel: Sicherstellung des Schutzes von Informationen und informationsverarbeitenden Einrichtungen gegen Schadsoftware.		
A.12.2.1	Maßnahmen gegen Schadsoftware	Die Maßnahme ISO/IEC 27001 A.12.2.1 gilt.
A.12.3 Sicherung		
Ziel: Schutz vor Datenverlust.		
A.12.3.1	Sicherung von Informationen	Die Organisation muss die Maßnahme ISO/IEC 27001 A.12.3.1 umsetzen und dabei die zusätzlichen Leitlinien in EN ISO/IEC 27701, 6.7.1.1, beachten.
A.12.4 Protokollierung und Überwachung		
Ziel: Aufzeichnung von Ereignissen und Erbringung von Beweismitteln.		

Tabelle A.1 (fortgesetzt)

A.12.4.1	Ereignisprotokollierung	Die Organisation muss die Maßnahme ISO/IEC 27001 A.12.4.1 umsetzen und dabei die zusätzlichen Leitlinien in EN ISO/IEC 27701, 6.9.4.1, beachten.
A.12.4.2	Schutz der Protokollinformationen	Die Organisation muss die Maßnahme ISO/IEC 27001 A.12.4.2 umsetzen und dabei die zusätzlichen Leitlinien in EN ISO/IEC 27701, 6.9.4.2, beachten.
A.12.4.3	Administratoren- und Bedienerprotokolle	Die Maßnahme ISO/IEC 27001 A.12.4.3 gilt.
A.12.4.4	Uhrensynchronisation	Die Maßnahme ISO/IEC 27001 A.12.4.4 gilt.
A.12.5 Steuerung von Software im Betrieb		
Ziel: Die Integrität von Systemen im Betrieb ist sichergestellt.		
A.12.5.1	Installation von Software auf Systemen im Betrieb	Die Maßnahme ISO/IEC 27001 A.12.5.1 gilt.
A.12.6 Handhabung technischer Schwachstellen		
Ziel: Die Ausnutzung technischer Schwachstellen wird verhindert.		
A.12.6.1	Handhabung von technischen Schwachstellen	Die Maßnahme ISO/IEC 27001 A.12.6.1 gilt.
A.12.6.2	Einschränkungen von Softwareinstallation	Die Maßnahme ISO/IEC 27001 A.12.6.2 gilt.
A.12.7 Überlegungen für Audits von Informationssystemen		
Ziel: Die Auswirkung von Audittätigkeiten auf Systeme im Betrieb ist minimiert.		
A.12.7.1	Maßnahme für Audits von Informationssystemen	Die Maßnahme ISO/IEC 27001 A.12.7.1 gilt.
A.13 Kommunikationssicherheit		
A.13.1 Netzwerksicherheitsmanagement		
Ziel: Sicherstellung des Schutzes von Informationen in Netzwerken und den sie unterstützenden informationsverarbeitenden Einrichtungen.		
A.13.1.1	Netzwerksteuerungsmaßnahmen	Die Maßnahme ISO/IEC 27001 A.13.1.1 gilt.
A.13.1.2	Sicherheit von Netzwerkdiensten	Die Maßnahme ISO/IEC 27001 A.13.1.2 gilt.
A.13.1.3	Trennung in Netzwerken	Die Maßnahme ISO/IEC 27001 A.13.1.3 gilt.
A.13.2 Informationsübertragung		
Ziel: Aufrechterhaltung der Sicherheit von übertragenen Informationen, sowohl innerhalb einer Organisation als auch bei jeder externen Entität.		
A.13.2.1	Richtlinien und Verfahren für die Informationsübertragung	Die Organisation muss die Maßnahme ISO/IEC 27001 A.13.2.1 umsetzen und dabei die zusätzlichen Leitlinien in EN ISO/IEC 27701, 6.10.2.1, beachten.
A.13.2.2	Vereinbarungen zur Informationsübertragung	Die Maßnahme ISO/IEC 27001 A.13.2.2 gilt.

Tabelle A.1 (fortgesetzt)

A.13.2.3	Elektronische Nachrichtenübermittlung	Die Maßnahme ISO/IEC 27001 A.13.2.3 gilt.
A.13.2.4	Vertraulichkeits- oder Geheimhaltungsvereinbarungen	Die Organisation muss die Maßnahme ISO/IEC 27001 A.13.2.4 umsetzen und dabei die zusätzlichen Leitlinien in EN ISO/IEC 27701, 6.10.2.4, beachten.
A.14 Anschaffung, Entwicklung und Instandhaltung von Systemen		
A.14.1 Sicherheitsanforderungen an Informationssysteme		
Ziel: Sicherstellung, dass Informationssicherheit und Datenschutz über den gesamten Lebenszyklus hinweg ein integraler Bestandteil von Informationssystemen sind. Dazu gehören auch die Anforderungen an Informationssysteme, die Dienste über öffentliche Netze anbieten.		
A.14.1.1	Analyse und Spezifikation von Informationssicherheitsanforderungen	Die Maßnahme ISO/IEC 27001 A.14.1.1 gilt.
A.14.1.2	Sicherung von Anwendungsdiensten in öffentlichen Netzwerken	Die Organisation muss die Maßnahme ISO/IEC 27001 A.14.1.2 umsetzen und dabei die zusätzlichen Leitlinien in EN ISO/IEC 27701, 6.11.1.2, beachten.
A.14.1.3	Schutz der Transaktionen bei Anwendungsdiensten	Die Maßnahme ISO/IEC 27001 A.14.1.3 gilt.
A.14.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen		
Ziel: Sicherstellung, dass die Informationssicherheit und der Datenschutz im Rahmen des Entwicklungszyklus von Informationssystemen geplant und umgesetzt werden.		
A.14.2.1	Richtlinie für sichere Entwicklung	Die Organisation muss die Maßnahme ISO/IEC 27001 A.14.2.1 umsetzen und dabei die zusätzlichen Leitlinien in EN ISO/IEC 27701, 6.11.2.1, beachten.
A.14.2.2	Verfahren zur Verwaltung von Systemänderungen	Die Maßnahme ISO/IEC 27001 A.14.2.2 gilt.
A.14.2.3	Technische Überprüfung von Anwendungen nach Änderungen an der Betriebsplattform	Die Maßnahme ISO/IEC 27001 A.14.2.3 gilt.
A.14.2.4	Beschränkung von Änderungen an Softwarepaketen	Die Maßnahme ISO/IEC 27001 A.14.2.4 gilt.
A.14.2.5	Kurzbeschreibung der Analyse, Entwicklung und Pflege sicherer Systeme	Die Organisation muss die Maßnahme ISO/IEC 27001 A.14.2.5 umsetzen und dabei die zusätzlichen Leitlinien in EN ISO/IEC 27701, 6.11.2.5, beachten.
A.14.2.6	Sichere Entwicklungsumgebung	Die Maßnahme ISO/IEC 27001 A.14.2.6 gilt.
A.14.2.7	Ausgegliederte Entwicklung	Die Organisation muss die Maßnahme ISO/IEC 27001 A.14.2.7 umsetzen und dabei die zusätzlichen Leitlinien in EN ISO/IEC 27701, 6.11.2.7, beachten.

Tabelle A.1 (fortgesetzt)

A.14.2.8	Testen der Systemsicherheit	Die Maßnahme ISO/IEC 27001 A.14.2.8 gilt.
A.14.2.9	Systemabnahmetest	Die Maßnahme ISO/IEC 27001 A.14.2.9 gilt.
A.14.3 Testdaten		
Ziel: Sicherstellung des Schutzes der für die Prüfung verwendeten Daten.		
A.14.3.1	Schutz von Testdaten	Die Organisation muss die Maßnahme ISO/IEC 27001 A.14.3.1 umsetzen und dabei die zusätzlichen Leitlinien in EN ISO/IEC 27701, 6.11.3.1, beachten.
A.15 Lieferantenbeziehungen		
A.15.1 Informationssicherheit in Lieferantenbeziehungen		
Ziel: Sicherstellung des Schutzes der Werte der Organisation, die für Lieferanten zugänglich sind.		
A.15.1.1	Informationssicherheitsrichtlinie für Lieferantenbeziehungen	Die Organisation muss die Maßnahme ISO/IEC 27001 A.15.1.1 umsetzen.
A.15.1.2	Behandlung von Sicherheit in einem Lieferantenvertrag	Die Organisation muss die Maßnahme ISO/IEC 27001 A.15.1.2 umsetzen und dabei die zusätzlichen Leitlinien in EN ISO/IEC 27701, 6.12.1.2, beachten.
A.15.1.3	Lieferkette für Informations- und Kommunikationstechnologie	Die Organisation muss die Maßnahme ISO/IEC 27001 A.15.1.3 umsetzen.
A.15.2 Steuerung der Dienstleistungserbringung von Lieferanten		
Ziel: Eine vereinbarte Stufe der Informationssicherheit und des Datenschutzes sowie der Dienstleistungserbringung wird im Einklang mit Lieferantenverträgen aufrechterhalten.		
A.15.2.1	Überwachung und Überprüfung von Lieferantendienstleistungen	Die Organisation muss die Maßnahme ISO/IEC 27001 A.15.2.1 umsetzen.
A.15.2.2	Handhabung der Änderungen von Lieferantendienstleistungen	Die Organisation muss die Maßnahme ISO/IEC 27001 A.15.2.2 umsetzen.
A.16 Handhabung von Informationssicherheitsvorfällen		
A.16.1 Handhabung von Informationssicherheitsvorfällen und -verbesserungen		
Ziel: Sicherstellung eines konsistenten und effektiven Ansatzes für das Management von Vorfällen im Bereich der Informationssicherheit und des Datenschutzes, einschließlich der Kommunikation über Ereignisse und Schwachstellen im Bereich der Sicherheit und des Datenschutzes.		

Tabelle A.1 (fortgesetzt)

A.16.1.1	Verantwortlichkeiten und Verfahren	Die Organisation muss die Maßnahme ISO/IEC 27001 A.16.1.1 umsetzen und dabei die zusätzlichen Leitlinien in EN ISO/IEC 27701, 6.13.1.1, und diese zusätzlichen Verfeinerungen beachten: — Die Organisation muss Verantwortlichkeiten und Verfahren für das Management von Vorfällen im Bereich der Informationssicherheit und des Datenschutzes einführen, die Folgendes umfassen: — Kriterien für die Benachrichtigung der erforderlichen Parteien (Aufsichtsbehörde, Kunde, (gemeinsamer) Datenbeauftragter, betroffene Personen); — Zeitpunkt für die Mitteilungen; und — Mitteilungsinhalt. — Die Organisation muss die geltenden Mitteilungspflichten ermitteln und die Einhaltung dieser Pflichten dokumentieren (z. B. Mitteilung an die zuständige Aufsichtsbehörde ohne unangemessene Verzögerung, wenn möglich innerhalb von 72 Stunden nach Kenntnisnahme).
A.16.1.2	Meldung von Informationssicherheitsereignissen	Die Maßnahme ISO/IEC 27001 A.16.1.2 gilt.
A.16.1.3	Meldung von Schwächen in der Informationssicherheit	Die Maßnahme ISO/IEC 27001 A.16.1.3 gilt.
A.16.1.4	Beurteilung von und Entscheidung über Informationssicherheitsereignisse	Die Maßnahme ISO/IEC 27001 A.16.1.4 gilt.

Tabelle A.1 (fortgesetzt)

A.16.1.5	Reaktion auf Informationssicherheitsvorfälle	Die Organisation muss die Maßnahme ISO/IEC 27001 A.16.1.5 umsetzen und dabei die zusätzlichen Leitlinien in EN ISO/IEC 27701, 6.13.1.5, und diese zusätzlichen Verfeinerungen beachten: Verfeinerungen für verantwortliche Stellen: Die Organisation muss die geltenden Verpflichtungen in Bezug auf die Kriterien für Mitteilungen an die Aufsichtsbehörde und/oder an die betroffenen Personen ermitteln und die Einhaltung dieser Verpflichtungen dokumentieren (z. B. Kriterien in Bezug auf die Risiken für die betroffenen Personen). Mitteilungen müssen mindestens Folgendes enthalten: — eine Kontaktstelle, bei der weitere Informationen erhältlich sind; — eine Beschreibung und die wahrscheinlichen Folgen des Verstoßes; — die Anzahl der betroffenen Personen sowie der Anzahl der betroffenen Aufzeichnungen; — getroffene oder geplante Maßnahmen. Verfeinerungen für Auftragsdatenverarbeiter: Im Falle einer Verletzung personenbezogener Daten muss der Auftragsdatenverarbeiter die verantwortliche Stelle unverzüglich nach Bekanntwerden der Verletzung benachrichtigen, damit die verantwortliche Stelle die geeigneten Maßnahmen ergreifen kann.
A.16.1.6	Erkenntnisse aus Informationssicherheitsvorfällen	Die Maßnahme ISO/IEC 27001 A.16.1.6 gilt.
A.16.1.7	Sammeln von Beweismaterial	Die Maßnahme ISO/IEC 27001 A.16.1.7 gilt.
A.17 Informationssicherheitsaspekte beim Business Continuity Management		
A.17.1 Aufrechterhaltung der Informationssicherheit		
Ziel: Die Aufrechterhaltung der Informationssicherheit und des Datenschutzes muss in die Business Continuity Management-Systeme eingebettet sein.		
A.17.1.1	Planung zur Aufrechterhaltung der Informationssicherheit	Die Maßnahme ISO/IEC 27001 A.17.1.1 gilt.
A.17.1.2	Umsetzung der Aufrechterhaltung der Informationssicherheit	Die Maßnahme ISO/IEC 27001 A.17.1.2 gilt.
A.17.1.3	Verifizieren und Bewerten der Aufrechterhaltung der Informationssicherheit	Die Maßnahme ISO/IEC 27001 A.17.1.3 gilt.
A.17.2 Redundanzen		

Tabelle A.1 (fortgesetzt)

Ziel: Sicherstellung der Verfügbarkeit von informationsverarbeitenden Einrichtungen		
A.17.2.1	Verfügbarkeit von informationsverarbeitenden Einrichtungen	Die Maßnahme ISO/IEC 27001 A.17.2.1 gilt.
A.18 Einhaltung		
A.18.1 Einhaltung gesetzlicher und vertraglicher Anforderungen		
Ziel: Vermeidung von Verstößen gegen rechtliche, gesetzliche, behördliche oder vertragliche Verpflichtungen im Zusammenhang mit der Informationssicherheit und dem Datenschutz sowie gegen jegliche Sicherheits- und Datenschutzanforderungen.		
A.18.1.1	Bestimmung der anwendbaren Gesetzgebung und der vertraglichen Anforderungen	Die Organisation muss die Maßnahme ISO/IEC 27001 A.18.1.1 umsetzen und dabei die zusätzlichen Leitlinien in EN ISO/IEC 27701, 6.15.1.1, beachten.
A.18.1.2	Geistige Eigentumsrechte	Die Maßnahme ISO/IEC 27001 A.18.1.2 gilt.
A.18.1.3	Schutz von Aufzeichnungen	Die Organisation muss die Maßnahme ISO/IEC 27001 A.18.1.3 umsetzen und dabei die zusätzlichen Leitlinien in EN ISO/IEC 27701, 6.15.1.3, beachten.
A.18.1.4	Privatsphäre und Schutz personenbezogener Daten	Die Organisation muss die Maßnahme ISO/IEC 27001 A.18.1.4 umsetzen.
A.18.1.5	Regelung der kryptographischen Maßnahme	Die Maßnahme ISO/IEC 27001 A.18.1.5 gilt.
A.18.2 Überprüfungen der Informationssicherheit		
Ziel: Sicherstellung, dass die Informationssicherheit und der Datenschutz in Übereinstimmung mit den organisatorischen Richtlinien und Verfahren umgesetzt und betrieben werden.		
A.18.2.1	Unabhängige Überprüfung der Informationssicherheit	Die Organisation muss die Maßnahme ISO/IEC 27001 A.18.2.1 umsetzen und dabei die zusätzlichen Leitlinien in EN ISO/IEC 27701, 6.15.2.1, beachten.
A.18.2.2	Einhaltung von Sicherheitsrichtlinien und -normen	Die Maßnahme ISO/IEC 27001 A.18.2.2 gilt.
A.18.2.3	Überprüfung der Einhaltung von technischen Vorgaben	Die Organisation muss die Maßnahme ISO/IEC 27001 A.18.2.3 umsetzen und dabei die zusätzlichen Leitlinien in EN ISO/IEC 27701, 6.15.2.3, beachten.

Anhang B (normativ)

PIMS-spezifische Referenzmaßnahmenziele und -Maßnahmen (verantwortliche Stellen)

Dieser Anhang ist zur Verwendung durch Organisationen bestimmt, die als verantwortliche Stellen mit oder ohne Einsatz von Auftragsdatenverarbeitern tätig sind. Er verfeinert EN ISO/IEC 27701:2021, Anhang A.

In Tabelle B.1 sind Verweisungen auf Maßnahmen nach EN ISO/IEC 27701:2021 in der Form „Die Organisation muss die Maßnahme EN ISO/IEC 27701 [Maßnahmennummer A.x.y.z.] unter Beachtung der zusätzlichen Leitlinien in ... umsetzen“; das heißt, dass die Organisation alle diese Maßnahmen unter Beachtung der entsprechenden Leitlinien umsetzen muss, um die allgemeine Anforderung in Abschnitt 6 zu erfüllen (in allen Fällen, unabhängig von der Risikobewertung und Risikobehandlung).

ANMERKUNG Die Abschnittsnummern in diesem Anhang beziehen sich auf die Unterabschnittsnummern in EN ISO/IEC 27701:2021, Anhang A.

Tabelle B.1 — Maßnahmenziele und Maßnahmen

B.7.2 Bedingungen für die Erhebung und Verarbeitung		
Ziel: Bestimmen und Dokumentieren, dass die Verarbeitung rechtmäßig ist, mit einer rechtlichen Grundlage nach den geltenden Rechtssystemen und mit klar definierten und legitimen Zwecken		
B.7.2.1	Identifizieren und Dokumentieren des Zwecks	Die Organisation muss die Maßnahme EN ISO/IEC 27701 A.7.2.1 umsetzen und dabei die Leitlinien in EN ISO/IEC 27701, 7.2.1, beachten.
B.7.2.2	Identifizieren der rechtmäßigen Grundlage	Die Organisation muss die Maßnahme EN ISO/IEC 27701 A.7.2.2 umsetzen und dabei die Leitlinien in EN ISO/IEC 27701, 7.2.2, beachten.
B.7.2.3	Bestimmen, wann und wie die Einwilligung einzuholen ist	Die Organisation muss die Maßnahme EN ISO/IEC 27701 A.7.2.3 umsetzen und dabei die Leitlinien in EN ISO/IEC 27701, 7.2.3, beachten.
B.7.2.4	Einholung und Aufzeichnung der Einwilligung	Die Organisation muss die Maßnahme EN ISO/IEC 27701 A.7.2.4 umsetzen und dabei die Leitlinien in EN ISO/IEC 27701, 7.2.4, beachten.

Tabelle B.1 (fortgesetzt)

B.7.2.5	Datenschutz-Folgenabschätzung	Die Organisation muss die Maßnahme EN ISO/IEC 27701 A.7.2.5 umsetzen und dabei die Leitlinien in EN ISO/IEC 27701, 7.2.5, und diese Verfeinerungen beachten: — Die Organisation muss die Verarbeitungsvorgänge ermitteln, die zu hohen Risiken für die Rechte und Freiheiten der Auftraggeber von personenbezogenen Daten führen können. — Die Organisation muss Datenschutz-Folgenabschätzungen für Verarbeitungsvorgänge mit hohem Risiko durchführen und dokumentieren. — Die Organisation muss den Datenschutzbeauftragten oder die für den Datenschutz zuständigen Personen (falls kein Datenschutzbeauftragter benannt ist) in die Überprüfung von Verarbeitungen mit hohem Risiko und in die Durchführung der Datenschutz-Folgenabschätzung einbeziehen. — Die Organisation muss gegebenenfalls die Meinung der betroffenen Personen oder ihres Vertreters einholen, ohne dass der Schutz der kommerziellen oder öffentlichen Interessen oder die Sicherheit der Verarbeitungsvorgänge beeinträchtigt wird. — Wenn eine Datenschutz-Folgenabschätzung eine Verarbeitung identifiziert, die zu hohen Risiken für die betroffenen Personen führen kann, muss die Organisation die Aufsichtsbehörden vor der Verarbeitung konsultieren und ihnen die erforderlichen Einzelheiten mitteilen, sofern der Datenbeauftragte keine Maßnahmen zur Minderung des Restrisikos ergriffen hat. Die Datenschutz-Folgenabschätzung muss mindestens: — systematisch die geplanten Verarbeitungsvorgänge und ihre Zwecke beschreiben; — die Rechtsgrundlage der Verarbeitungstätigkeit beschreiben; — die Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge im Hinblick auf die Zwecke beurteilen; — Risiken für die betroffenen Personen ermitteln und beurteilen; — die Maßnahmen ermitteln, mit denen die Risiken für die betroffenen Personen behandelt werden können.
B.7.2.6	Verträge mit Auftragsdatenverarbeitern	Die Organisation muss die Maßnahme EN ISO/IEC 27701 A.7.2.6 umsetzen und dabei die Leitlinien in EN ISO/IEC 27701, 7.2.6, beachten.
B.7.2.7	Gemeinsame verantwortliche Stelle	Die Organisation muss die Maßnahme EN ISO/IEC 27701 A.7.2.7 umsetzen und dabei die Leitlinien in EN ISO/IEC 27701, 7.2.7, beachten.