

	DIN EN 17926	
ICS 35.030 Datenschutz-Informationssystem per ISO/IEC 27701 – Konkretisierungen im europäischen Kontext; Deutsche Fassung EN 17926:2023 Privacy Information Management System per ISO/IEC 27701 – Refinements in European context; German version EN 17926:2023 Système de management de la protection de la vie privée conformément à l'EN ISO/IEC 27701 – Affinements relatifs au contexte européen; Version allemande EN 17926:2023 Gesamtumfang 40 Seiten DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)		

Nationales Vorwort

Dieses Dokument (EN 17926:2023) 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).

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
ISO/IEC 27001:2013	siehe	DIN EN ISO/IEC 27001:2017-06
ISO/IEC 27701:2021*	siehe	DIN EN ISO/IEC 27701:2021-07

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

* Fehler in der Referenzfassung: Das korrekte Ausgabejahr von ISO/IEC 27701 ist 2019.

Nationaler Anhang NA (informativ)

Literaturhinweise

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

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

DIN EN ISO/IEC 27701:2021-07, *Sicherheitstechniken — Erweiterung zu ISO/IEC 27001 und ISO/IEC 27002 für das Management von Informationen zum Datenschutz — Anforderungen und Leitlinien (ISO/IEC 27701:2019); Deutsche Fassung EN ISO/IEC 27701:2021*

DIN ISO/IEC 27001:2017-06, *Informationstechnik — Sicherheitsverfahren — Informationssicherheits-managementsysteme — Anforderungen (ISO/IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2:2015)*

– Leerseite –

Deutsche Fassung

Datenschutz-Informationssystem per
ISO/IEC 27701 —
Konkretisierungen im europäischen Kontext

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

Système de management de la protection de la vie
privée conformément à l'EN ISO/IEC 27701 —
Affinements relatifs au contexte européen

Diese Europäische Norm wurde vom CEN am 13. April 2023 angenommen.

Die CEN und CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN und CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN und CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN- und CENELEC-Mitglieder sind die nationalen Normungsinstitute und elektrotechnischen Komitees von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

Inhalt

	Seite
Europäisches Vorwort	3
Einleitung	4
1 Anwendungsbereich	5
2 Normative Verweisungen	5
3 Begriffe	5
4 Aufbau dieses Dokuments	5
5 Datenschutz-Informationssystem für Verarbeitungsvorgänge von personenbezogenen Daten	6
6 Anforderung für Verarbeitungsvorgänge personenbezogener Daten	6
Anhang A (normativ) Maßnahmen für Informationssicherheit und den Datenschutz	7
Anhang B (normativ) PIMS-spezifische Referenzmaßnahmenziele und -Maßnahmen (verantwortliche Stellen)	18
Anhang C (normativ) PIMS-spezifische Referenzmaßnahmenziele und -Maßnahmen (Auftragsverarbeiter)	25
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	18
Tabelle C.1 — Maßnahmenziele und Maßnahmen	25
Tabelle E.1 — Zuordnung der DSGVO-Artikel zu diesem Dokument	31

Europäisches Vorwort

Dieses Dokument (EN 17926:2023) wurde vom Technischen Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ erarbeitet, dessen Sekretariat von DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Mai 2024, und etwaige entgegenstehende nationale Normen müssen bis Mai 2024 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Liste dieser Institute ist auf den Internetseiten von CEN abrufbar.

Entsprechend der CEN CENELEC Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die Republik Nordmazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Einleitung

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 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 ISO/IEC 27701 im Kontext der DSGVO implementiert werden.

Dieses Dokument enthält Konkretisierungen zur ISO/IEC 27701 bei der Anwendung von Maßnahmen und Leitlinien in 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 als verantwortliche Stellen und/oder Auftragsverarbeiter im Rahmen eines ISMS (Informationssicherheitsmanagementsystem) personenbezogene Daten verarbeiten Auftragsverarbeiter. Dies soll von Organisationen im Zusammenhang mit der DSGVO verwendet werden, um die Einhaltung ihrer Verpflichtungen nachzuweisen. ISO/IEC 27701 in Verbindung mit den Konkretisierungen 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 ISO/IEC 27701 allein.

Somit kann ISO/IEC 27701 als internationales Rahmenwerk betrachtet werden, das für einen bestimmten regionalen Kontext (im Fall dieses Dokuments die Datenschutz-Grundverordnung) konkretisiert 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 Konkretisierungen zur 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 Konkretisierungen 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 Zertifizierungsverfahren 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 Konkretisierungen für eine Anwendung von 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 als verantwortliche Stellen und/oder Auftragsverarbeiter im Rahmen eines ISMS (Informationssicherheitsmanagementsystem) personenbezogene Daten verarbeiten.

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

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

ISO/IEC 27701:—¹, *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*

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 ISO/IEC 27701 definierte Datenschutz-Informationssicherheitsmanagementsystem und legt zusätzliche Anforderungen und Konkretisierungen 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.

1 Derzeit in Vorbereitung. Stufe zum Zeitpunkt der Veröffentlichung: ISO/IEC DIS 27701:2023.

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

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

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 ISO/IEC 27701 einführen, umsetzen, aufrechterhalten und fortlaufend verbessern.

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

ISO/IEC 27701:2021, 5.2.3, wird wie folgt konkretisiert:

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 konkretisiert:

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 Kontext von Risiken für die Informationssicherheit als auch von 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 konkretisiert:

Erstellung einer Erklärung zur Anwendbarkeit, die Folgendes enthält:

- die notwendigen Maßnahmen [siehe ISO/IEC 27001:2013, 6.1.3 b) und c), wie oben konkretisiert];
- 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 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, Anhang C geforderten Maßnahmen durchführen, je nach Rolle der Organisation (siehe ISO/IEC 27701, 5.2.1).

Anhang A
(normativ)

Maßnahmen für Informationssicherheit und den Datenschutz

Dieser Anhang ist zur Verwendung durch alle Organisationen bestimmt, unabhängig von ihrer Rolle (als verantwortliche Stelle, als Auftragsverarbeiter 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 Konkretisierungen 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 (ISO/IEC 27701, 5.4.1.2) und Risikobehandlung (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] umsetzen und dabei die zusätzlichen Leitlinien in ... beachten“ 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 Konkretisierungen der Leitlinien von 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

PIMS.5 Informationssicherheitsrichtlinien		
PIMS.5.1 Vorgaben der Leitung für Informationssicherheit		
Ziel: Vorgaben und Unterstützung für die Informationssicherheit und den Datenschutz sind seitens der Leitung in Übereinstimmung mit geschäftlichen Anforderungen und den relevanten Gesetzen und Vorschriften bereitgestellt.		
PIMS ISMS 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 ISO/IEC 27701, 6.2.1.1, beachten.
PIMS ISMS 5.1.2	Überprüfung der Informationssicherheitsrichtlinien	Die Maßnahme ISO/IEC 27001 A.5.1.2 gilt.
PIMS ISMS 6 Organisation der Informationssicherheit		
PIMS ISMS 6.1 Interne Organisation		
Ziel: Ein Rahmenwerk für die Leitung, mit dem die Umsetzung der Informationssicherheit und des Datenschutzes in der Organisation eingeleitet und gesteuert werden kann, ist eingerichtet.		

Tabelle A.1 (fortgesetzt)

PIMS ISMS 6.1.1	Informationssicherheitsrollen und -verantwortlichkeiten	Die Organisation muss die Maßnahme ISO/IEC 27001 A.6.1.1 umsetzen und dabei die zusätzlichen Leitlinien in ISO/IEC 27701, 6.3.1.1, und diese zusätzlichen Konkretisierungen beachten: — Die Organisation muss einen Datenschutzbeauftragten (DSB) als Verantwortlichen entsprechend 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 allen 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.
PIMS ISMS 6.1.2	Aufgabentrennung	Die Organisation muss die Maßnahme ISO/IEC 27001 A.6.1.2 umsetzen.
PIMS ISMS 6.1.3	Kontakt zu Behörden	Die Maßnahme ISO/IEC 27001 A.6.1.3 gilt.
PIMS ISMS 6.1.4	Kontakt zu speziellen Interessengruppen	Die Maßnahme ISO/IEC 27001 A.6.1.4 gilt.
PIMS ISMS 6.1.5	Informationssicherheit im Projektmanagement	Die Maßnahme ISO/IEC 27001 A.6.1.5 gilt.
PIMS ISMS 6.2 Mobilgeräte und Telearbeit		
Ziel: Die Informationssicherheit und der Datenschutz bei Telearbeit und der Nutzung von Mobilgeräten sind sichergestellt.		
PIMS ISMS 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 ISO/IEC 27701, 6.3.2.1, beachten.
PIMS ISMS 6.2.2	Telearbeit	Die Maßnahme ISO/IEC 27001 A.6.2.2 gilt.
PIMS ISMS 7 Personalsicherheit		
PIMS ISMS 7.1 Vor der Beschäftigung		
Ziel: Es ist sichergestellt, dass Beschäftigte und Auftragnehmer ihre Verantwortlichkeiten verstehen und für die für sie vorgesehenen Rollen geeignet sind.		
PIMS ISMS 7.1.1	Sicherheitsüberprüfung	Die Maßnahme ISO/IEC 27001 A.7.1.1 gilt.
PIMS ISMS 7.1.2	Beschäftigungs- und Vertragsbedingungen	Die Maßnahme ISO/IEC 27001 A.7.1.2 gilt.