

DIN EN 17483

ICS 03.080.99; 13.310

Einsprüche bis 2020-06-17

Entwurf**Private Sicherheitsvorkehrungen zum Schutz kritischer Infrastrukturen;
Deutsche und Englische Fassung prEN 17483:2020**

Private security provision for the protection of Critical Infrastructure;
German and English version prEN 17483:2020

Dispositions de sécurité privée pour la protection des infrastructures critiques;
Version allemande et anglaise prEN 17483:2020

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2020-04-17 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 nadl@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 Dienstleistungen (NADL), 10772 Berlin oder Saatwinkler Damm 42/43, 13627 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 50 Seiten

DIN-Normenausschuss Dienstleistungen (NADL)

Nationales Vorwort

Dieses Dokument (prEN 17483:2020) wurde vom Technischen Komitee CEN/TC 439 „Private Sicherheitsdienstleistungen“ erarbeitet, dessen Sekretariat von ASI (Österreich) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Arbeitsausschuss NA 159-01-02 AA „Wach- und Sicherheitsdienstleistungen“ im DIN-Normenausschuss Dienstleistungen (NADL).

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 14001	siehe	DIN EN ISO 14001
ISO 22300	siehe	DIN EN ISO 22300
ISO 26000	siehe	DIN ISO 26000
ISO 31000	siehe	DIN ISO 31000
ISO 45001	siehe	DIN ISO 45001

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 14001, *Umweltmanagementsysteme — Anforderungen mit Anleitung zur Anwendung*

DIN EN ISO 22300, *Sicherheit und Resilienz — Vokabular*

DIN ISO 26000, *Leitfaden zur gesellschaftlichen Verantwortung*

DIN ISO 31000, *Risikomanagement — Leitlinien*

DIN ISO 45001, *Managementsysteme für Sicherheit und Gesundheit bei der Arbeit — Anforderungen mit Anleitung zur Anwendung*

Private Sicherheitsvorkehrungen zum Schutz kritischer Infrastrukturen

Dispositions de sécurité privée pour la protection des infrastructures critiques

Private security provision for the protection of Critical Infrastructure

ICS:

Deskriptoren

Dokument-Typ: Europäische Norm

Dokument-Untertyp:

Dokument-Stage: CEN-Umfrage

Dokument-Sprache: D

STD Version 2.10b

Inhalt

	Seite
Europäisches Vorwort.....	4
1 Anwendungsbereich.....	5
2 Normative Verweisungen	5
3 Begriffe	5
4 Dienstleister	7
4.1 Allgemeines.....	7
4.2 Struktur.....	7
4.2.1 Managementstruktur.....	7
4.2.2 Verwaltung personeller Ressourcen	9
4.3 Management von Gesundheit und Sicherheit.....	10
4.4 Risikomanagement.....	10
4.5 Operative und finanzielle Leistungsfähigkeit.....	10
4.6 Geschäftskontinuitätsmanagement.....	11
4.7 Versicherungen	11
4.8 Unternehmensführung und Compliance.....	11
4.9 IT-Sicherheitsmanagement.....	11
5 Verträge.....	12
5.1 Allgemeines.....	12
5.2 Finanzielle Bedingungen.....	12
5.3 Vertragliche Haftung	12
5.4 Vertragsmanager.....	13
5.5 Verwaltung am Standort.....	13
5.6 Pflicht des Kunden.....	13
5.7 Ressourcen.....	13
5.8 Zusammenarbeit mit weiteren maßgeblichen Parteien.....	13
5.9 Unterauftragnehmer	13
5.9.1 Allgemeines.....	13
5.9.2 Aufträge	14
5.9.3 Auswahl	14
5.10 Leiharbeitskräfte.....	14
6 Personal	14
6.1 Allgemeines.....	14
6.1.1 Einleitung.....	14
6.1.2 Bedingungen und Konditionen des Arbeitsverhältnisses.....	14
6.1.3 Sicherheitsscreening.....	15
6.1.4 Verletzung der Bedingungen und Konditionen des Arbeitsverhältnisses.....	15
6.1.5 Identifizierung des Personals	16
6.1.6 Dienstkleidung.....	16
6.2 Personalbeschaffung und Auswahl	16
6.2.1 Allgemeines.....	16
6.2.2 Für die Anstellung zu erfüllende Kriterien.....	17
6.2.3 Auswahl	17
6.2.4 Bewerbungsgespräch.....	17
6.2.5 Anstellung.....	18
6.3 Schulung.....	19

6.3.1	Schulungskonzept.....	19
6.3.2	Schulungsleiter.....	19
6.3.3	Anforderungen an Schulungen.....	19
7	Dienstleistungserbringung.....	20
7.1	Arbeits- und Vertragsbeginn.....	20
7.2	Betriebliche Abläufe.....	20
7.3	Kommunikation mit dem Kunden.....	20
7.4	Einsatzplan und Dienstplanung.....	21
7.5	Dienstleistungsvereinbarung.....	21
7.6	Vertragsbeendigung und Einstellung der Dienstleistungen.....	21
Anhang A (informativ) Beispiele für Branchen mit kritischen Infrastrukturen.....		22
Literaturhinweise.....		25

Europäisches Vorwort

Dieses Dokument (prEN 17483:2020) wurde vom Technischen Komitee CEN/TC 439 „Private Sicherheitsdienstleistungen“ erarbeitet, dessen Sekretariat von ASI gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

1 Anwendungsbereich

Dieses Dokument ist die übergreifende Norm für die Bereitstellung privater Sicherheitsdienstleistungen für kritische Infrastrukturen. Es wird ergänzt durch vertikale untergeordnete Normen für bestimmte Branchen mit einem umfassenderen Schwerpunkt auf den zugehörigen Dienstleistungen wie z. B. Sicherheit in der Luftfahrt und Sicherheit in der Seeschifffahrt/von Seehäfen.

Es legt Dienstleistungsanforderungen an die Qualität in Bezug auf Organisation, Prozesse, Personal und Verwaltung eines Sicherheitsdienstleisters/Sicherungsdienstleisters und/oder von dessen unabhängigen Zweigstellen und Niederlassungen nach Handelsrecht als Anbieter von Sicherheitsdienstleistungen fest.

Es legt Qualitätskriterien für das Erbringen von Sicherheitsdienstleistungen fest, die von öffentlichen und privaten Kunden nachgefragt werden.

Dieses Dokument ist geeignet für die Auswahl, Zuteilung, Auftragsvergabe und Kontrolle des am besten geeigneten Anbieters von Sicherheitsdienstleistungen.

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 15602:2008, *Sicherheitsdienstleister/Sicherungsdienstleister — Terminologie*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach EN 15602 und die folgenden Begriffe.

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

— IEC Electropedia: verfügbar unter <http://www.electropedia.org/>

— ISO Online Browsing Platform: verfügbar unter <http://www.iso.org/obp>

3.1

kritische Infrastruktur

Anlage, System oder Teil davon, die von wesentlicher Bedeutung für die Aufrechterhaltung grundlegender gesellschaftlicher Funktionen, der Gesundheit, Sicherheit, Sicherung und des wirtschaftlichen oder sozialen Wohlergehens von Menschen sind, und deren Störung oder Zerstörung infolge der Erfolglosigkeit, diese Funktionen aufrechtzuerhalten, sich erheblich auf eine Gesellschaft auswirken würde

Anmerkung 1 zum Begriff: Beispiele für Branchen mit kritischer Infrastruktur sind in Anhang A angegeben.

3.2

Insider-Bedrohung

Bedrohung, die vom unbefugten Zugriff, von unbefugter Nutzung oder von der Offenlegung vertraulicher Informationen, Verfahren, Technologien, Anlagen oder Räumlichkeiten durch eine Person mit rechtmäßigem oder indirektem Zugang ausgeht, welche zu Beeinträchtigungen oder Schäden führen könnte

3.3

Strategie für Insider-Bedrohungen

Strategie, die darauf abzielt, Insider-Bedrohungen zu erkennen und abzuschwächen

3.4

Risikobewertung

systematischer Prozess zur Identifizierung, Analyse und Beurteilung von Bedrohungen, um die Auswirkung der Folgen von Gefährdungen und Bedrohungen in Bezug auf die Wahrscheinlichkeit ihres Auftretens zu ermitteln

3.5

Sicherheitsanalyse

Gesamtheit festgelegter organisatorischer, personalbezogener, technischer und struktureller Sicherheitsmaßnahmen für die Verhinderung und/oder Abwendung von Gefährdungen durch schriftliche Analyse möglicher Angriffs- und Schadensszenarien mit dem Ziel, ein festgelegtes Schutzniveau zu erreichen

Anmerkung 1 zum Begriff: Sicherheitsanalysen beruhen auf einem strukturierten Ansatz, der im Allgemeinen die folgenden Kriterien einschließt:

- Bestimmung des zu schützenden Objekts und der Schutzziele;
- Analyse von Bedrohungen/Schadensszenarien/Gefährdungen;
- Beurteilung der Eintrittswahrscheinlichkeit und des potenziellen Schadensausmaßes;
- Erarbeitung von Maßnahmen zur Verringerung von Schäden und von deren Eintrittswahrscheinlichkeit;
- Erarbeitung von Maßnahmen, um Sicherheitsleistungen frühestmöglich einzuleiten (z. B. Koordinierung elektronischer und mechanischer Sicherheitsvorrichtungen, um einen Alarm auszulösen, bevor die mechanischen Sicherheitseinrichtungen vollständig überwunden wurden);
- Planung von Maßnahmen und Bereitstellung von Mitteln zur Schadensregulierung und -begrenzung im Schadensfall;
- Analyse der eigenen Risikotragfähigkeit und Bewertung des Restrisikos.

Selbst mit einer differenzierten Sicherheitsanalyse kann das Restrisiko nicht vollständig beseitigt werden. Aus diesem Grund wird oftmals ein Krisen- und Katastrophenmanagement eingeführt, um in einem Notfall Leben und Sachwerte weitestgehend zu schützen.

3.6

Strategie für das Leistungsmanagement des Personals

systematischer Prozess, durch den der Dienstleister seine Mitarbeiter als Einzelpersonen und Mitglieder einer Gruppe an der Verbesserung der organisatorischen Effektivität bei der Umsetzung seines Auftrags und seiner Ziele beteiligt

Anmerkung 1 zum Begriff: Diese Strategie ist ein Werkzeug, das angewendet wird, um das organisatorische Ziel gegenüber den Mitarbeitern einzeln zu kommunizieren, ihnen eine individuelle Verantwortlichkeit gegenüber diesem Ziel zuzuweisen, und den Fortschritt bei der Erreichung der zugewiesenen Ziele zu verfolgen sowie die individuelle Leistung der Mitarbeiter zu beurteilen. Die Strategie für das Leistungsmanagement des Personals spiegelt die individuelle Leistung oder Aufgabenbewältigung eines Mitarbeiters wider und beurteilt alle Mitarbeiter der Organisation und behält den Überblick über diese.

3.7

branchenspezifische untergeordnete Norm

ergänzende vertikale Normen zu dieser übergreifenden Norm innerhalb der Branchen mit kritischer Infrastruktur

Anmerkung 1 zum Begriff: Beispiele für Branchen mit kritischer Infrastruktur sind in Anhang A angegeben.

Anmerkung 2 zum Begriff: Siehe Bild 1.

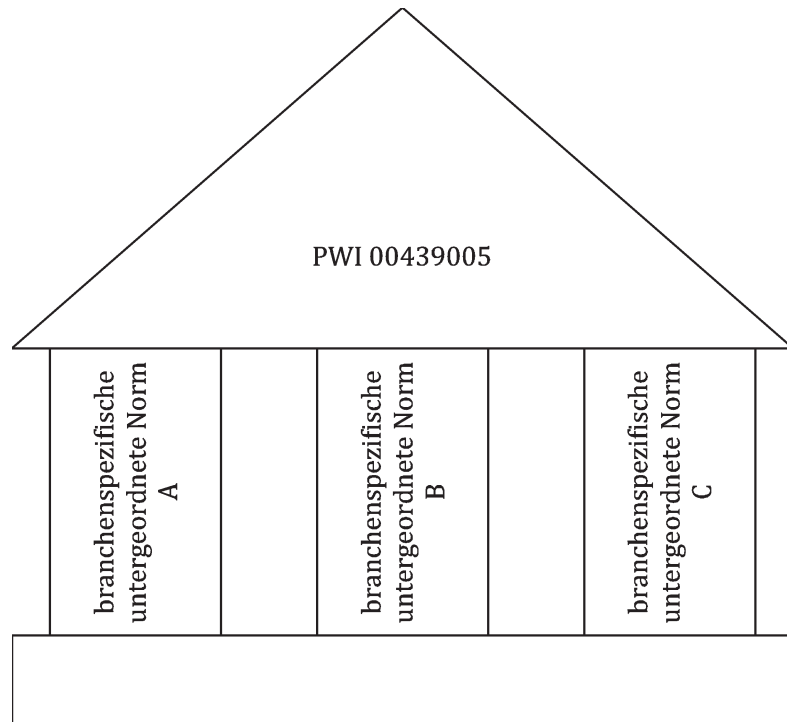


Bild 1 — Struktur für branchenspezifische untergeordnete Normen

4 Dienstleister

4.1 Allgemeines

Der Dienstleister muss durch die zuständigen Behörden zur Erbringung privater Sicherheitsdienstleistungen für kritische Infrastrukturen ermächtigt werden, sofern diese bereits festgelegt und/oder durch öffentliche Behörden in Übereinstimmung mit dem nationalen gesetzlichen Rahmen geregelt sind.

Ein Dienstleister darf nur diejenigen privaten Sicherheitsdienstleistungen für kritische Infrastrukturen anbieten, für die er von der zuständigen Behörde die erforderliche Autorisierung entsprechend der/den branchenspezifischen untergeordneten Norm(en) erhalten hat.

4.2 Struktur

4.2.1 Managementstruktur

Der Dienstleister muss nachweisen, dass seine Eigentümer, Vorstandsmitglieder und sein Management ein reines Strafregister haben, und z. B. nicht wegen irgendwelcher Straftaten verurteilt wurden oder keine Verfahren anhängig sind in Zusammenhang mit beispielsweise:

- a) Waffen- und/oder Drogenschmuggel und/oder organisiertem Verbrechen;
- b) Bestechung und/oder Korruption;
- c) Betrug und/oder Geldwäsche und/oder Finanzierung von Terrorismus;
- d) dem Versuch oder Begehen terroristischer Straftaten;
- e) Kinderarbeit und/oder Menschenhandel;

- f) vorsätzlichen Straftaten gegenüber Menschen und öffentlichem oder privatem Eigentum;
- g) Steuerhinterziehung oder Hinterziehung von Sozialversicherungsbeiträgen.

Sofern gesetzlich zutreffend, müssen sie im Besitz der für ihre Funktion erforderlichen Lizenz sein.

Der Dienstleister muss

- 1) eine Managementstruktur haben, die auf jeder Ebene des Betriebes die Führung, Kontrolle und Verantwortlichkeit zeigt,
- 2) über einen Verhaltenskodex hinsichtlich Ethik, Drogen und Alkohol verfügen,
- 3) über einen Verhaltenskodex hinsichtlich Compliance und sozialer Unternehmensverantwortung verfügen,
- 4) über einen Verhaltenskodex bezüglich der Betriebsabläufe (z. B. Auftreten, Verhalten, Pünktlichkeit) verfügen,
- 5) Strukturen und Verfahren klar an alle operativen Ebenen kommunizieren,
- 6) ein Beschwerdemanagementsystem in Übereinstimmung mit Qualitätsmanagementsystemen unterhalten,
- 7) die sichere Lagerung aller wichtigen und vertraulichen Dokumente mit Bezug zu dem Auftrag sicherstellen,
- 8) unter Geheimhaltung von Informationen und Daten mit Bezug zu dem Unternehmen arbeiten,
- 9) Vorschriften bezüglich der Weitergabe von Vertragsinformationen an Dritte bereitstellen,
- 10) eine betriebliche Präsenz in einer angemessenen Entfernung zum Ausführungsort der Dienstleistung während der Laufzeit des Vertrages oder zumindest für die Dauer der Ausführung der Dienstleistungen haben,
- 11) die Eigentumsverhältnisse seines Unternehmens sowie die *Lebensläufe* seines Führungspersonals offenlegen,
- 12) jegliche ausstehenden Haftstrafen oder nicht entlasteten Konkurs eines Geschäftsinhabers oder Geschäftsführers offen legen,
- 13) über seine Mitgliedschaft in Berufsverbänden Auskunft erteilen und
- 14) über die Einhaltung der anwendbaren Umweltschutzgesetzgebung bei seinen Tätigkeiten Auskunft erteilen.

Falls der potenzielle Kunde es verlangt, muss der Dienstleister in der Lage sein, gegenüber diesem Vorstehendes vor der Vertragsunterzeichnung nachzuweisen. Der Dienstleister kann gegenüber dem potenziellen Kunden weitere maßgebende Informationen wie beispielsweise hinsichtlich einer weiteren Zertifizierung offen legen.

4.2.2 Verwaltung personeller Ressourcen

4.2.2.1 Allgemeines

Der Dienstleister muss über ein Regelwerk bezüglich personeller Ressourcen verfügen, das Folgendes umfassen muss:

- a) Einhaltung der Arbeits- und Sozialgesetzgebung und von Tarifverträgen;
- b) Einhaltung von Gesetzen und Vorschriften bezüglich Gesundheit und Sicherheit und entsprechender interner Leitlinien für Gesundheit und Sicherheit;
- c) Aufrechterhaltung genauer Angaben/Daten über die Belegschaftsstruktur und den Personalbestand;
- d) eine Leitlinie für die Personalbeschaffung einschließlich der Stellenbeschreibung;
- e) Leitlinien zur Mitarbeiterbindung;
- f) Leitlinien zur Karriereentwicklung;
- g) eine Schulungsleitlinie;
- h) Leitlinien zur Verminderung von Fehlzeiten;
- i) Leitlinien zur Gleichstellung;
- j) Disziplinar- und Beschwerdeverfahren;
- k) Prüfung/Aufsicht;
- l) Betriebsführung;
- m) Personalzufriedenheitsquoten;
- n) Mitarbeitervertretung (Mitbestimmungsrecht).

4.2.2.2 Mitarbeitermotivation

Der Dienstleister muss seine Strategie zur Motivation seines Sicherheitspersonals nachweisen. Diese Strategie muss mindestens Folgendes umfassen:

- angewendete Methodiken;
- Motivationsmesssystem;
- Motivationstechniken;
- verantwortungsvolles Handeln im Beruf;
- Selbstmanagement (Schichtdienst, Maßnahmen gegen Langeweile);
- Kommunikation im Beruf (Umgang mit Kunden und Kollegen);
- Sicherheitsbewusstsein.

Der Dienstleister muss in das Unternehmen eintretendes Personal über Karrieremöglichkeiten in Kenntnis setzen.

4.2.2.3 Strategie für das Leistungsmanagement des Personals

Der Dienstleister muss eine eindeutig festgelegte Strategie für das Leistungsmanagement des Personals umsetzen.

4.3 Management von Gesundheit und Sicherheit

Der Dienstleister muss über ein strukturiertes Managementsystem für Gesundheit und Sicherheit bei der Arbeit verfügen (z. B. ISO 45001 [10]).

ANMERKUNG ISO 45001 [10] (alt: OHSAS 18001:2007 [12]) ist eine Arbeits- und Gesundheitsschutz-Bewertungsreihe für Gesundheits- und Sicherheitsmanagementsysteme. Ein solches Managementsystem ist dafür vorgesehen, den Dienstleister bei der Steuerung der Arbeitsgesundheits- und -sicherheitsrisiken zu unterstützen.

Der Dienstleister muss berufliche Risiken verhindern und nachweisen, dass der Kunde stets aktiv einbezogen wird.

Das Arbeitsumfeld muss dem Stand der sozialen und technischen Entwicklung entsprechen, die sich auf die Gesundheit und Sicherheit auswirkt.

Die Arbeit muss so geplant werden, dass sie in einer sicheren und gesunden Umgebung durchgeführt werden kann.

Der Dienstleister muss Unfälle zusammen mit dem Gesundheits- und Sicherheitsvertreter des Kunden und/oder des Personals, sofern vorhanden, untersuchen, durchgehend Risiken bewerten und alle notwendigen Vorkehrungen treffen.

Der Dienstleister muss die Arbeitsbedingungen, die Aktionspläne und die Maßnahmen zu ihrer Verbesserung dokumentieren.

Der Dienstleister muss außerdem den Angestellten vorbeugende medizinische Betreuung zur Verfügung stellen, die für deren Arbeitsbedingungen angemessen ist. Bei einem gesundheits- und sicherheitsrelevanten Vorfall muss der Dienstleister dem Mitarbeiter außerdem auch eine medizinische Behandlung kostenfrei zur Verfügung stellen.

4.4 Risikomanagement

Der Dienstleister muss ein Risikomanagementsystem einrichten und aufrechterhalten und in der Lage sein, dies nachzuweisen (z. B. EN ISO 22301 [3] oder ISO 31000 [7]).

4.5 Operative und finanzielle Leistungsfähigkeit

Der Dienstleister muss nachweisen, dass er über die notwendige Kapazität hinsichtlich der Infrastruktur, des Personals und der Verfahren verfügt, um die vollständige Umsetzung aller Bedingungen und Bestimmungen des Vertrags zwischen dem Dienstleister und dem Kunden zu garantieren.

Der Dienstleister muss dem potenziellen Kunden bezüglich seiner Unternehmensstruktur, gegebenenfalls bezüglich seines speziell abgestellten, verantwortlichen Managements, des Umfangs der angebotenen Dienstleistungen, für die er autorisiert ist, und der Länge seiner bisherigen Tätigkeit im Bereich der Sicherheitsdienstleistungen für kritische Infrastrukturen Informationen zur Verfügung stellen.

Auf Ersuchen des potenziellen Kunden muss der Dienstleister auch eine projektbezogene Betriebs- und Finanzplanung bereitstellen, falls der Anteil des Umfangs der nachgefragten Sicherheitsdienstleistungen einen Wert von 15 % im Verhältnis zum Gesamtumsatz des letzten abgeschlossenen Geschäftsjahres des Dienstleisters übersteigt.

4.6 Geschäftskontinuitätsmanagement

Der Dienstleister muss ein dokumentiertes Regelwerk bezüglich der Geschäftskontinuität einschließlich operativer Notfallpläne aufstellen.

Der Dienstleister muss einen Nachweis darüber erbringen, welche signifikanten Risiken hinsichtlich seiner betrieblichen Abläufe und Verfahren und der zu diesem Zweck eingesetzten Technologien bestehen, z. B. auf der Grundlage von EN ISO 9001 [6]. Insbesondere müssen die kritischen Prozesse identifiziert werden und es sind geeignete Maßnahmen zur Risikominimierung festzulegen.

ANMERKUNG Weitere Informationen und Beispiele sind z. B. in EN ISO 22301 [3] angegeben.

4.7 Versicherungen

Es wird erwartet, dass der Dienstleister internationale und/oder nationale Vorschriften und Tarifverträge bezüglich Versicherungen einhält.

Die Versicherungen des Dienstleisters müssen Folgendes abdecken:

- Unfälle von Mitarbeitern während des Dienstes (einschließlich der erforderlichen Onboarding- und Offboarding-Zeit vor und nach dem Dienst);
- allgemeine Haftung;
- Sozialversicherung/Betriebshaftpflicht.

Der Dienstleister muss dem Kunden Informationen über seine Strategie und Auffassungen bezüglich der Haftpflicht gegenüber Dritten zur Verfügung stellen.

Der Dienstleister muss sicherstellen, dass der Kunde einen hinreichenden Nachweis über geeigneten Versicherungsschutz erhält.

Bei der Untervergabe von Arbeiten an einen Dritten muss der Dienstleister sicherstellen, dass ein für das Geschäft angemessener Versicherungsschutz besteht.

4.8 Unternehmensführung und Compliance

Der Dienstleister muss eine strukturierte Richtlinie zur Unternehmensführung oder ein gleichwertiges Regelwerk vorweisen und muss hierfür einen Nachweis erbringen:

- Verhaltenskodex für Führungskräfte und Angestellte;
- interne und externe Überwachungsverfahren und Audits;
- Regelungen für die Rechenschaftslegung — finanziell und betrieblich;

4.9 IT-Sicherheitsmanagement

Der Dienstleister muss ein dokumentiertes IT-Sicherheitsmanagement entsprechend bestehender Normen, z. B. auf der Grundlage von EN ISO/IEC 27001 [4] einrichten.

5 Verträge

5.1 Allgemeines

Ein schriftlich niedergelegter Vertrag zwischen dem Dienstleister und dem Kunden muss von beiden Parteien unterzeichnet werden. Der Vertrag muss die Rechte und Pflichten des Dienstleisters und des Kunden darlegen, einschließlich der jeweiligen Haftungen und Verantwortlichkeiten sowie der finanziellen und wirtschaftlichen Aspekte. Der Vertrag muss den Einsatz von Unterauftragnehmern sowie diesbezügliche Bedingungen eindeutig festlegen.

Der Kunde muss dem Dienstleister eine Sicherheitsanalyse in dem für die Erbringung der Sicherheitsdienstleistung erforderlichen Umfang zur Verfügung stellen. In der Sicherheitsanalyse müssen kritische Infrastrukturen (siehe 3.1) gesondert identifiziert werden.

Wenn der Kunde nicht in der Lage ist, eine Sicherheitsanalyse bereitzustellen, sollte der Dienstleister eine Risikobewertung des Standortes der kritischen Infrastruktur durchführen:

- Bewertung der Wahrscheinlichkeit einer Sicherheitsverletzung und/oder Bedrohung und die Folge eines solchen Ereignisses für den Standort;
- Festlegung von Gegenmaßnahmen und des Sicherheitsplanes;
- Klarstellung, dass der vorgeschlagene Vertrag der Risikobewertung entspricht.

Die Sicherheitsanalyse/-bewertung bildet die Grundlage für die Erarbeitung des Sicherheitsplanes. Der Sicherheitsplan sollte die Optimierung der geforderten Dienstleistungen durch die Nutzung von Technologien, Verfahren und Arbeitskräften berücksichtigen. Der Sicherheitsplan muss Informationen enthalten, um die fortlaufende Erbringung von Dienstleistungen und den Einsatz von Managern am Standort sicherzustellen.

5.2 Finanzielle Bedingungen

Der Dienstleister muss dem potenziellen Kunden die folgenden Informationen zur Verfügung stellen bezüglich:

- Bilanzaufstellungen und Gewinn- und Verlustrechnungen der vergangenen drei Geschäftsjahre, wenn ihre Veröffentlichung durch die Gesetzgebung oder Praktiken des Landes, in dem der Bewerber registriert ist, vorgeschrieben ist;
- einer gültigen steuerlichen Unbedenklichkeitsbescheinigung, sofern maßgebend;
- einer Unbedenklichkeitsbescheinigung der Sozialversicherungsbehörden bezüglich der erforderlichen Sozialversicherungsabgaben, sofern maßgebend.

5.3 Vertragliche Haftung

Die Haftung des Dienstleisters für Schäden, die im Verlaufe der Erbringung von Dienstleistungen entstehen und für die der Dienstleister verantwortlich ist, muss zwischen dem Dienstleister und dem Kunden im Rahmen des Vertrages vereinbart werden.

Der vom Kunden geforderte Haftungsbetrag muss zumindest bei leichter Fahrlässigkeit begrenzt werden. Diese Haftungsgrenzen müssen im Vertrag geregelt und zur Risikoanalyse/-bewertung und zum Auftragswert ins Verhältnis gesetzt werden. Die Haftungsgrenzbeträge dürfen nicht die Versicherungsdeckung übersteigen.

5.4 Vertragsmanager

Der Dienstleister muss einen Vertragsmanager bestimmen und dem Kunden vorstellen, der für die Organisation und Umsetzung des Vertrages verantwortlich ist. Diese Person muss die Vollmacht haben, alle beschäftigungsbezogenen Angelegenheiten hinsichtlich des Vertrages abzuwickeln.

5.5 Verwaltung am Standort

Wenn an einem Standort gleichzeitig mehrere Sicherheitsmitarbeiter im Dienst sind, muss ein Einsatzleiter festgelegt werden (z. B. dienstältester Bediensteter, Teamleiter, Schichtleiter).

5.6 Pflicht des Kunden

Der Kunde muss sicherstellen, dass es eine speziell zugeordnete verantwortliche Person gibt, die sich mit allen betrieblichen Angelegenheiten in Bezug auf den Vertrag befasst. Diese Person oder ein fest zugeordneter Vertreter muss für den Vertragsmanager des Dienstleisters oder weitere maßgebende Personen jederzeit erreichbar sein. Der Kunde muss regelmäßige Vertragsmanagement-Besprechungen mit dem Dienstleister festsetzen, um diesen hinsichtlich vorliegender und bevorstehender Angelegenheiten auf den neuesten Stand zu bringen. Der Kunde muss den Dienstleister über entscheidende Angaben zu und Änderungen der Sicherheitsrisiken informieren, da diese für die Erfüllung der vertraglichen Verpflichtungen maßgebend sind.

5.7 Ressourcen

Alle für die Erfüllung der vertraglichen Pflichten erforderlichen Ausrüstungen, Systeme und Fahrzeuge müssen vom Kunden oder Dienstleister bereitgestellt werden.

Der Eigentümer der vom Dienstleister verwendeten Ausrüstungen, Systeme und Fahrzeuge ist verantwortlich für deren vollständige Instandhaltung und den ordnungsgemäßen betrieblichen Einsatz. Internationale, nationale oder örtliche Vorschriften gelten genauso wie Leitlinien des Herstellers. Die Verantwortung für die Instandhaltung kann alternativ vom Eigentümer einer anderen Partei übertragen werden, die gebührend für die Erfüllung dieser Aufgabe qualifiziert ist.

Internationale, nationale oder örtliche Vorschriften gelten für den Einsatz von Hunden zur Durchführung spezieller Kontrolltätigkeiten im Rahmen des Vertrages.

5.8 Zusammenarbeit mit weiteren maßgeblichen Parteien

Falls erforderlich muss der Dienstleister mit weiteren maßgeblichen Parteien (z. B. Polizei, Feuerwehr, Notdienste, Behörden, weitere Dienstleister) zusammenarbeiten.

5.9 Unterauftragnehmer

5.9.1 Allgemeines

Der Dienstleister darf keine seiner vertraglichen Verpflichtungen ohne die vorherige, schriftliche Zustimmung des Kunden untervergeben. Im Fall einer solchen Untervergabe muss der Dienstleister im vollen Umfang für die ordnungsgemäße Erfüllung seiner vertraglichen Verpflichtungen haftbar bleiben.

Eine weitere Untervergabe von Dienstleistungen durch den Unterauftragnehmer des Dienstleisters, der direkt im Auftrag des Kunden handelt, ist nicht zulässig.

Mitarbeiter, die beim Dienstleister verpflichtet sind, dürfen nicht gleichzeitig über einen Unterauftragnehmer oder als unabhängiger Unterauftragnehmer für den Dienstleister arbeiten.