

Compliance-Management im Unternehmen

Inhalt

Compliance organisieren – so gehen Unternehmen vor	2
Compliance-Richtlinien – wichtige Inhalte, Themen, Bereiche	10
NIS-2-Richtlinie – wer ist betroffen, was ist zu tun?	18
Betriebsbeauftragte: Welche müssen bestellt werden?	27
Empfehlungen aus dem Management-Handbuch	40
Autoren	42

Compliance organisieren – so gehen Unternehmen vor

Jedes Unternehmen muss seine Compliance organisieren, um alle gesetzlichen Vorgaben einzuhalten. Bei der Fülle von relevanten Regelungen ist das für die Beschäftigten aber schwer zu bewältigen. Deshalb sollte eine Compliance-Vereinbarung erstellt und ein Beauftragter eingerichtet werden. Erfahren Sie hier: Wie wird Compliance im Unternehmen kommuniziert? Warum kann eine Compliance-Vereinbarung sinnvoll sein und was sollte diese regeln? Welche Aufgaben hat ein Compliance-Beauftragter?

Zuletzt geändert am 16.04.2024

Von Jan Lehmann, Jan Lehmann – Redaktionsbüro



Worum geht es bei Compliance?

Mit dem Begriff Compliance ist die Befolgung sämtlicher Regeln gemeint, die im Zusammenhang mit dem Geschäftsalltag stehen. Es geht also um die **Einhaltung von Gesetzen, Verordnungen, Verträgen, Vereinbarungen und Richtlinien**.

Tag für Tag müssen in einem Unternehmen zahlreiche Regeln beachtet werden, wie zum Beispiel Datenschutzvorgaben, steuerliche Vorschriften, Arbeitsschutzbestimmungen oder Umweltschutzauflagen. Dazu kommen in vielen Betrieben interne Regeln wie Verhaltens-Richtlinien oder Anweisungen zum richtigen Umgang mit Kundengeschenken. Die Einhaltung all dieser Regeln wird unter dem Begriff „Compliance“ zusammengefasst.

Warum ist Compliance wichtig?

Inzwischen herrscht in Unternehmen ein großes Bewusstsein für Compliance. Spätestens dann, wenn Unternehmen aufgrund von Gesetzesverstößen hohe Strafen zahlen müssen oder wenn die Presse über schlechte Machenschaften berichtet, wird klar, dass es klare Regeln für das Unternehmen und alle Beschäftigten braucht.

Es geht bei Compliance darum,

- sich regelkonform zu verhalten, um negative rechtliche Konsequenzen zu vermeiden, sowie
- eine Unternehmenskultur zu entwickeln und zu etablieren, in der die Beachtung ethischer Standards einen hohen Stellenwert hat.

Die Unternehmens- und Geschäftsleitung muss dafür zu sorgen, dass straf- oder bußgeldbewehrte Pflichten nicht verletzt werden. Das schreibt das **Ordnungswidrigkeitengesetz (OWiG)** vor. Dieses Gesetz ist eine wichtige Grundlage für Compliance im Unternehmen.

Was sind die Ziele von Compliance?

Ziel von Compliance sollte es sein, dass sämtliche Geschäftspraktiken und Unternehmensprozesse den geltenden Gesetzen, betriebsinternen Richtlinien und ethischen Standards entsprechen.

Mit Compliance-Maßnahmen soll insbesondere erreicht werden,

- Fehlverhalten der Arbeitnehmerinnen und Arbeitnehmer zu verhindern,
- Haftungsrisiken zu minimieren,
- Schadensersatzansprüche, Bußgeldzahlungen und Strafen zu vermeiden,
- Transparenz und Klarheit zu schaffen, damit alle im Unternehmen wissen, was gilt,
- Compliance als Teil der Unternehmenskultur zu etablieren,
- das Arbeitgeberimage zu verbessern und einen Imageverlust zu vermeiden sowie
- die Glaubwürdigkeit des Unternehmens in der Öffentlichkeit zu erhalten und zu verbessern.

Tipp**Compliance nach ISO 37301**

Für die Organisation eines Compliance-Management-Systems (CMS) können Sie sich an der ISO-Norm 37301:2021 orientieren. In dieser Norm ist erläutert, welche Verantwortung die Führung trägt, mit welchen Maßnahmen Compliance umgesetzt und sichergestellt wird und wie das Compliance-Management-System überprüft wird.

Wie sollte Compliance im Unternehmen kommuniziert werden?

Um ein Bewusstsein für Compliance nachhaltig im Unternehmen zu verankern, müssen Führungskräfte und Beschäftigte zu diesem Thema informiert und dafür sensibilisiert werden. Zum Beispiel mittels:

- betrieblichen Infoveranstaltungen
- Schulungen und Seminare
- E-Learning-Kurse
- Workshops

Ausführliche Kommunikation der vereinbarten und geltenden Regeln im Unternehmen ist ein wichtiger Baustein der Unternehmens-Compliance. Zum einen müssen alle Beschäftigten wissen, in welcher Situation sie wie agieren dürfen – und was nicht erlaubt ist. Zum anderen müssen sie die Gründe und Hintergründe kennen, warum die jeweilige Regel wichtig und einzuhalten ist.

Warum ist eine Compliance-Vereinbarung sinnvoll?

Eine Compliance-Vereinbarung oder eine Compliance-Richtlinie kann als wichtige unternehmensinterne Richtschnur dienen, wie Regelverstöße verhindert oder aufgedeckt werden können und welche Konsequenzen einen Compliance-Verstoß nach sich ziehen kann.

Was sollte in einer Compliance-Vereinbarung geregelt sein?

Branchenübergreifend empfiehlt es sich, in der Compliance-Vereinbarung allgemeine Verhaltensregeln für das Unternehmen aufzustellen sowie spezielle Anforderungen für den Umgang mit Kunden, Geschäftspartnern und Wettbewerbern zu definieren.

Beispiel

Regeln für den Umgang mit Kundinnen und Kunden

In der Compliance-Vereinbarung wird festgelegt, was bei einem Kundenbesuch zulässig ist und was nicht:

- Darf der Kunde in ein Restaurant eingeladen werden?
- Bis zu welchem Betrag sind Geschenke an Kunden erlaubt?
- Bei einem Kundenbesuch in Ihrem Unternehmen: Welche Form von Catering ist zulässig?

Zudem sollte der Aspekt Gleichbehandlung thematisiert und auf die geltenden Regeln zur Gleichbehandlung von Frauen und Männern sowie zum Schutz vor Diskriminierungen hingewiesen werden. Auch sollte die Vereinbarung eine Regelung zu möglichen Konsequenzen und Sanktionsmöglichkeiten bei Compliance-Verstößen enthalten.

Welche spezifischen Compliance-Anforderungen sind zu beachten?

Darüber hinaus sollte jedes Unternehmen seine **branchen- und unternehmensspezifischen Besonderheiten** und Risiken analysieren und seine Compliance-Anforderungen entsprechend ausrichten.

Beispiel 1: In der Lebensmittelbranche ist die Beachtung der geltenden Hygienevorschriften von zentraler Bedeutung. Dieser Aspekt sollte sich dementsprechend auch in der Compliance-Vereinbarung wiederfinden.

Beispiel 2: Bestimmte gesetzliche Pflichten gelten nur für Unternehmen ab einer bestimmten Größe, so zum Beispiel die Sorgfaltspflichten gemäß dem Lieferkettengesetz.

Was sind die Aufgaben eines Compliance-Beauftragten?

Der Compliance-Beauftragte ist dafür verantwortlich, dass die betrieblichen Compliance-Vorgaben umgesetzt und eingehalten werden. Er sollte dabei eng mit den einzelnen Abteilungen des Unternehmens zusammenarbeiten, um mögliche Risiken frühzeitig erkennen und minimieren zu können. Dabei sollte er als Schnittstelle fungieren. Er ist zudem der interne Ansprechpartner zum Thema Compliance.

Die Aufgaben des Compliance-Beauftragten sind beispielsweise:

- Überwachung der Prozesse im Unternehmen im Hinblick auf die Einhaltung von Regeln und ethischen Standards
- Identifizierung möglicher Risiken, welche durch die Nichteinhaltung von Regeln entstehen können
- Etablierung von Compliance-Prozessen im Unternehmen
- Mitarbeit an Compliance-Vereinbarungen
- Beratung der Geschäftsführung in Compliance-Fragen
- Organisation von Mitarbeiterschulungen zum Thema Compliance
- Zusammenarbeit mit den zuständigen Aufsichtsbehörden



Tipp: Verantwortung an Beauftragte delegieren

Grundsätzlich ist die Geschäftsleitung für Compliance verantwortlich. Sie kann damit verbundene Aufgaben an einen Beauftragten delegieren – den Compliance-Beauftragten. Er hat dann eine eigene Mitwirkungs-, Überwachungs- und Beratungspflicht.

Erfahren Sie im [Ratgeber zur Bestellung von Beauftragten](#), wie Sie entsprechende Pflichten und Aufgaben delegieren.

Welche Qualifikationen und Soft Skills brauchen Compliance-Beauftragte?

Es werden zwar Schulungen angeboten, bei denen man sich zum Compliance-Beauftragten ausbilden lassen kann. Allerdings gibt es keine gesetzlich vorgeschriebenen Qualifikationen, die ein Compliance-Beauftragter zwingend erfüllen muss.

Folgende **Qualifikationen** sind jedoch von Vorteil für diese Rolle:

- Rechtsverständnis und Kenntnisse von relevanten Gesetzen
- Erfahrung im Risikomanagement
- Erfahrung in der Einführung unternehmensinterner Richtlinien und Prozesse
- Verständnis von wirtschaftlichen Zusammenhängen

Als **Soft Skills** sollte ein Compliance-Beauftragter mitbringen:

- Kommunikations- und Verhandlungsgeschick
- Durchsetzungsvermögen
- Fähigkeit zur Konfliktlösung
- integratives Verhalten
- Fähigkeit zur Teamarbeit
- hohe ethische Maßstäbe

Wie sollten Unternehmen mit Compliance-Verstößen umgehen?

Arbeitgeber sollten ein klares System und klare Regeln festlegen, wie sie intern mit Verstößen gegen eine Compliance-Vereinbarung und mit Compliance-Verdachtsfällen umgehen.

Folgende Aspekte sollten insbesondere geregelt sein:

- Wo kann man einen möglichen Compliance-Verstoß betriebsintern melden?
- Wo und von wem werden Compliance-Verstöße dokumentiert?
- In welcher Form läuft die Aufarbeitung von Compliance-Verstößen ab?
- Welche arbeitsrechtlichen Konsequenzen zieht ein Compliance-Verstoß nach sich?

**Hinweis: Beschwerdestelle als Anlaufstelle bei Compliance-Verstößen**

Alle Unternehmen müssen eine Beschwerdestelle einrichten und ihren Beschäftigten bekanntmachen. Im **Ratgeber Beschwerdestelle im Betrieb einrichten** erfahren Sie, wie dort auch Hinweise zu Compliance-Verstößen bearbeitet werden können.

Praxis**Compliance im Unternehmen sicherstellen und Regelungen einhalten**

Welche Aufgaben haben Sie als Compliance-Beauftragter? Und wie gehen Sie vor, um sicherzustellen, dass

- alle gesetzlichen Regelungen in Ihrem Unternehmen von allen Beschäftigten eingehalten werden;
- Compliance-Regeln vereinbart, dokumentiert und bekannt sind, die für das ethische Verhalten des Unternehmens und seiner Beschäftigten wichtig sind.

Im folgenden Leitfaden sind die Schritte und die einzelnen Aufgaben benannt, die Sie als Compliance-Beauftragter dazu im Blick haben und erfüllen sollten.

**Leitfaden für den Compliance-Beauftragten**

Art.-Nr. 99.266.01

Datei business-wissen_9926601.docx

Microsoft Word 2016

Beispiel für die Prüfung der Compliance: das KI-Gesetz

Durch technologische und gesellschaftliche Entwicklungen und Innovationen, regeln staatliche Behörden, was Unternehmen dürfen und was nicht. Ein Beispiel sind die Regelungen, die nach und nach zum Thema Künstliche Intelligenz (KI) wichtig werden

Die Europäische Union hat dazu ein KI-Gesetz entwickelt, das hier ausführlich beschrieben ist: [Wie Unternehmen das KI-Gesetz umsetzen](#).

Was dies für Unternehmen bedeutet und wie Sie vorgehen, um die Anforderungen des KI-Gesetzes zu erfüllen, ist in dieser Vorlage zusammengestellt.



Vorbereitung auf KI-Gesetz

Art.-Nr. 99.266.02

Datei business-wissen_9926602.docx

Microsoft Word 2016

Compliance-Richtlinien – wichtige Inhalte, Themen, Bereiche

Compliance-Richtlinien dienen als unternehmensinterne Richtschnur zur Einhaltung von rechtlichen Vorgaben und ethischen Standards. Welche Aspekte sind für Unternehmen dabei besonders wichtig?

Zuletzt geändert am 24.07.2024

Von Jan Lehmann, Jan Lehmann – Redaktionsbüro



Was gehört in eine Compliance-Richtlinie?

Unabhängig von der jeweiligen Branche sollte eine Compliance-Richtlinie allgemeine **Verhaltensregeln für die Beschäftigten** festlegen.

Eine wichtige Rolle sollten die folgenden Aspekte spielen:

- Gleichbehandlung
- Diskriminierungsschutz
- Arbeitssicherheit
- Umweltschutz
- Datenschutz

Außerdem beinhalten Compliance-Richtlinien oft spezielle Anforderungen für den Umgang mit Kunden, Geschäftspartnern und Wettbewerbern.

Eine Compliance-Richtlinie beinhaltet zunächst einen allgemeinen Verhaltenskodex. Damit werden die wichtigsten Regeln benannt, die alle im Unternehmen beachten sollen.

Anschließend werden solche Aspekte genauer geregelt, die für das Unternehmen und seine Branche besondere Bedeutung haben. Oft sind das Themen, in denen es in der

Vergangenheit zu Vorfällen kam, die für das Unternehmensimage im Außenraum besonders wichtig sind oder die mit besonderen Risiken für das Unternehmen verbunden sind.

Hinweis

Compliance-Richtlinien sind spezifisch auf das Unternehmen zugeschnitten

Im Folgenden werden einige wichtige Aspekte, die branchenübergreifend in Compliance-Richtlinien aufgenommen werden, beispielhaft betrachtet.

Zu beachten ist, dass einzelne Branchen auf bestimmte Compliance-Themen mehr Wert legen. So hat zum Beispiel die Einhaltung von Arbeitsschutzvorschriften in der Baubranche eine größere Bedeutung als in einer Anwaltskanzlei. Oder: Für den Lebensmittelhandel gelten spezielle Hygienevorschriften, die in anderen Berufssparten keine Rolle spielen.

Allgemeiner Verhaltenskodex

Eine unternehmensinterne Compliance-Richtlinie sollte zunächst bestimmte grundsätzliche Verhaltensanforderungen festlegen, die an die Mitarbeiterinnen und Mitarbeiter gestellt werden. Dazu gehören zum **Beispiel**:

- Mit Kollegen und Geschäftspartnern fair und respektvoll umgehen.
- Geltende Gesetze und Regeln im zuständigen Verantwortungsbereich einhalten, zum Beispiel Arbeitssicherheitsvorschriften, Verschwiegenheitspflichten oder Datenschutzbestimmungen.
- Vermeiden von Interessenkonflikten zwischen privaten und geschäftlichen Angelegenheiten.
- Sich oder anderen keine unrechtmäßigen Vorteile verschaffen.
- Compliance-Verstöße zeitnah bei der zuständigen Stelle melden.

Führungskräfte müssen für ihren Verantwortungsbereich sicherstellen, dass die Vorgaben der Compliance-Richtlinie umgesetzt werden.

Gleichbehandlung, Gleichberechtigung, Schutz vor Diskriminierung

Im Rahmen der Compliance-Richtlinie sollte auf das Diskriminierungsverbot hingewiesen werden. Es wird klargestellt, dass Benachteiligungen aufgrund der Rasse, der ethnischen Herkunft, des Geschlechts, der Religion oder Weltanschauung, einer Behinderung, des Alters oder der sexuellen Identität verboten sind.

Das gilt:

- im Verhältnis der Arbeitskollegen untereinander,
- für Vorgesetzte und Führungskräfte gegenüber den ihnen unterstellten Mitarbeitenden und
- gegenüber Bewerberinnen und Bewerbern.

Geistiges Eigentum Dritter

Die Beschäftigten sind darauf hinzuweisen, das geistige Eigentum Dritter zu respektieren, wie zum Beispiel:

- Markenrechte
- Urheberrechte
- Patente

Gesundheit und Sicherheit am Arbeitsplatz

Führungskräfte müssen gewährleisten, dass die gesetzlichen Bestimmungen zur Arbeitssicherheit und zum Gesundheitsschutz am Arbeitsplatz eingehalten und umgesetzt werden.

Weiterhin muss jeder einzelne Mitarbeiter darauf achten, dass an seinem Arbeitsplatz die Vorgaben und Standards zur Arbeitssicherheit und zum Arbeitsschutz eingehalten werden. Dazu gibt es spezielle Unterweisungen und Schulungen, an denen alle Beschäftigten teilnehmen müssen.

Zusammenarbeit mit Kunden, Lieferanten und Geschäftspartnern

Compliance ist nicht auf das eigene Unternehmen begrenzt. Die Mitarbeitenden sollten dafür sensibilisiert werden, die geltenden Gesetze auch im Umgang mit Kunden, Lieferanten und Geschäftspartnern einzuhalten.

Ein besonderes Augenmerk sollte dabei auf die Einhaltung der gesetzlichen Bestimmungen innerhalb der Lieferkette gelegt werden, zum Beispiel im Hinblick auf die Einhaltung von Menschenrechten, das Verbot von Kinderarbeit oder den Umweltschutz.



Mehr dazu lesen Sie im [Beitrag zum Lieferkettengesetz](#).

Korruption und Bestechung

Korruption und Bestechung sind verboten. Ebenso ist es untersagt, andere bei Korruption oder Bestechung zu unterstützen oder sie dazu anzustiften.

Geschenke und persönliche Vorteile

Wichtig ist, den Umgang mit Geschenken, Einladungen oder anderen persönlichen Vorteilen zu regeln. Die Regelung sollte sich einerseits auf den Umgang mit Geschenken oder anderen Vorteilen beziehen, die von Geschäftspartnern in Aussicht gestellt werden. Andererseits sollte auch klargestellt werden, dass die eigenen Beschäftigten nur im zulässigen Rahmen Geschenke an Geschäftspartner, Lieferanten etc. verteilen.

Persönliche Vorteile dürfen dann angenommen oder in Aussicht gestellt werden, wenn dafür keine geschäftliche Gegenleistung erwartet wird.

Beispiel

Wenn ein Einkäufer des Unternehmens einen Lieferanten besucht und dort zum Mittagessen in die Kantine eingeladen wird, darf er diese Einladung annehmen.

Wird der Einkäufer kurz vor der Entscheidung zu einem Lieferantenvertrag vom Verkäufer des Lieferanten in ein Gourmet-Restaurant eingeladen und werden teure Speisen und Getränke angeboten, soll diese Einladung abgelehnt werden.

Umgang mit Wettbewerbern

Führungskräfte und Mitarbeitende sind darauf hinzuweisen, dass die wettbewerbs- und kartellrechtlichen Regelungen einzuhalten sind. Tabu sind beispielsweise Preisabsprachen unter Wettbewerbern oder die Aufteilung bestimmter Liefergebiete.

Umweltschutz und Umgang mit Ressourcen

Die Mitarbeitenden sind darauf hinzuweisen, dass sie in ihrem Arbeitsbereich für den Umweltschutz und den schonenden Umgang mit Ressourcen verantwortlich sind. Dazu zählen beispielsweise:

- der Umgang mit natürlichen Ressourcen wie Wasser, Rohstoffen oder Materialien,
- der Energieverbrauch,
- die korrekte Behandlung und Entsorgung von Abfällen.

Datenschutz

Die geltenden Datenschutzbestimmungen sind zu befolgen. Personenbezogene Daten dürfen nur erhoben und verarbeitet werden, wenn dies gesetzlich erlaubt ist.

Geschäftliche Daten und betriebliche Interna sind vertraulich zu behandeln. Zudem sind vertragliche Verschwiegenheitspflichten einzuhalten.

Der Datenschutzbeauftragte und die IT-Abteilung müssen dafür sorgen, dass nur die Mitarbeitenden im Unternehmen auf personenbezogene Daten Zugriff haben, die dazu befugt sind. Zudem sind Unterweisungen und Schulungen zum Datenschutz für alle verpflichtend.

Nutzung von Social Media, KI und Internet

Compliance-Richtlinien können auch Vorgaben zur Nutzung von Social Media, KI-Tools und Internet beinhalten. Dabei kann beispielsweise thematisiert werden,

- dass betriebsinterne Vorgaben zur privaten Internetnutzung am Arbeitsplatz eingehalten werden müssen,
- dass die Regeln zur Veröffentlichung von Video- und Bildmaterial beachtet werden müssen,
- wie sich das Unternehmen auf Social-Media-Plattformen präsentiert,
- wie und zu welchen Zwecken die Beschäftigten KI-Tools nutzen dürfen.

Umgang mit Compliance-Verstößen

Last but not least sollte eine Compliance-Richtlinie darüber Aufschluss geben, wie die Arbeitnehmer auf Compliance-Verstöße reagieren sollten und wo im Unternehmen Compliance-Verstöße gemeldet werden können.

Außerdem kann das Unternehmen erläutern, wie es mit Regelverstößen und entsprechenden Meldungen oder Hinweisen umgeht und welche Konsequenzen damit verbunden sind.



Verstöße gegen die Compliance-Richtlinien im Unternehmen sollten der internen Beschwerdestelle gemeldet werden. Lesen Sie in diesem Beitrag, **wie Sie eine Beschwerdestelle einrichten und wie diese funktioniert.**

Grundlage dafür ist das Hinweisgeberschutzgesetz. Hier erfahren Sie, **was Sie zum Hinweisgeberschutzgesetz und Whistleblowing beachten müssen.**

Praxis

Compliance-Richtlinie prüfen

Hat Ihr Unternehmen eigene Compliance-Richtlinien? Wenn ja – prüfen Sie:

- Decken die Regeln in Ihrer Compliance-Richtlinie alle Bereiche ab, die für Ihre Branche und Ihr Unternehmen wichtig sind?
- Wie werden die Regeln von den Mitarbeitenden im Alltag beachtet?
- Wo kam es in der Vergangenheit (immer wieder oder gelegentlich) zu Problemen oder Verstößen?
- Wie werden Verstöße gegen die Compliance-Regeln gemeldet?
- Wie gehen Sie in Ihrem Unternehmen mit diesen Meldungen um?
- Was passiert dann im Einzelnen – mit welchem Ergebnis oder welchen Folgen?
- Wie zufrieden sind die Geschäftsleitung, die Führungskräfte und die Beschäftigten mit der Compliance-Richtlinie insgesamt?

Compliance-Richtlinie überarbeiten oder neu erstellen

Sammeln Sie die Aspekte, die Sie in Ihrer Compliance-Richtlinie behandeln und regeln wollen. Klären Sie dazu:

- Welche Anforderungen und Erwartungen hat Ihre Geschäftsleitung?
- Welche Anforderungen und Erwartungen haben die unterschiedlichen Stakeholder Ihres Unternehmens?
- Welche besonderen gesetzlichen Vorgaben und Bestimmungen gelten für Ihr Unternehmen (national und international)?
- Was empfehlen Ihre Branchenverbände?
- Was regeln Ihre Wettbewerber in ihren jeweiligen Compliance-Richtlinien?

Auf der Grundlage der recherchierten Informationen und Antworten auf diese Fragen erstellen Sie einen Entwurf für Ihre Compliance-Richtlinie.

Diesen Entwurf stimmen Sie mit der Geschäftsleitung und gegebenenfalls mit weiteren Führungskräften ab.

Für einzelne Aspekte müssen Sie eventuell eine rechtliche Prüfung veranlassen.

Nutzen Sie für Ihre Planung und die Aufgaben zur Erstellung einer Compliance-Richtlinie diese Vorlage.



Leitfaden für den Compliance-Beauftragten

Art.-Nr. 99.266.01

Datei business-wissen_9926601.docx

Microsoft Word 2016

Liste der Inhalte für eine Compliance-Richtlinie

Nutzen Sie die folgende Vorlage als Grundlage oder Muster, um eine eigene Compliance-Richtlinie zu schreiben. Sie finden darin viele wichtigen Aspekte und mögliche Regelungsbereiche.

Ergänzen Sie die Vorlage an den Stellen, an denen Sie branchen- oder unternehmensspezifische Aspekte regeln wollen oder müssen.



Inhalte für eine Compliance-Richtlinie

Art.-Nr. 99.266.03

Datei business-wissen_9926603.docx

Microsoft Word 2016

NIS-2-Richtlinie – wer ist betroffen, was ist zu tun?

Die NIS-2 ist eine EU-Richtlinie zur Verschärfung der Sicherheitsanforderungen für Netz- und Informationssysteme. Sie soll die Cybersicherheit in der EU verbessern. Die Richtlinie umfasst strengere Meldepflichten für Sicherheitsvorfälle und führt neue Sicherheitsvorkehrungen für kritische Sektoren ein. Was schreibt die Richtlinie genau vor? Und wer ist davon betroffen?

Zuletzt geändert am 02.08.2024

Von Redaktion business-wissen.de, b-wise GmbH



Was ist die NIS-2-Richtlinie?

Die NIS-2-Richtlinie (Network and Information Security Directive 2) ist eine erweiterte und aktualisierte Version der ursprünglichen NIS-Richtlinie der Europäischen Union. Sie zielt darauf ab, die Anforderungen zur Cybersicherheit für bestimmte Sektoren zu verschärfen und die Cybersicherheitsregelungen in der EU zu harmonisieren.

Was ändert sich durch NIS-2?

Die Regeln hinsichtlich der Cybersicherheit werden strenger:

- Geltungsbereiche werden erweitert.
- Anwendungsbereiche werden ausgeweitet; auch kleine und mittlere Unternehmen sind jetzt betroffen.
- Viele Akteure (auch Kleinunternehmen) innerhalb der Lieferkette werden einbezogen.
- Sicherheitsanforderungen werden strenger.
- Die Meldepflichten werden ausgeweitet.

- Bußgelder bei Nichteinhaltung werden höher und schneller verhängt.
- Unternehmen müssen proaktiv vorgehen, um Sicherheitsprotokolle laufend zu überwachen und ihre Maßnahmen zur Abwehr von Cyberkriminalität weiter zu verbessern.

Hinweis

Hier finden Sie ausführliche Informationen

Um sich über aktuelle Änderungen oder Anpassungen zu informieren, besuchen Sie die [Website des Bundesamts für Sicherheit in der Informationstechnik](#).

Aktuell handelt es sich (noch) um einen Gesetzesentwurf. Den Entwurf mit Bearbeitungsstand Juli 2024 finden Sie auf der [Website des Bundesministeriums für Innern und für Heimat](#).

Für wen gilt die NIS-2-Richtlinie?

Ob Ihr Unternehmen von der Richtlinie betroffen ist, hängt von dessen Größe und der Zugehörigkeit zu bestimmten Sektoren ab.

Hinsichtlich der Größe sind Unternehmen betroffen, die:

- mindestens 50 Mitarbeitende beschäftigen oder
- einen Jahresumsatz von mehr als 10 Millionen EUR haben.

Kleine Unternehmen sind in der Pflicht, wenn sie kritische Tätigkeiten ausüben, die wesentliche Auswirkungen auf die öffentliche Sicherheit haben. Ist das Unternehmen Akteur in einer kritischen Lieferkette, kann es ebenfalls den Regeln der NIS-2-Richtlinie unterliegen.

Betroffene Sektoren sind:

- Energie
- Transport
- Bankwesen
- Finanzmarktinfrastrukturen
- Gesundheitswesen

- Trinkwasserversorgung
- Abwasserentsorgung
- Digitale Infrastruktur
- Öffentliche Verwaltung
- Raumfahrt
- Lebensmittelproduktion und -verteilung
- Digitale Dienste (zum Beispiel: Online-Marktplätze, Suchmaschinen, soziale Netzwerke)
- Post- und Kurierdienste
- Abfallwirtschaft
- Chemische Industrie
- Hersteller bestimmter Produkte (zum Beispiel: Medizinprodukte, Chemikalien, elektronische Geräte)
- Anbieter von IKT-Diensten (zum Beispiel: Cloud-Computing, Rechenzentren)

NIS-2 teilt diese Sektoren in zwei Gruppen ein: **wesentliche Sektoren** und **wichtige Sektoren**.

Was sind wesentliche und wichtige Sektoren?

Die Umsetzung der Sicherheitsmaßnahmen wird für beide Kategorien gleichermaßen gefordert. Allerdings unterscheiden sie sich hinsichtlich der Überprüfung und der Sanktionen erheblich:

Bei **wesentlichen Einrichtungen** erfolgen regelmäßige und gezielte Sicherheitsprüfungen („ex-ante“) sowie Stichprobenkontrollen. Der Bußgeldrahmen liegt bei maximal 10 Millionen EUR oder 2 Prozent des weltweiten Umsatzes, je nachdem welcher Betrag höher ist.

Wichtige Einrichtungen werden nur bei begründetem Verdacht („ex-post“) überprüft und vor Ort kontrolliert. Hier liegt der Bußgeldrahmen bei maximal 7 Millionen EUR oder 1,4 Prozent des weltweiten Umsatzes, je nachdem welcher Betrag höher ist.

Wesentliche Einrichtungen

Eine Einrichtung gilt als wesentlich, wenn:

- Sie eine erhebliche wirtschaftliche Bedeutung hat, etwa durch hohe Umsätze oder eine große Anzahl an Beschäftigten,
- die Einrichtung in einem Sektor tätig ist, der als kritisch für die nationale und europäische Wirtschaft und Gesellschaft angesehen wird oder
- Auswirkungen eines Ausfalls oder einer Sicherheitsverletzung in der Einrichtung erhebliche Folgen für die öffentliche Sicherheit oder den nationalen Wohlstand haben können.

Wichtige Einrichtungen

Eine Einrichtung gilt als wichtig, wenn:

- sie zwar von geringerer Größe oder wirtschaftlicher Bedeutung ist als wesentliche Einrichtungen, aber dennoch eine signifikante Rolle in ihrem Sektor spielt,
- die Einrichtung in einem Sektor tätig ist, der von hoher Bedeutung für die Aufrechterhaltung kritischer sozialer oder wirtschaftlicher Aktivitäten ist, jedoch nicht zwingend als kritisch im Sinne der wesentlichen Einrichtungen eingestuft wird oder
- die Auswirkungen eines Ausfalls oder einer Sicherheitsverletzung in der Einrichtung merkliche, aber nicht unbedingt erhebliche Folgen für die öffentliche Sicherheit oder den nationalen Wohlstand haben können.

Wesentliche Einrichtungen unterliegen strengeren regulatorischen Anforderungen und Meldepflichten als wichtige Einrichtungen. Trotzdem: Sowohl wesentliche als auch wichtige Einrichtungen sollen eng mit den nationalen Behörden zusammenarbeiten und von ihnen Unterstützung erhalten, um ihre Cyberabwehr und Cybersicherheit zu stärken.

Die genauen Klassifizierungen variieren je nach Mitgliedstaat und dessen jeweiligen gesetzlichen Bestimmungen.

Gibt es Ausnahmen?

Zwei Arten von Ausnahmen sind vorgesehen: Einerseits können Unternehmen von der NIS-2-Richtlinie betroffen sein, obwohl sie nicht zu den genannten relevanten Sektoren gehören. Andererseits können Unternehmen ausnahmsweise ausgenommen sein.

Ausgenommen sind Einrichtungen, die in den Bereichen Verteidigung, nationale oder öffentliche Sicherheit und Strafverfolgung tätig sind. Auch Zentralbanken, die Justiz und Parlamente müssen sich nicht an die Regelungen gemäß NIS-2 halten.

Von der NIS-2 betroffen, unabhängig von der Unternehmensgröße, können sein:

- Unternehmen, die „kritische Tätigkeiten“ ausführen oder
- Unternehmen, deren Tätigkeiten sich auf die öffentliche Ordnung auswirken oder
- wenn Systemrisiken bestehen.

Was unterscheidet KRITIS und NIS?

Sowohl KRITIS (Kritische Infrastrukturen) als auch NIS (Netz- und Informationssicherheit) sind Konzepte, die sich auf den Schutz von wesentlichen Infrastrukturen und die Sicherheit von Netz- und Informationssystemen konzentrieren. Sie sind eng miteinander verbunden, da viele kritische Infrastrukturen auf Netz- und Informationssysteme angewiesen sind.

Während KRITIS einen breiteren Ansatz verfolgt, der sowohl physische als auch digitale Sicherheitsaspekte umfasst, konzentriert sich NIS auf die Sicherheit von IT-Systemen und Netzwerken. Beide Ansätze ergänzen sich und tragen dazu bei, die Resilienz und Sicherheit wichtiger Dienste und Infrastrukturen zu gewährleisten.

In Deutschland ist das IT-Sicherheitsgesetz ein zentrales Gesetz für KRITIS, während die NIS-Richtlinie (EU-Richtlinie über Netz- und Informationssicherheit) den Rahmen für NIS bildet.

Die betroffenen Sektoren überschneiden sich oft. Kritische Infrastrukturen umfassen Sektoren wie Energie, Wasser, Gesundheit, Finanzen, Transport und Kommunikation, die alle auch Netz- und Informationssysteme nutzen.

Betrifft NIS-2 auch KRITIS-regulierte Unternehmen?

Wenn Ihr Unternehmen bereits KRITIS-reguliert ist, ist die NIS-2-Richtlinie dennoch relevant für Sie. Betreiber kritischer Infrastrukturen müssen nun laut NIS-2 etwa kritische Sicherheitsvorfälle an Stakeholder kommunizieren – auch an Kundinnen und Kunden, Lieferanten und die Öffentlichkeit. Neben der Meldepflicht wurde auch die Schulungspflicht erweitert.

Kurzum: Es kommen verschärfte oder zusätzliche Maßnahmen auf Sie zu, die nicht durch KRITIS abgedeckt sind.

Was unterscheidet NIS und NIS-2 ?

Das NIS-2-Umsetzungsgesetz gilt für Deutschland und wird mit leichten Abweichungen des Ist-Standes und Anpassungen, die speziell für Deutschland gelten, wahrscheinlich ab Oktober 2024 in Kraft treten. Im Vergleich zum Vorgänger (NIS-Direktive aus 2016) gibt es mehr Verpflichtungen für mehr betroffene Unternehmen, die von der EU beaufsichtigt werden.

Außerdem neu: Cybersicherheit muss laut NIS-2 auch in Lieferketten bedacht und gewahrt werden. Verstöße gegen die Richtlinie werden vergleichsweise früher und härter geahndet.

Was fordert NIS-2 von Unternehmen?

Das sind die wichtigsten Forderungen der Richtlinie NIS-2:

Mehr und strengere Sicherheitsmaßnahmen

- Unternehmen müssen umfassende Cybersicherheitsmaßnahmen implementieren, einschließlich Risikomanagement, Zugangskontrollen, Netzwerksicherheit und Verschlüsselung.
- Es müssen Vorkehrungen zur Vermeidung und Minimierung von Schäden durch Cyberangriffe getroffen werden.
- Die Cybersicherheit muss nicht nur innerhalb des Unternehmens, sondern innerhalb der gesamten Lieferkette gewährleistet sein.

Meldepflichten

- Die Registrierung beim Bundesamt für Sicherheit und Informationstechnik (BSI) ist obligatorisch.
- Unternehmen sind verpflichtet, Sicherheitsvorfälle an die zuständigen Behörden zu melden. Dies beinhaltet eine vierstufige Meldepflicht von der ersten Meldung bis zur Abschlussmeldung
- Wird ein erheblicher Sicherheitsvorfall erkannt, muss er innerhalb von 24 Stunden gemeldet werden.
- Kritische Sicherheitsvorfälle müssen außerdem relevanten Stakeholdern mitgeteilt werden; auch Kunden, Lieferanten und der Öffentlichkeit.

Risikomanagement und Kontinuitätsplanung

Unternehmen müssen Systeme zur Wiederherstellung und Notfallpläne implementieren, um den Geschäftsbetrieb im Falle eines Cybervorfalles sicherzustellen.

Schulung

Es besteht eine Schulungspflicht zum Thema Cybersicherheit.

Alle wesentlichen Stakeholder müssen in das Sicherheitstraining sowie in die Planung und Umsetzung der Maßnahmen zur Cybersicherheit einbezogen werden.

Zuständigkeiten und Verantwortlichkeiten

Die Geschäftsleitung der Unternehmen ist direkt für die Einhaltung der Richtlinie verantwortlich und muss sicherstellen, dass alle Maßnahmen zur Cybersicherheit umgesetzt und überwacht werden.



Weitere Erläuterungen, welche Maßnahmen zur Cybersicherheit Sie im Zusammenspiel mit der NIS-2-Richtlinie umsetzen sollten, lesen Sie in diesem Beitrag: [Wie Sie die NIS-2-Richtlinie umsetzen](#).

Welche Konsequenzen drohen bei Nichteinhaltung?

Unternehmen können mit erheblichen Geldstrafen belegt werden, wenn sie die Anforderungen nicht erfüllen. Diese Bußgelder richten sich nach Größe und Umsatz des Unternehmens.

Handelt es sich um eine Einrichtung aus dem wesentlichen Sektor, können Bußgelder in Millionenhöhe fällig werden. Die genaue Höhe der Strafe hängt in vielen Fällen auch vom Jahresumsatz des Unternehmens ab.

Zusätzlich können Behörden Maßnahmen ergreifen, indem sie etwa anordnen, dass die Cybersicherheitsmaßnahmen des Unternehmens verbessert oder ergänzt werden.

Die Geschäftsleitung haftet bei Verstößen oder Nichteinhaltung.

Unternehmen sollten aber auch **aus eigenem Interesse** für die Sicherheit ihrer IT-Systeme sorgen. Denn Angriffe können dem Geschäft erhebliche wirtschaftliche Schäden verursachen. Unternehmen sollten deshalb geeignete Sicherheitsmaßnahmen umsetzen und kontinuierliches Risikomanagement betreiben.

Kommt es zu einem Vorfall, kann das den Ruf eines Unternehmens erheblich schädigen und das Vertrauen der Kunden und Partner negativ beeinträchtigen.

Praxis

Anforderungen der NIS-2-Richtlinie erfüllen

In der folgenden Vorlage zur Vorbereitung, Planung und Umsetzung zur Richtlinie NIS-2 finden Sie Details zu den notwendigen Maßnahmen. Außerdem erhalten Sie Empfehlungen und Tipps zur systematischen Umsetzung.



Maßnahmen zur NIS-2-Richtlinie

Art.-Nr. 99.266.05

Datei business-wissen_9926605.docx

Microsoft Word 2016

Risiko bewerten

Nutzen Sie die folgenden Vorlagen zur Risikobewertung:



Risikobewertung und Maßnahmen planen

Art.-Nr. 99.045.20

Datei business-wissen_9904520.xlsx
Microsoft Excel 2016



Risikomatrix mit 3x3-Felder-Diagramm für Schadenshöhe und Eintritt

Art.-Nr. 99.045.15

Datei business-wissen_9904515.xlsx
Microsoft Excel 2016

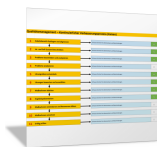


Lesen Sie in diesem Beitrag, was zum **Risikomanagement** gehört und welche Methoden dabei eingesetzt werden.

Maßnahmen zur Cybersicherheit verbessern

Eine wesentliche Anforderung, die sich aus der NIS-2-Richtlinie ergibt, ist die kontinuierliche Verbesserung der Maßnahmen zur Cybersicherheit.

Nutzen Sie die folgende Vorlage, um die Methode Kaizen zur kontinuierlichen Verbesserung anzuwenden. Planen Sie, welche Maßnahmen Sie bei jedem Schritt durchführen wollen und wie weit Sie mit der Umsetzung jeweils sind.



Ablauf Kontinuierlicher Verbesserungsprozess (Kaizen-Prozess)

Art.-Nr. 99.129.37

Datei business-wissen_9912937.xlsx
Microsoft Excel 2016

Betriebsbeauftragte: Welche müssen bestellt werden?

Unternehmen bestimmter Größen und Branchen sind gesetzlich dazu verpflichtet, Betriebsbeauftragte zu benennen, darunter Umwelt-, Immissionsschutz- und Datenschutzbeauftragte. Häufig müssen diese bei den zuständigen Behörden gemeldet werden. Welche Beauftragten für Ihr Unternehmen relevant sind und welche Meldepflichten jeweils bestehen, erfahren Sie in diesem Beitrag.

Zuletzt geändert am 15.08.2024

Von Redaktion business-wissen.de, b-wise GmbH



Wozu braucht man Betriebsbeauftragte?

Der Gesetzgeber hat Unternehmen eine Vielzahl von Pflichten auferlegt. Die Unternehmen sind verantwortlich dafür, die Einhaltung der geltenden Vorschriften sowie behördlicher Auflagen zu gewährleisten. Dafür werden Betriebsbeauftragte bestellt.

Sowohl externe Personen als auch Mitarbeitende können bestellt werden. Bestellte Personen:

- überwachen Prozesse,
- beraten das Management,
- schulen Mitarbeitende und
- melden relevante Informationen an Behörden.

Die Bestellung von Betriebsbeauftragten ist teilweise gesetzlich vorgeschrieben.

In einem Betrieb können mehrere Betriebsbeauftragte tätig sein. Häufig ist es auch möglich, dass ein Betriebsbeauftragter mehrere Aufgaben in Personalunion übernimmt.



Betriebsbeauftragte auswählen und bestellen

Wie Sie betriebliche Beauftragte auswählen, bestellen und unterstützen, erläutert der Expertenbeitrag **Beauftragte für betriebliche Aufgaben bestellen**.

Sicherheitsbeauftragter

Unternehmen sollen einen Sicherheitsbeauftragten benennen, um die Sicherheit und den Gesundheitsschutz der Mitarbeitenden zu gewährleisten. Bei bestimmten Branchen und Betriebsgrößen ist zudem die Benennung einer Fachkraft für Arbeitssicherheit erforderlich.

Unternehmen mit über 20 Mitarbeitenden müssen einen Sicherheitsbeauftragten benennen (§ 22 SGB VII). Wie viele Beauftragte gestellt werden müssen, legen die Unfallversicherungsträger für den Betrieb fest. Meist hängt dies ab von:

- Anzahl der Beschäftigten
- zeitliche Nähe (der Gefahr) zu den Beschäftigten
- räumliche Nähe (der Gefahr) zu den Beschäftigten
- fachliche Nähe (der Gefahr) zu den Beschäftigten
- Art der Unfall- und Gesundheitsgefahren im Unternehmen

Meldepflicht:

Sicherheitsbeauftragte müssen in der Regel nicht gesondert bei einer Behörde gemeldet werden. Es besteht jedoch eine interne Dokumentationspflicht im Unternehmen.

Kontrolle:

Die Einhaltung dieser Verpflichtungen wird durch die Berufsgenossenschaften oder das Gewerbeaufsichtsamt im Rahmen von Audits oder Betriebsbesichtigungen überprüft.

Ersthelfer

Sie als Arbeitgeber müssen gemäß § 10 ArbSchG sicherstellen, dass im Betrieb bei einem Notfall Erste Hilfe geleistet werden kann.

Sobald sich auf dem Firmengelände mindestens zwei versicherte Mitarbeitende gleichzeitig aufhalten, müssen Unternehmen einen betrieblichen Ersthelfer benennen und so schulen, dass er seinen Aufgaben im Notfall gerecht werden kann.

Es besteht keine Meldepflicht.



Im Beitrag **Was Sie zum Ersthelfer im Betrieb gewährleisten müssen** erfahren Sie, welche Aufgaben der Ersthelfer hat, wie Sie ihn dazu befähigen und wie viele Ersthelfer Sie überhaupt benötigen.

Betriebsarzt

Ein Betriebsarzt ist für jeden Arbeitgeber Pflicht; das gilt unabhängig von der Anzahl der Mitarbeitenden. Regeln zur Bestellung, Aufgaben und Anforderungen an Betriebsärzte werden durch das ASiG, die DGUV Vorschrift 2 und weitere gesetzliche Regelungen festgelegt.

Meldepflicht:

Unternehmen sind verpflichtet, die Bestellung eines Betriebsarztes und einer Fachkraft für Arbeitssicherheit der zuständigen Aufsichtsbehörde zu melden. Dies erfolgt in der Regel durch Mitteilung an die zuständige Berufsgenossenschaft oder die Arbeitsschutzbehörde.

Kontrolle:

Die Einhaltung der Vorschriften wird von den staatlichen Arbeitsschutzbehörden sowie von den Berufsgenossenschaften kontrolliert. Diese Behörden führen regelmäßig Betriebsbesichtigungen durch und können die Dokumentation des Unternehmens einsehen.

Arbeitsschutzbeauftragter

In Betrieben mit mehr als 20 wahlberechtigten Arbeitnehmern kann der Betriebsrat verlangen, dass der Arbeitgeber einen Arbeitsschutzbeauftragten oder eine Person zur Wahrnehmung von Arbeitgeberpflichten benennt (§ 80 Abs. 1 Nr. 1 BetrVG).

Es gibt keine gesetzliche Meldepflicht.

Datenschutzbeauftragter

Unternehmen, die personenbezogene Daten automatisiert verarbeiten, müssen einen Datenschutzbeauftragten benennen, wenn regelmäßig mindestens 20 Personen mit personenbezogenen Daten arbeiten (§ 38 BDSG).

Unternehmen, die eine Datenschutz-Folgeabschätzung durchführen müssen oder die mit personenbezogenen Daten handeln, brauchen immer einen Datenschutzbeauftragten.

Meldepflicht:

Unternehmen, die nach der Datenschutz-Grundverordnung (DSGVO) und dem Bundesdatenschutzgesetz (BDSG) verpflichtet sind, einen Datenschutzbeauftragten zu benennen, müssen diesen der zuständigen Aufsichtsbehörde (in der Regel das jeweilige Landesamt für Datenschutz) melden.

Kontrolle:

Die Aufsichtsbehörden können im Rahmen von Datenschutzprüfungen kontrollieren, ob ein Datenschutzbeauftragter benannt wurde und ob dieser ordnungsgemäß tätig ist.



Im Beitrag [Datenschutz: Was Führungskräfte beachten und veranlassen müssen](#) erfahren Sie mehr über die Rechte und Pflichten zum Datenschutz in Unternehmen.

Geldwäschebeauftragter

Unternehmen, die unter das Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz) fallen, müssen einen Geldwäschebeauftragten benennen, der für die Einhaltung der geldwäscherechtlichen Vorschriften verantwortlich ist (§ 7 GwG). Dazu gehören zum Beispiel Finanzdienstleister und Immobilienmakler.

Meldepflicht:

Die Benennung eines Geldwäschebeauftragten muss der zuständigen Aufsichtsbehörde gemeldet werden. Für Banken und Finanzdienstleister ist die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) zuständig. Für andere Branchen können es auch andere Aufsichtsbehörden sein, wie die Industrie- und Handelskammern (IHK) oder Landesaufsichtsbehörden.

Kontrolle:

Die Aufsichtsbehörden überwachen die Einhaltung der Meldepflicht und können bei Verstößen gegen das Geldwäschegesetz Bußgelder verhängen. Es ist daher wichtig, dass die Benennung des Geldwäschebeauftragten fristgerecht und korrekt erfolgt.

Immissionsschutzbeauftragter

Betreiber von Anlagen, die unter den Anwendungsbereich des Bundesimmissionsschutzgesetzes fallen, müssen einen Immissionsschutzbeauftragten benennen (§ 53 Absatz 1 BImSchG):

... sofern dies im Hinblick auf die Art oder die Größe der Anlagen wegen der

- 1. von den Anlagen ausgehenden Emissionen,*
 - 2. technischen Probleme der Emissionsbegrenzung oder*
 - 3. Eignung der Erzeugnisse, bei bestimmungsgemäßer Verwendung schädliche Umwelteinwirkungen durch Luftverunreinigungen, Geräusche oder Erschütterungen hervorzurufen,*
- erforderlich ist.*

Meldepflicht:

In Betrieben, die nach dem Bundesimmissionsschutzgesetz (BImSchG) genehmigungspflichtig sind, muss ein Immissionsschutzbeauftragter benannt und der Behörde gemeldet werden.

Kontrolle:

Die zuständige Immissionsschutzbehörde prüft die Einhaltung der Vorgaben durch regelmäßige Kontrollen und Betriebsbesichtigungen.

Gewässerschutzbeauftragter

Unternehmen, die wassergefährdende Stoffe handhaben, müssen einen Gewässerschutzbeauftragten benennen (§ 64 WHG), wenn sie an einem Tag mehr als 750 Kubikmeter Abwasser einleiten dürfen. Unter bestimmten Umständen können die Behörden unabhängig davon anordnen, dass einer oder mehrere Beauftragte zu bestellen sind.

Meldepflicht:

Diese Beauftragten müssen in der Regel bei der zuständigen Überwachungsbehörde (häufig Umweltamt oder Bezirksregierung) gemeldet werden. Die Meldung umfasst in der Regel die Kontaktdaten des Beauftragten und die Bestellung.

Kontrolle:

Die zuständige Behörde kann im Rahmen von Überwachungen und Betriebsbesichtigungen prüfen, ob die Bestellung des Beauftragten erfolgt ist und ob der Beauftragte seine Pflichten erfüllt. Zudem können entsprechende Dokumentationen und Bestellurkunden angefordert werden.

Gefahrstoffbeauftragter

Für bestimmte Tätigkeiten mit gefährlichen Stoffen müssen Unternehmen einen Gefahrstoffbeauftragten ernennen, der für die Sicherheit bei der Handhabung dieser Stoffe zuständig ist (§ 7 GefStoffV).

Meldepflicht:

Die Benennung muss häufig innerhalb des Unternehmens dokumentiert und gegebenenfalls der zuständigen Behörde gemeldet werden.

Kontrolle:

Die Einhaltung der Vorschriften wird durch das Gewerbeaufsichtsamt oder die Berufsgenossenschaft überwacht. Im Rahmen von Betriebsbesichtigungen wird geprüft, ob ein Gefahrstoffbeauftragter benannt und ordnungsgemäß tätig ist.

Brandschutzbeauftragter

Nicht jedes Unternehmen muss einen Brandschutzbeauftragten bestellen. Die Pflicht besteht, wenn:

- laut Gefährdungsbeurteilung ein erhöhtes Brandrisiko besteht,
- eine Verkaufsfläche von mehr als 2000 Quadratmeter vorhanden ist,
- der Gebäudeversicherer dies fordert oder
- die Bauordnung oder die Industriebaurichtlinie dies vorschreiben.

Geregelt wird diese Pflicht in § 10 ArbSchG.

Meldepflicht:

Diese Bestellung muss in der Regel nicht bei einer Behörde gemeldet werden, jedoch intern dokumentiert sein.

Kontrolle:

Die Einhaltung der Brandschutzbestimmungen wird durch die Feuerwehr oder das Bauamt im Rahmen von Begehungen und Prüfungen kontrolliert.



Im Beitrag [Vorschriften und Maßnahmen zum betrieblichen Brandschutz](#) erfahren Sie, welche Brandschutzmaßnahmen vorgeschrieben sind und wie Ihr Unternehmen seinen bestehenden gesetzlichen Pflichten nachkommen.

Evakuierungsbeauftragter

Grundsätzlich sind Unternehmen nicht verpflichtet, einen Evakuierungshelfer zu bestellen. Jedoch muss laut § 10 Arbeitsschutzgesetz (ArbSchG) gesichert sein, dass eine sichere und geordnete Evakuierung im Notfall gewährleistet ist.

Manche Arbeitgeber bestimmen und schulen zu diesem Zweck freiwillig einen Evakuierungsbeauftragten.

Gleichstellungsbeauftragter

Private Unternehmen sind nicht dazu verpflichtet, einen Gleichstellungsbeauftragten zu stellen. Nur Behörden, soziale Einrichtungen und Gemeinden, in denen mindestens 100 Mitarbeitende tätig sind, müssen eine Person benennen, die sich unter anderem für die Gleichstellung von Beschäftigten unterschiedlicher Geschlechter einsetzt.

Inklusionsbeauftragter

Gemäß § 181 SGB IX müssen alle Arbeitgeber in Deutschland einen oder mehrere Inklusionsbeauftragten bestellen, wenn sie schwerbehinderte Menschen beschäftigen (oder beschäftigen müssen; siehe § 154 SGB IX).

Meldepflicht:

In Deutschland muss der Schwerbehindertenbeauftragte beim zuständigen Integrationsamt gemeldet werden. Dies erfolgt in der Regel durch eine formlose Mitteilung, die den Namen und die Kontaktdaten des Beauftragten sowie den Arbeitgeber umfasst.

Kontrolle:

Der Betriebsrat oder Personalrat hat das Recht und die Pflicht, darauf zu achten, dass die gesetzlichen Vorgaben in Bezug auf die Beschäftigung von Menschen mit Behinderungen eingehalten werden. Außerdem kann das Integrationsamt oder die Agentur für Arbeit prüfen, ob ein Inklusionsbeauftragter vorhanden ist.

Menschenrechtsbeauftragter

Unternehmen mit einer Niederlassung oder einem Zweig in Deutschland mit mehr als 1000 Mitarbeitenden müssen laut deutschem Lieferkettengesetz einen Menschenrechtsbeauftragten benennen.

Es gibt keine Meldepflicht.



Welche Aufgaben der Menschenrechtsbeauftragte hat und worauf Unternehmen bei seiner Bestellung achten, erfahren Sie im Beitrag **Menschenrechtsbeauftragter gemäß Lieferkettengesetz**.

Compliance-Beauftragter

Kein Unternehmen ist dazu verpflichtet, einen Compliance-Beauftragten zu bestellen. Gerade große Unternehmen bestellen trotzdem häufig einen sogenannten „Compliance Officer“. Er soll rechtliche Risiken identifizieren, einordnen und dafür sorgen, dass alle Gesetze im Unternehmen eingehalten und die Risiken vermindert werden.

CE-Beauftragter oder Bevollmächtigter für Produktsicherheit

Unternehmen können Bevollmächtigte bestellen, die sich um die Produktsicherheit kümmern und die dafür sorgen, dass die rechtlichen Vorgaben dazu eingehalten werden. Sie sind gleichzeitig Ansprechpartner für staatliche Aufsichtsbehörden.

Die rechtliche Grundlage dazu bilden:

- Maschinenrichtlinie 2006/42/EG
- Produktsicherheitsgesetz (ProdSG)
- Verordnung (EU) 2023/988 zur Produktsicherheit

Es gibt keine gesetzlichen Anforderungen an die Fachkunde des Beauftragten; lediglich technischer sowie rechtlicher Sachverstand und Kenntnisse zur Produkthaftung und Umweltrecht sollten vorhanden sein.

Es besteht keine Pflicht, einen CE-Beauftragten oder entsprechende Bevollmächtigte zu bestellen. Wenn es diese gibt, sollten Sie den jeweils zuständigen Behörden benannt werden, da sie die zentralen Ansprechpartner für die Behörden sind.

Die Bevollmächtigten müssen auf Verlangen der Behörde ein Dokument des Unternehmens vorlegen, das ihre Vollmachten bestätigt.

Beauftragter für Medizinproduktesicherheit

Eine zentrale Anforderung der Medizinprodukte-Betreiberverordnung (MPBetreibV) besteht darin, in Gesundheitseinrichtungen mit regelmäßig mehr als 20 Beschäftigten einen Beauftragten für Medizinproduktesicherheit zu benennen.

Das Bundesamt für Arzneimittel und Medizinprodukte beantwortet die häufigsten Fragen vonseiten der Unternehmen verständlich und knapp auf der Webseite „[Weitere Informationen für Beauftragte für Medizinproduktesicherheit](#)“.

Meldepflicht:

Unternehmen, die Medizinprodukte herstellen oder vertreiben, müssen den Beauftragten bei der zuständigen Behörde melden, meist dem Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM).

Prüfung:

Die Überwachung und Prüfung erfolgt durch das BfArM im Rahmen von Audits und Inspektionen.

Exportkontrollbeauftragter

Es gibt kein Gesetz, welches explizit und allgemeingültig fordert, einen Exportkontrollbeauftragten zu bestellen. Die Regelungen zur Exportkontrolle und die Verantwortlichkeiten in Unternehmen ergeben sich jedoch aus einer Kombination mehrerer Gesetze und Verordnungen:

- Außenwirtschaftsgesetz (AWG)
Legt fest, dass Unternehmen ihre Exportvorgänge im Einklang mit den gesetzlichen Bestimmungen überwachen müssen. Die Pflicht zur Bestellung eines Exportkontrollbeauftragten ergibt sich indirekt aus der Pflicht zur Einhaltung der Exportkontrollvorschriften.
- Außenwirtschaftsverordnung (AWV)
Auch hier gibt es keine direkte Vorgabe zur Bestellung eines Exportkontrollbeauftragten, aber Unternehmen sind verpflichtet, interne Kontrollmaßnahmen zu etablieren, um die Einhaltung der Vorschriften zu gewährleisten.
- Kriegswaffenkontrollgesetz (KWKG)
Unternehmen, die mit Rüstungsgütern handeln, unterliegen strengen Kontrollen und haben umfangreiche Pflichten, die ebenfalls die Notwendigkeit eines verantwortlichen Ansprechpartners – wie eines Exportkontrollbeauftragten – implizieren.

Meldepflicht:

Die Bestellung ist nicht zwingend bei einer Behörde zu melden, muss jedoch im Unternehmen dokumentiert sein.

Kontrolle:

Die Einhaltung der Exportkontrollvorschriften wird durch die zuständige Behörde (zum Beispiel: Bundesamt für Wirtschaft und Ausfuhrkontrolle) geprüft. Bei Audits kann die Benennung und die Tätigkeit des Beauftragten überprüft werden.

Sonderfälle: Umgang mit Gefahrstoffen

Da die folgenden Beauftragten lediglich von Unternehmen in speziellen Branchen gestellt werden müssen, werden sie nur der Vollständigkeit halber aufgeführt. Falls in Ihrem Unternehmen mit Gefahrstoffen umgegangen wird, sollten Sie sich zu den folgenden Beauftragten informieren; nicht alle sind verpflichtend zu bestellen:

- Asbest-Sachkundiger
- Begasungsleiter
- Beauftragter für biologische Sicherheit
- Entsorgungsverantwortlicher
- Explosionsschutzbeauftragter
- Sprengstoffbeauftragter
- Strahlenschutzbeauftragter

Diese Beauftragten müssen in der Regel bei der zuständigen Überwachungsbehörde (häufig Umweltamt oder Bezirksregierung) gemeldet werden. Die Meldung umfasst in der Regel die Kontaktdaten des Beauftragten und die Bestellung.

Praxis

Bestellung von Beauftragten planen und sicherstellen

Nutzen Sie die folgende Vorlage (Ablaufplan), um betriebliche Beauftragte auszuwählen, zu bestellen und zu unterstützen.

**Vorgehen zur Bestellung von betrieblich Beauftragten**

Art.-Nr. 99.245.02

Datei business-wissen_9924502.docx

Microsoft Word 2016

Grundlage dafür ist: Prüfen Sie anhand der geltenden Gesetze und Verordnungen, welche Betriebsbeauftragten Sie zwingend bestellen müssen.

Ein Beispiel: Gemäß § 181 SGB IX müssen Arbeitgeber einen Inklusionsbeauftragten bestellen, der den Arbeitgeber in Angelegenheiten schwerbehinderter Menschen verantwortlich vertritt.

Klären Sie darüber hinaus, welche Beauftragten, die nicht gesetzlich vorgeschrieben sind, für Ihren Betrieb sinnvoll sind. Dort können dann entsprechende Aufgaben gebündelt und verantwortlich wahrgenommen werden.

Liste zu Beauftragten erstellen

Erstellen Sie eine Liste oder Übersicht, welche Betriebsbeauftragten Sie in Ihrem Unternehmen benötigen. Daraus sollte hervorgehen:

- die Funktion des Beauftragten; wofür er bestellt ist
- auf Basis welcher Rechtsgrundlage die Bestellung erfolgt
- ab welchem Zeitpunkt der Beauftragte seine Tätigkeit aufnehmen soll

Erstellen Sie zusätzlich für jeden Beauftragten eine Übersicht mit dessen wesentlichen Aufgaben.

Nutzen Sie dafür die folgende Vorlage.



Liste der Betriebsbeauftragten

Art.-Nr. 99.245.03

Datei business-wissen_9924503.docx

Microsoft Word 2016

Kriterien-Liste für die Auswahl der Betriebsbeauftragten zusammenstellen

Erstellen Sie eine Kriterien-Liste, anhand der Sie die beauftragte Person auswählen:

- Welche persönlichen Eigenschaften sollte der Beauftragte für seine Tätigkeit mitbringen?
- Welche Fachkompetenzen muss er haben?

- Sind bestimmte Qualifikationen und Zertifikate notwendig oder gesetzlich vorgeschrieben?
- Inwiefern kann die notwendige Qualifikation durch eine Weiterbildung erreicht werden?

Halten Sie Ihre Kriterien in der folgenden Vorlage fest.



Liste der Kriterien für die Auswahl der Beauftragten

Art.-Nr. 99.245.04
Datei business-wissen_9924504.docx
Microsoft Word 2016

Bestellung von Beauftragten schriftlich dokumentieren

Die Bestellung eines Beauftragten sollte aus Gründen der Rechtssicherheit unbedingt schriftlich erfolgen. Halten Sie dabei fest:

- Name der beauftragten Person
- Name und Anschrift der Firma
- Titel und Funktion der beauftragten Person
- Beschreibung der Aufgaben oder Tätigkeiten, welche die beauftragte Person übernehmen soll
- Unterschrift durch den Besteller (meist die Geschäftsleitung) und den Beauftragten

Wenn für das Tätigkeitsfeld bestimmte Qualifikationen notwendig sind, sind diese Qualifikationen vom Beauftragten nachzuweisen und die Nachweise vom Arbeitgeber zu archivieren.

Nutzen Sie für Ihre Bestellung von Beauftragten die folgende Mustervorlage.



Schriftliche Bestellung eines Betriebsbeauftragten (Muster)

Art.-Nr. 99.245.05
Datei business-wissen_9924505.docx
Microsoft Word 2016

Empfehlungen aus dem Management-Handbuch

Beschwerdestelle

Worauf Sie bei der Einrichtung einer Beschwerdestelle in Ihrem Unternehmen achten und welche Pflichten Sie gemäß AGG dabei erfüllen müssen. Mit Vorlagen zu den Aufgaben der Beschwerdestelle und zur Erfassung und Bearbeitung eingehender Beschwerden.

<https://www.business-wissen.de/id/kapitel/256/>

Pflichten der Geschäftsleitung

Arbeitgeber haben rechtliche Pflichten gegenüber Mitarbeitenden und anderen Stakeholdern. Was muss die Unternehmensleitung konkret tun, um die Verkehrssicherungspflicht und die Pflicht zur Bestellung von Beauftragten zu erfüllen?

<https://www.business-wissen.de/id/kapitel/245/>

Nachhaltigkeitsbericht

Worum es bei der Nachhaltigkeitsberichterstattung geht, was EU-weit vorgeschrieben ist und was der Nachhaltigkeitsbericht beinhalten muss. Mit einer Anleitung zum Erstellen des Nachhaltigkeitsberichts.

<https://www.business-wissen.de/id/kapitel/260/>

Whistleblowing

Was genau mit dem Hinweisgeberschutzgesetz (HinSchG) geschützt wird und was Unternehmen deshalb beachten, umsetzen und sicherstellen müssen. Mit einer Vorlage zur Maßnahmenplanung und einem Formular für eine Meldung.

<https://www.business-wissen.de/id/kapitel/255/>

Nutzen Sie als
Premium-Mitglied
alle
Handbuch-Kapitel
mit mehr als
3.000 Checklisten und Excel-Vorlagen

Jetzt anmelden

www.business-wissen.de/anmelden/

Autoren

Jan Lehmann



Jan Lehmann ist Freier Journalist und Online-Redakteur für unterschiedliche Fachmedien. Sein inhaltlicher Schwerpunkt: Personalthemen, insbesondere Arbeitsrecht.

E-Mail jl@lehmann-redaktion.de

Anschrift Jan Lehmann – Redaktionsbüro
Vogesenstraße 3
77781 Biberach/Baden
Deutschland

Web <https://www.lehmann-redaktion.de>

Redaktion business-wissen.de

E-Mail redaktion@business-wissen.de

Telefon +49 721 18397-0

Anschrift b-wise GmbH
Bismarckstr. 21
76133 Karlsruhe
Deutschland

Web <https://www.business-wissen.de>

Impressum

b-wise GmbH
Bismarckstraße 21
76133 Karlsruhe
DEUTSCHLAND

service@business-wissen.de

Telefon +49 721 18397-0

Copyright 2025, b-wise GmbH, All Rights Reserved