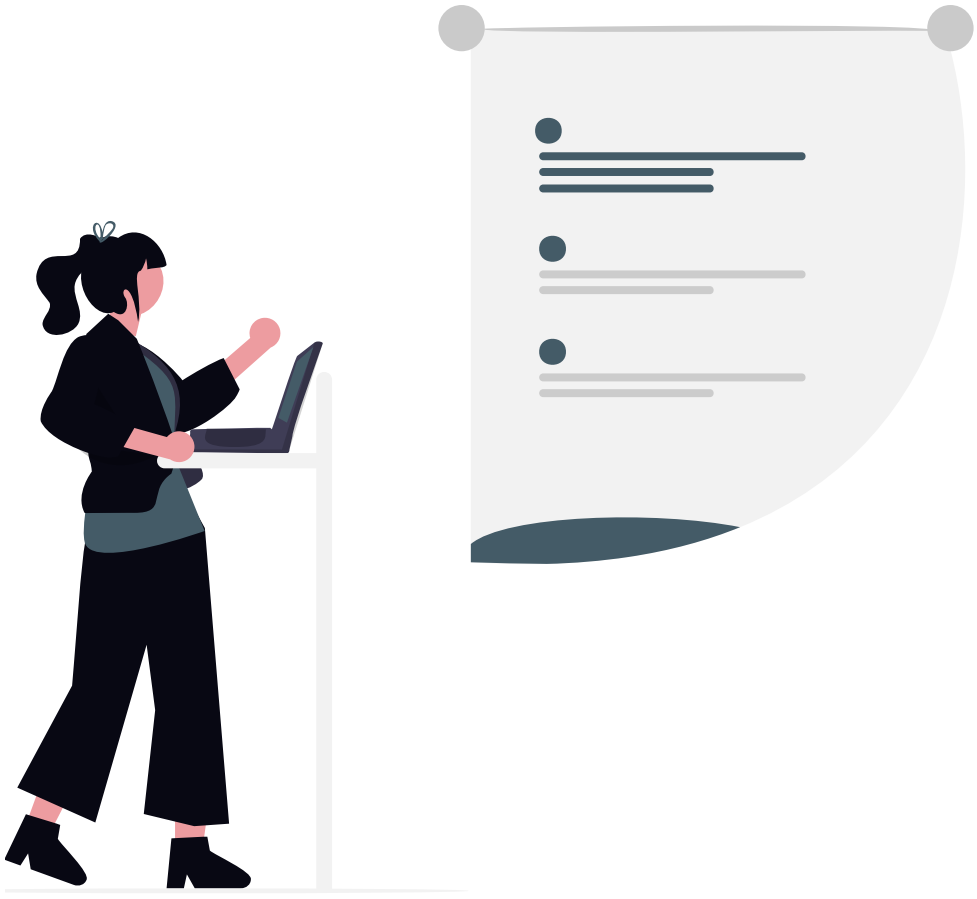
Muster Berater GmbH

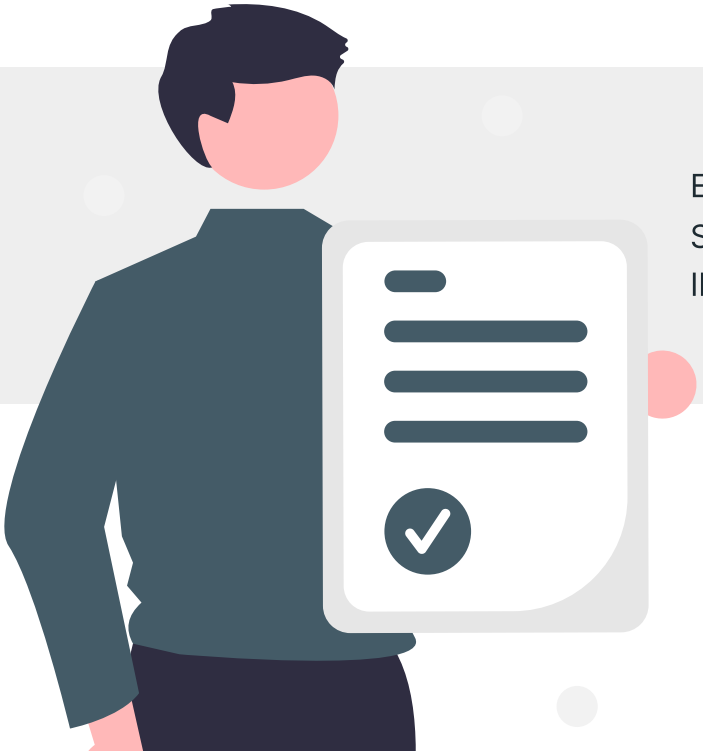
DPMS in der Praxis: In 8 Schritten ein ISMS aufbauen



Stand: Januar 2026

DPMS in der Praxis: In 8 Schritten ein ISMS aufbauen

Muster Berater GmbH



Entdecken Sie, wie Sie mit moderner Software Schritt für Schritt ein Managementsystem für Ihre Informationssicherheit aufbauen.

DPMS in der Praxis: In 8 Schritten ein ISMS aufbauen

Mit unserer Compliance-Software DPMS geben wir Ihnen ein praxisbewährtes Werkzeug an die Hand, mit dem Sie ein Managementsystem für Ihre Informations- und Cybersicherheit aufbauen und pflegen.

Was ist ein ISMS?

Ein ISMS ist ein strukturiertes System, mit dem Unternehmen sämtliche Informationen, die sie verarbeiten, wirksam schützen. Ziel ist es, Risiken frühzeitig zu erkennen, Sicherheitsmaßnahmen gezielt umzusetzen und die IT-Sicherheit im Unternehmen laufend zu verbessern. Typischerweise orientiert sich der Aufbau eines ISMS an anerkannten Standards wie der ISO/IEC 27001. Ein ISMS besteht aber nicht nur aus technischen Maßnahmen. Es berücksichtigt auch organisatorische Fragen:

- Wer hat Zugriff auf welche Daten?
- Was passiert im Notfall?
- Welche IT-Systeme sind besonders schützenswert?

Ein ISMS ist also kein Projekt für die IT-Abteilung allein – es betrifft das gesamte Unternehmen und verbessert die Zusammenarbeit zwischen IT, Geschäftsleitung, Datenschutz, Personal und weiteren Fachabteilungen. Wir geben Ihnen im Folgenden einen Überblick, wie Sie ein ISMS aufbauen – Schritt für Schritt unterstützt durch unsere Compliance-Software DPMS.

DPMS in der Praxis: In 8 Schritten ein ISMS aufbauen

Muster Berater GmbH

1. Anforderungskatalog für Ihr Managementsystem anlegen

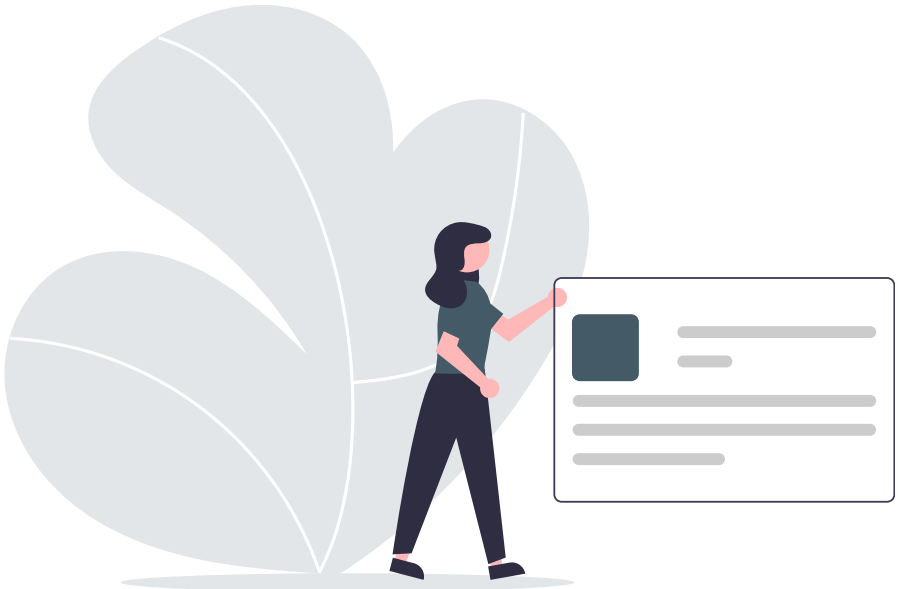
Im ersten Schritt legen Sie einen strukturierten Anforderungskatalog an, der sämtliche Anforderungen des gewünschten Managementsystems enthält – zum Beispiel gemäß ISO/IEC 27001. Im DPMS stehen dafür zwei Möglichkeiten zur Verfügung:

- Eigene Kataloge anlegen bzw. importieren (z. B. aus einer Excel-Vorlage)
- Vorkonfigurierte Kataloge aus einer Vorlage (sofern vorhanden) nutzen

Der Katalog dient als zentrale Arbeitsgrundlage zur Umsetzung der entsprechenden Norm. Er ermöglicht es Ihnen, den Umsetzungsstand systematisch zu erfassen und den Reifegrad zu bewerten. Ausstehende Umsetzungsschritte können Sie direkt als Maßnahme anlegen und einem Verantwortlichen zuteilen.

→ Umsetzung im DPMS mit dem Modul „Managementsysteme“

- Behalten Sie den aktuellen Fortschritt der Normerfüllung immer im Blick
- Erstellen und verwalten Sie Maßnahmen und zugehörige Aufgaben
- Erstellen Sie Online-Fragebögen (Selbst-Audits) für die Zusammenarbeit mit Kollegen oder externen Partnern
- Report: Generieren Sie mit einem Klick die Erklärung zur Anwendbarkeit (Statement of Applicability – SoA)



2. Geltungsbereich festlegen

Definieren Sie, welche Organisationseinheiten Ihr ISMS abdecken soll und halten Sie dies in einem Leitdokument fest (Definition des Anwendungsbereichs bzw. Scope). Im Anschluss dokumentieren Sie alle für diesen Anwendungsbereich relevanten Standorte, Systeme, Geräte, Prozesse und weiteren Unternehmenswerte – die Assets.

Systemlandschaft und Applikationen dokumentieren

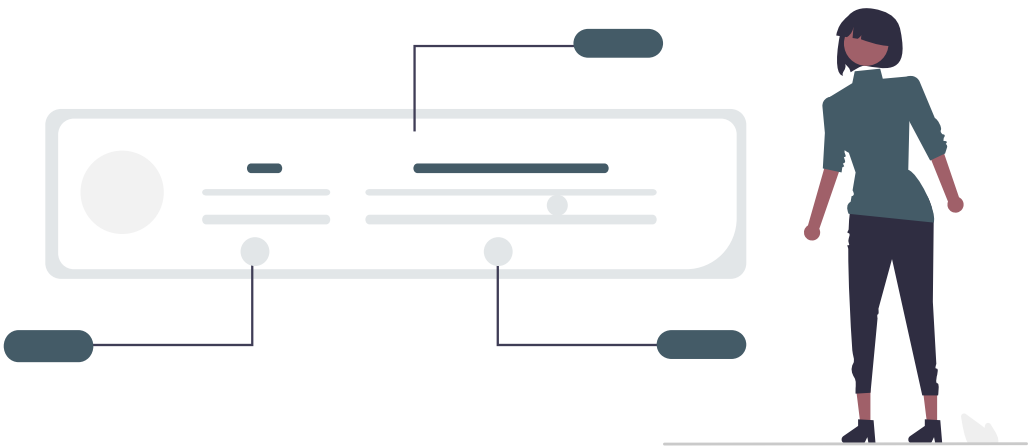
Im DPMS können Sie Ihre gesamte Systemlandschaft abbilden. Legen Sie zunächst Standorte an. Anschließend fügen Sie Geräte und Systeme hinzu. Zudem können Sie Software-Anwendungen dokumentieren.

→ Umsetzung im DPMS mit dem Modul „Systemlandschaft“

- Verwalten Sie sämtliche Geräte – inkl. digitalem Übergabeprotokoll bei der Ausgabe an Ihre Beschäftigten
- Behalten Sie mit der digitalen Besucherregistrierung im Blick, wer Ihr Unternehmen besucht (Anmeldung/Abmeldung)
- Fügen Sie Gerätegruppen hinzu wie Netzwerk, Backup oder Monitoring

→ Umsetzung im DPMS mit dem Modul „Applikationen“

- Dokumentieren Sie den aktuellen Softwarebestand
- Definieren Sie, welche Abteilungen auf welche Software zugreifen dürfen



DPMS in der Praxis: In 8 Schritten ein ISMS aufbauen

Muster Berater GmbH

Prozesse definieren

Es bietet sich insbesondere für das betriebliche Kontinuitätsmanagement an, die Kernprozesse Ihres Unternehmens zu modellieren. Die hierbei eingesetzten IT-Systeme und Geräte sind besonders wichtig für das Tagesgeschäft. Auf dieser Basis fällt die spätere Betrachtung in Bezug auf tolerierbare Ausfallzeiten und Schutzbedarf leichter. Zusätzlich sollten Sie wichtige Verfahrensschritte als Prozesse anlegen, um beispielsweise Vorfälle zu melden und zu behandeln (Notfallprozesse).

→ Umsetzung im DPMS mit dem Modul „Prozesse“

- Modellieren Sie Ihre relevanten Geschäftsprozesse (BPMN-Format)
- Definieren Sie IT- und Notfallprozesse

Asset-Register anlegen und pflegen

Parallel zu Ihrer Dokumentation der Standorte, Prozesse, Geräte und Applikationen erstellen Sie Ihr Asset-Register. Es umfasst sämtliche Unternehmenswerte und enthält Informationen zum Schutzbedarf. Damit bildet es die Grundlage für Ihre Risikoanalyse und die Beurteilung, welche Maßnahmen in Ihrem Fall erforderlich sind.

→ Umsetzung im DPMS mit dem Modul „Asset-Register“

- Verwalten Sie alle Assets zentral auf einer Oberfläche
- Legen Sie den Schutzbedarf fest
- Nutzen Sie die voreingestellten Risikomatrizen oder erstellen Sie Ihre eigenen
- Dokumentieren Sie maximale Ausfallzeiten und Wiederanlaufzeiten im Zuge des Betrieblichen Kontinuitätsmanagements

3. Risiken erkennen und minimieren

Egal ob Ransomware, Ausfälle oder interne Fehler: Informationssicherheitsrisiken können enorme Auswirkungen auf Ihr Unternehmen haben – sowohl operativ als auch rechtlich. Analysieren Sie diese Risiken systematisch in Bezug auf Vertraulichkeit, Verfügbarkeit und Integrität Ihrer Daten.

→ Umsetzung im DPMS mit den Modulen „Risikoanalysen“ und „Bedrohungen“

- Ordnen Sie den Assets Bedrohungen und Schwachstellen zu
- Leiten Sie Maßnahmen zur Reduzierung des Risikos ab (Risikobehandlungsplan)
- Betrachten Sie die aktuellen Risikowerte nach der Risikobehandlung

4. Richtlinien aufsetzen und verteilen

Viele Maßnahmen müssen Sie nicht nur technisch, sondern auch organisatorisch umsetzen. Es werden daher auch einige Konzepte, Richtlinien und Verfahrensanweisungen Teil Ihres ISMS sein. Diese müssen Sie freigeben (lassen) und an die Mitarbeitenden verteilen.

→ Umsetzung im DPMS mit den Modulen „Dokumente“ und „Intranet“

- Erstellen Sie mit dem Dokumentengenerator schnell neue Richtlinien (Vorlagenpaket)
- Lenken und versionieren Sie Ihre Dokumente digital und automatisiert
- Klassifizieren Sie Ihre Dokumente, z. B. nach „öffentlich“, „intern“, „vertraulich“
- Veröffentlichen Sie Ihre Dokumente und lassen Sie die Kenntnisnahme durch die Mitarbeitenden digital bestätigen

5. Mitarbeitende schulen und sensibilisieren

Technische Schutzmaßnahmen allein reichen nicht aus. Die Wirksamkeit ist abhängig von den Mitarbeitenden, die täglich mit den IT-Systemen arbeiten. Studien zeigen: Über 90 % der Sicherheitsvorfälle lassen sich auf menschliches Fehlverhalten zurückführen – etwa durch Phishing, unsichere Passwörter oder versehentlich gelöschte Daten.

Deshalb müssen Unternehmen ihre Mitarbeitenden regelmäßig schulen und sensibilisieren – und nachweisen, dass sie dies auch tun.

Aber auch die Geschäftsleitung selbst muss sich weiterbilden: Eine neue Anforderung, die das BSIG mitbringt, ist die Schulungspflicht für Geschäftsleitungen. Das bedeutet, sie müssen ebenfalls regelmäßig an Schulungen teilnehmen, um Kenntnisse im Bereich des Risikomanagements und in der IT-Sicherheit zu erlangen. Mit DPMS bauen Sie ein strukturiertes Awareness-Programm auf.

→ Umsetzung im DPMS mit dem Modul „Schulungen“

- Erstellen Sie Online-Mitarbeiterschulungen inkl. Abschlusstest (z. B. zur Informationssicherheit oder für die Phishing-Sensibilisierung)
- Verschicken Sie automatisiert die Teilnahmezertifikate
- Verfolgen Sie den Fortschritt der Teilnehmenden
- Nutzen Sie die automatische Erinnerungsfunktion

6. Sicherheitsvorfälle managen

Da es trotz etablierter Sicherheitsmaßnahmen und regelmäßiger Mitarbeitersensibilisierung zu Informationssicherheitsvorfällen kommen kann, müssen Sie einen Prozess zur Meldung und Bewältigung von Vorfällen einführen.

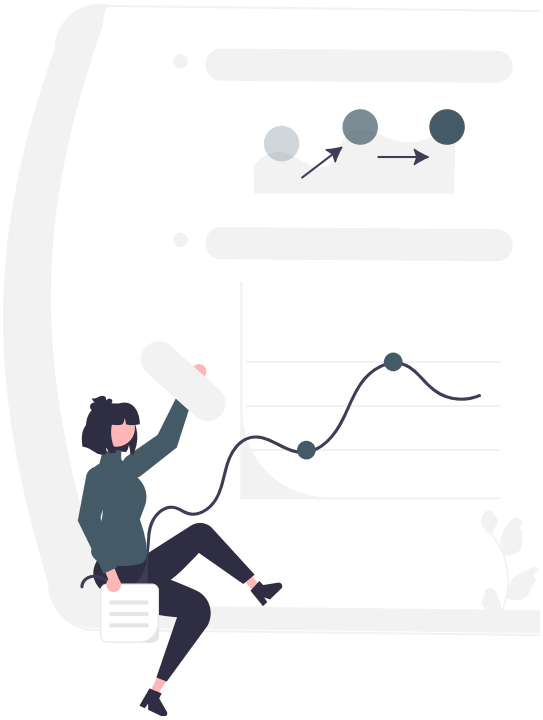
Den Beschäftigten muss klar sein, was ein Vorfall ist, wer in diesem Fall informiert werden muss und über welchen Kanal. Es sind konkrete verantwortliche Personen zu benennen, die zuständig sind, den Vorfall zu bearbeiten und zu eskalieren.

→ Umsetzung im DPMS mit dem Modul „Intranet“

- Stellen Sie Ihren Beschäftigten eine zentrale Weboberfläche für die Meldung von Vorfällen zur Verfügung
- Definieren Sie Verantwortliche, die per E-Mail über Vorfälle informiert werden sollen

→ **Ausblick:** Bald können Sie Ihre Datenschutz- und Sicherheitsvorfällen mit dem Modul „Ereignisse“ bearbeiten und dokumentieren (erscheint in Kürze).

7. Auditieren und kontinuierlich verbessern



Ein einmal aufgebautes ISMS reicht nicht aus – Informationssicherheit ist ein fortlaufender Prozess. Sie müssen Ihr Sicherheitsniveau regelmäßig prüfen und verbessern.

Im Zentrum steht dabei der sogenannte PDCA-Zyklus (Plan – Do – Check – Act): Ein kontinuierlicher Verbesserungsprozess, mit dem Sie Schwachstellen aufdecken, Maßnahmen nachsteuern und Compliance dauerhaft sichern.

Praxistipp: Führen Sie Audits nicht nur „von oben“ durch – binden Sie Fachabteilungen aktiv ein. So steigern Sie das Sicherheitsbewusstsein und verbessern zugleich die Akzeptanz Ihres ISMS.

→ Umsetzung im DPMS mit dem Modul „Managementsysteme“

- Erstellen Sie Fragenkataloge, um einzelne Prüfbereiche zu auditieren
- Übernehmen Sie Antworten und Erkenntnisse automatisch in Ihr Managementsystem
- Leiten Sie Maßnahmen ab, um bei Abweichungen gegenzusteuern
- Generieren Sie hieraus die Grundlage für Ihre Managementbewertung

→ **Ausblick:** Bald können Sie Ihre internen Audits auch mit dem Modul „Interne Audits“ abbilden (erscheint in Kürze).

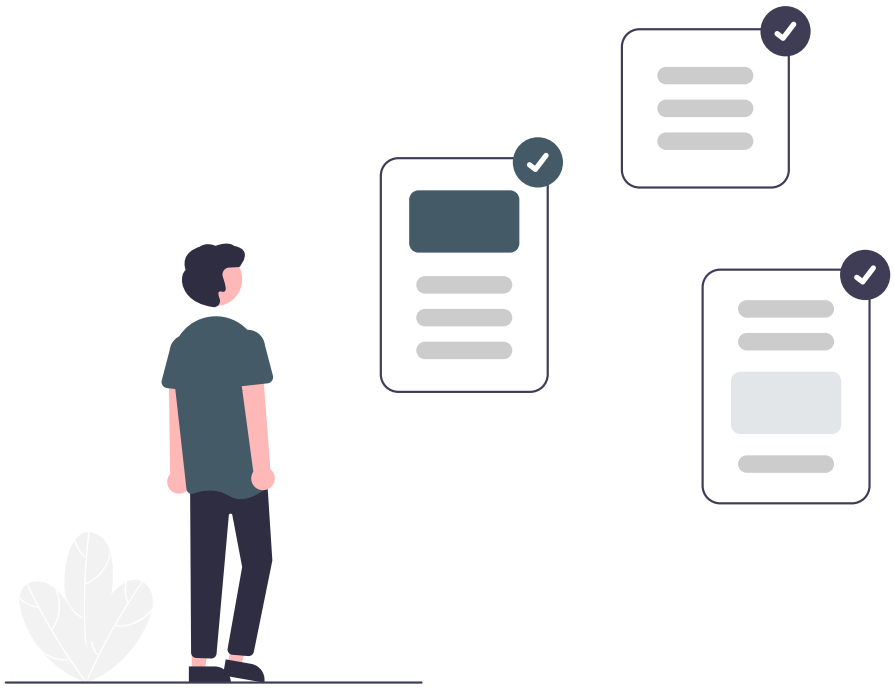
8. Lieferanten dokumentieren und bewerten

Auch wenn Ihr Unternehmen intern alles richtig macht – Sie arbeiten womöglich mit externen Partnern zusammen, die ebenfalls Zugriff auf IT-Systeme und sensible Daten haben, zum Beispiel durch Wartung, Hosting oder Support. Damit Sicherheitslücken nicht unbemerkt über externe Dienstleister ins eigene Unternehmen hineinwirken, ist es notwendig, auch die Sicherheitsvorkehrungen Ihrer Partner im Blick zu behalten.

Gesetzliche Rahmenwerke wie das BSIG (bzw. vorher NIS2-Umsetzungsgesetz) sehen vor, dass Unternehmen nachvollziehbar darlegen können, wie mit Risiken aus der Lieferkette umgegangen wird. Es geht darum, mögliche Risiken frühzeitig zu erkennen und angemessene Schutzmaßnahmen gemeinsam zu etablieren.

→ Umsetzung im DPMS mit dem Modul „Dienstleister/Lieferanten“

- Verwalten Sie all Ihre Dienstleister in einer übersichtlichen Struktur
- Dokumentieren Sie die Zulässigkeit von Datenübermittlungen
- Versenden Sie Fragebögen an Lieferanten, um automatisch einen Risikowert zu erhalten



Muster Berater GmbH

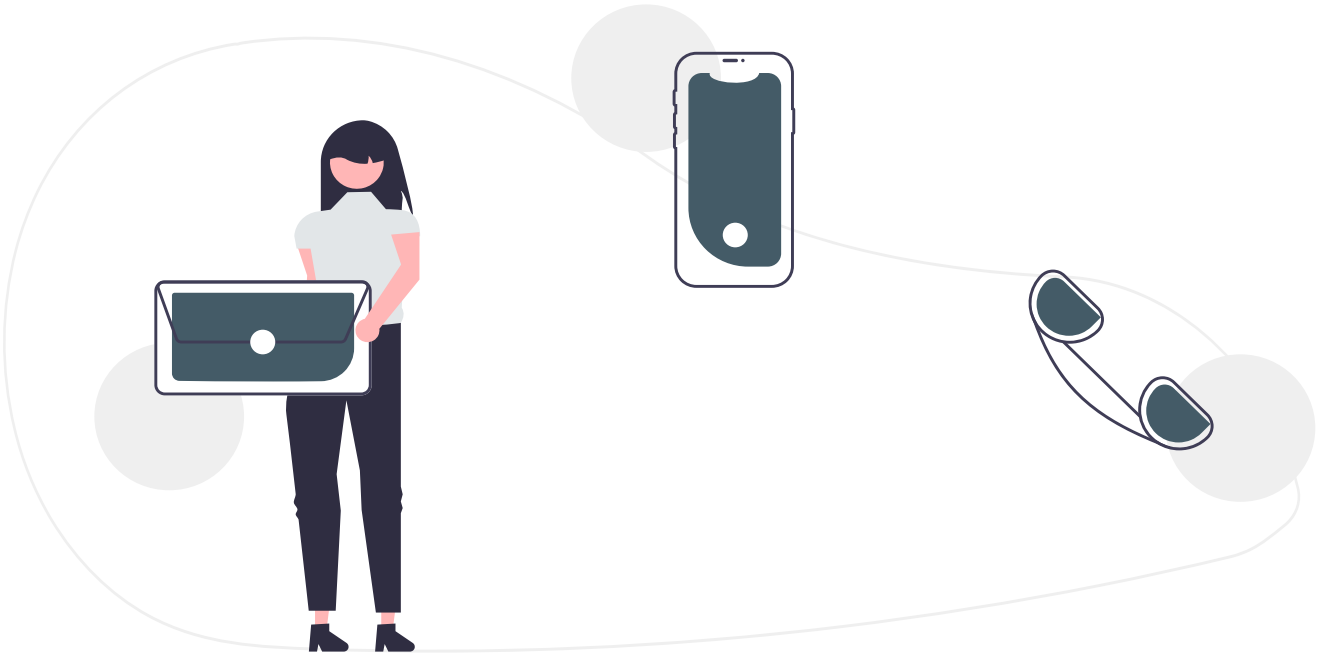
Vielen Dank für Ihr Vertrauen!

Sollten Sie Fragen haben oder eine individuelle Beratung wünschen, stehen wir Ihnen jederzeit gerne zur Verfügung.

Kontaktieren Sie uns

LegalInnovate Technologies GmbH
Geschäftsführer: Thomas Niersmann
Adresse: Issumer Tor 45, 47608 Geldern
E-Mail: info@dpms-online.de

www.dpms-online.de




MB
Muster
Berater GmbH