Datenschutzhandbuch

der *<Firmenname einfügen>*

Status:	Dokumentversion:	Erstellt am / von:	Letzte Änderung am / von:
Verteiler:	Ausgabe-Datum:	Erste Freigabe am / von:	Letzte Freigabe am / von:

<Logo einfügen>	**DATENSCHUTZHANDBUCH**

Inhaltsverzeichnis

1. Einleitung

1.1. Änderungskontrolle

Datum	Beschreibung der Änderung, Version	Autor

1.2. Gegenstand des Dokuments

Im Datenschutzhandbuch der *<Firmenname einfügen>* werden die im Unternehmen geltenden Regeln zum Umgang und der Verarbeitung von (personenbezogenen) Daten aufgeführt. Dazu werden hier die Organisation und die Ziele von Datenschutz und Informationssicherheit in übersichtlicher Form dargestellt.

Das Datenschutzhandbuch enthält die wesentlichen Vorgaben, die für den Umgang und die Verarbeitung von (personenbezogenen) Daten gelten. Von den Vorgaben darf nur abgewichen werden, wenn ein Vorgesetzter der Abweichung vorher zugestimmt hat. Abweichungen von den Vorgaben müssen begründet sein.

1.3. Ziele des Dokuments

Als Unternehmen verarbeiten wir eine Vielzahl von (auch personenbezogenen) Daten mit unterschiedlichem Schutzbedarf, um unsere Aufgaben und Pflichten gegenüber unseren Kunden, Vertragspartnern, Dienstleistern, öffentlichen Stellen und sonstigen Dritten zu erfüllen. Die Ziele des Datenschutzhandbuchs sind dabei die Sicherheit der Informationsverarbeitung und der Schutz von (personenbezogenen) Daten in unserem Unternehmen sowie die Vorgaben der Datenschutz-Grundverordnung (DSGVO) jederzeit zu gewährleisten. Das Handbuch soll dazu beitragen, dass die Integrität, Verfügbarkeit und Vertraulichkeit von Informationen zu jederzeit gewahrt ist.

1.4. Geltungsbereich

Dieses Datenschutzhandbuch und die jeweils aktuelle Fassung gilt für die *<Firmenname einfügen>* und erstreckt sich auf alle Standorte der *<Firmenname einfügen>*. Es ist für alle Mitarbeiter verbindlich und verpflichtet alle Beschäftigten zur Einhaltung der hier festgelegten Vorgaben. Änderungen am Datenschutzhandbuch werden den Beschäftigten in Form eines Aushangs mitgeteilt.

1.5. Maßnahmen

Die Maßnahmen zur Umsetzung dieses Datenschutzhandbuchs können in Form von technischen und organisatorischen Maßnahmen erfolgen. Dazu gehören auch Richtlinien, betriebliche Regelungen oder betriebliche Anweisungen. Diese sind von den Beschäftigten zu befolgen.

1.6. Verantwortlichkeiten

Die **Unternehmensleitung** übernimmt die Gesamtverantwortung für die Informationssicherheit und den Datenschutz im Unternehmen.

Die Verantwortlichkeiten vom Informationssicherheits- und Datenschutzbeauftragten sind in Kapitel zwei beschrieben.

Der **IT-Verantwortliche** setzt die Richtlinien und sonstigen Vorgaben zu Datenschutz und Informationssicherheit in seinem Verantwortungsbereich um. Er stimmt Maßnahmen, die Auswirkungen auf die Informationssicherheit haben, mit dem Informationssicherheitsbeauftragten ab.

Die **Administratoren** führen die technischen Maßnahmen in Abstimmung mit dem IT-Verantwortlichen durch und tragen durch Verbesserungsvorschläge zur Optimierung der Informationssicherheit bei.

Vorgesetzte mit Personalverantwortung haben die Aufgabe, sicherzustellen, dass die getroffenen technischen und organisatorischen Maßnahmen zur Informationssicherheit in Bezug auf die die in ihrem Verantwortungsbereich tätigen Personen umgesetzt werden.

Jeder **Mitarbeiter** trägt durch sein Verhalten zur Gewährleistung von Datenschutz und Informationssicherheit bei. Alle Beschäftigten sind verpflichtet, die Leitlinien und die Richtlinien zu *<Leit- und Richtlinien einfügen>*, der *<Firmenname einfügen>*, einzuhalten. Um Datenschutz und Informationssicherheit im Unternehmen zu gewährleisten ist jeder Mitarbeiter verpflichtet, Störungen, Sicherheitsvorfälle und Notfälle im Bereich der Informationssicherheit unverzüglich und direkt an *<Meldestelle einfügen>* zu melden. Vorfälle im Bereich des Datenschutzes sind von allen Beschäftigten unverzüglich nach Kenntnisnahme an *<Meldestelle einfügen>* zu melden. Es gelten die jeweiligen Richtlinien der *<Firmenname einfügen>*.

Projekt oder Prozessverantwortliche müssen *<Verantwortlichen einfügen>* bei allen Projekten mit Auswirkung auf die Verarbeitung personenbezogener Daten konsultieren, um sicherzustellen, dass datenschutzrechtliche Vorschriften eingehalten werden können. Ferner sind alle Projekt- oder Prozessverantwortlichen verpflichtet, *<Verantwortlichen einfügen>* bei allen Projekten zu konsultieren, die Auswirkung auf die Informationssicherheit im Unternehmen haben.

Lieferanten, externe Dienstleister und sonstige Auftragnehmer sind durch gesonderte Vereinbarungen zu verpflichten, die sie betreffenden Vorgaben zu Datenschutz und Informationssicherheit einzuhalten, wenn diese Daten im Auftrag verarbeiten oder die Möglichkeit der Kenntnisnahme von personenbezogenen Daten oder als nicht öffentlich klassifizierten Informationen des Unternehmens haben.

1.7. Bekanntgabe

Die jeweils aktuelle Version des Datenschutzhandbuchs wird über die Geschäftsführung der *<Firmenname einfügen>* an die einzelnen Mitarbeiter verteilt. Das Handbuch ist darüber hinaus für jeden zugänglich in *<Ablageort einfügen>* abgelegt.

Neue Mitarbeiter erhalten das Datenschutzhandbuch als Anlage zu ihrem Arbeitsvertrag.

Die Mitarbeiter müssen den Empfang und die Geltung dieses Handbuchs schriftlich bestätigen. Dies ist von der verantwortlichen Führungskraft in der Personalakte entsprechend zu dokumentieren.

1.8. Folgen bei Verstoß

Das Datenschutzhandbuch ist Teil des Arbeitsvertrages. Ein Verstoß gegen die Regelungen kann je nach Art des Vergehens arbeits- und/oder strafrechtlich verfolgt werden.

Alle Mitarbeiter sind verpflichtet, Verstöße gegen die Regeln dieses Handbuchs oder Auffälligkeiten umgehend ihrer Führungskraft, *<weitere Meldestellen einfügen>* der *<Firmenname einfügen>* zu melden.

2. Organisation von Datenschutz und Informationssicherheit

2.1. Informationssicherheitsbeauftragter

Zur Erreichung der Ziele dieses Handbuchs wurde ein Informationssicherheitsbeauftragter von der Unternehmensleitung benannt. Dabei handelt es sich um *<Name einfügen>*.

Verantwortlich für die Sicherheitsorganisation ist die Unternehmensleitung. Der Informationssicherheitsbeauftragte berät die Unternehmensleitung bei der Planung und Umsetzung der Informationssicherheit im Unternehmen. Er berichtet in seiner Funktion anlassbezogen, mindestens jedoch einmal jährlich, unmittelbar an die Unternehmensleitung. Der Informationssicherheitsbeauftragte hat weiter die Aufgabe der Initiierung, Planung, Umsetzung und Steuerung des Informationssicherheitsprozesses im Unternehmen. Er ist Ansprechpartner für Informationssicherheit im Unternehmen.

Dem Informationssicherheitsbeauftragten werden von der Leitung ausreichende finanzielle und zeitliche Ressourcen zur Verfügung gestellt, um sich regelmäßig weiterzubilden und zu informieren.

Der Informationssicherheitsbeauftragte ist frühzeitig in alle Projekte einzubinden, um schon in der Planungsphase sicherheitsrelevante Aspekte zu berücksichtigen.

2.2. Datenschutzbeauftragter

Die *<Firmenname einfügen>* hat einen Datenschutzbeauftragten (DSB) benannt. Der Datenschutzbeauftragte ist Ansprechpartner für das Thema Datenschutz im Unternehmen. Er berät, kontrolliert und unterstützt die Unternehmensleitung und Beschäftigten hinsichtlich der Verarbeitung von personenbezogenen Daten im Unternehmen. Seine weiteren Aufgaben ergeben sich vor allem aus Art. 39 DSGVO.

Im Bereich der Verarbeitung von personenbezogenen Daten ist Sorge dafür zu tragen, dass eine frühe Einbindung des Datenschutzbeauftragten bei der Planung und Einführung von neuen Prozessen, in deren Zusammenhang auch personenbezogenen Daten verarbeitet werden, erfolgt. Gleiches gilt für Änderungen an bestehenden Prozessen.

Der Datenschutzbeauftragte und der Informationssicherheitsbeauftragte informieren und unterstützen sich gegenseitig durch gegenseitigen Informationsabgleich, soweit keine gesetzlichen oder vertraglichen Pflichten entgegenstehen.

Nachfolgend seien die konkreten Aufgaben des Datenschutzbeauftragten im Einzelnen aufgeführt.

Nach Artikel 39 DSGVO obliegen dem Datenschutzbeauftragten folgende Aufgaben:

- **Unterrichtung und Beratung** des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten.
- **Überwachung der Einhaltung** dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen.
- **Beratung – auf Anfrage** – im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Artikel 35 DSGVO.
- **Zusammenarbeit mit der Aufsichtsbehörde**.
- **Tätigkeit als Anlaufstelle für die Aufsichtsbehörde** in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Artikel 36 DSGVO, und gegebenenfalls Beratung zu allen sonstigen Fragen.

Nach Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. obliegen dem Datenschutzbeauftragten folgende Aufgaben:

- **Beratung**
  Beraten der Unternehmensführung, zur Sicherstellung des Schutzes personenbezogener Daten.
  - Maßstab

Sicherstellen, dass die Persönlichkeitsrechte der betroffenen Personen geschützt werden und dass personenbezogene Daten im Einklang mit der DSGVO verarbeitet werden.

- Datenschutz-Folgenabschätzung

Wenn eine Risikobewertung ergibt, dass durch eine Datenverarbeitung ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen deren Daten verarbeitet werden entsteht, ist vorab eine Abschätzung der Folgen durchzuführen, die bei den vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogen Daten natürlicher Personen entstehen.

- Betroffene Personen

Unterstützung der Unternehmensführung bei der Aufklärung der betroffenen Personen über ihre Rechte und Freiheiten.

- Mitarbeitervertretung

Tätigkeit als unabhängiger Datenschutzbeauftragter für die Mitarbeitervertretung.

- **Überwachung**
  Überwachung der Einhaltung datenschutzrechtlicher Vorgaben im Unternehmen. Quartalsweise Überwachung der Verfahren nach den Grundsätzen von Artikel 5 bis 11 DSGVO.
- **Berichtspflicht**
  Erstellung eines Tätigkeitsberichtes für alle getätigten Maßnahmen hinsichtlich des Datenschutzes und regelmäßige Unterrichtung der Führungsebene und der Abteilungen zu wichtigen Datenschutzangelegenheiten des Unternehmens.
- **Kontaktstelle für Aufsichtsbehörde**
  Zusammenarbeit mit der zuständigen Aufsichtsbehörde.
- **Schulungs- und Sensibilisierungsaufgaben**
  Durchführung von Schulungsmaßnahmen für die Mitarbeiter, um über Verhaltensregeln und Gefahren aufzuklären.
- **Priorisierung**
  Herausfinden, welche Daten wirklich für den Zweck des Prozesses benötigt werden.

ENDE DER LESEPROBE

Die folgenden Kapitel müssen individuell beschrieben werden.