2 LEITLINIE ZU DATENSCHUTZ UND INFORMATIONSSICHERHEIT

VERSIONSHISTORIE

Version	Datum	Anmerkungen	Autor
1.0	12.04.2018	Initialfassung der Leitlinie	Sylke Burmester
1.1	09.05.2018	Redaktionelle Überarbeitung	Sylke Burmester

2.1 EINLEITUNG

Das **finanzkontor Kindler, Korth & Kolleginnen GmbH & Co. KG- im Folgenden das „finanzkontor" genannt** verabschiedet hiermit diese Leitlinie zu Datenschutz und Informationssicherheit in unserem Unternehmen.

Als Unternehmen verarbeiten wir eine Vielzahl von (auch personenbezogenen) Daten, um unsere Aufgaben und Pflichten gegenüber unseren Kund*innen, Vertragspartner*innen, Dienstleister*innen, öffentlichen Stellen und sonstigen Dritten zu erfüllen.

Dabei verarbeiten wir Daten mit unterschiedlichem Schutzbedarf. Die Sicherheit der Informationsverarbeitung und der Schutz von personenbezogenen Daten spielt eine wesentliche Rolle in unserem Unternehmen. Diese Leitlinie soll die Strategie, die Organisation und Ziele von Datenschutz und Informationssicherheit in unserem Unternehmen in übersichtlicher Form darstellen.

2.2 GELTUNGSBEREICH

Die Leitlinie gilt für das Finanzkontor. Sie erstreckt sich auf alle Standorte des finanzkontors.

Diese Leitlinie verpflichtet alle Beschäftigten des finanzkontors zur Einhaltung der hier festgelegten Pflichten.

2.3 ZIELE

Ziel dieser Leitlinie ist es, Datenschutz und Informationssicherheit im Unternehmen zu gewährleisten. Für diesen Zweck wird das Unternehmen bei der Planung, Einführung und während des Ablaufs von Prozessen nachfolgende Ziele berücksichtigen:

1. Rechtmäßigkeit
2. Transparenz
3. Zweckbindung
4. Datenminimierung
5. Richtigkeit
6. Speicherbegrenzung
7. Verfügbarkeit, Integrität und Vertraulichkeit, Belastbarkeit

8. Intervenierbarkeit und Verarbeitung nach Treu und Glauben („Fairness")
9. Rechenschaftspflicht („Accountability-Prinzip")

Die Berücksichtigung dieser Ziele wird durch gesonderte Richtlinien konkretisiert.

Bei der konkreten Umsetzung der Ziele müssen die getroffenen Schutzmaßnahmen in einem wirtschaftlich vertretbaren Verhältnis zum Schutzbedarf der verarbeiteten Daten und Informationen stehen.

2.4 Organisation von Datenschutz und Informationssicherheit

Zur Erreichung der Ziele dieser Richtlinie wurde eine **Informationssicherheitsbeauftragte** von der Unternehmensleitung benannt. Dabei handelt es sich um **Frau Maxi Arnold**.

Verantwortlich für die Sicherheitsorganisation ist die Geschäftsführung. Die Informationssicherheitsbeauftragte berät die Geschäftsführung bei der Planung und Umsetzung der Informationssicherheit im Unternehmen. Sie berichtet in ihrer Funktion anlassbezogen, mindestens jedoch einmal jährlich, unmittelbar an die Geschäftsführung.

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.

Das finanzkontor hat eine Datenschutzbeauftragte (DSB) benannt. Die Datenschutzbeauftragte ist Frau Sylke Burmester und Ansprechpartner für das Thema Datenschutz im Unternehmen. Sie berät, kontrolliert und unterstützt die Unternehmensleitung und Beschäftigten hinsichtlich der Verarbeitung von personenbezogenen Daten im Unternehmen. Ihre 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 der **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.

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

Im Unternehmen wird sowohl für den Bereich der Informationssicherheit als auch für den Bereich des Datenschutzes ein Managementsystem eingerichtet. Hierfür wird im Unternehmen ein Prozess der kontinuierlichen Verbesserung mit dem Ziel implementiert, die einzelnen Maßnahmen in den Bereichen Datenschutz und Informationssicherheit so zu koordinieren, dass die Ziele dieser Leitlinie erreicht werden.

Es wird ein **Datenschutz- und Informationssicherheitsteam („Datenschutzteam" – DST, das aus Maxi Arnold, Sylke Burmester und Jana Reer)** gebildet, das die Planung, Umsetzung und Evaluierung von Datenschutz und die Informationssicherheit im Unternehmen begleitet und unterstützt. Das DST wird die für die Umsetzung der Ziele dieser Leit-linie erforderlichen Richtlinien planen, mit der Geschäftsführung abstimmen und regelmäßig auf ihre Wirksamkeit überprüfen und erforderli-

chenfalls Anpassungen vornehmen. Für den Fall, dass das DST in Fragen der Planung, Umsetzung, Evaluierung oder Anpassung von Richtlinien oder bei der Beurteilung von Sach- oder Rechtsfragen uneinig ist, wird das DST dies der Geschäftsführung vortragen. Die Geschäftsführung wird dann entscheiden und die erforderlichen Maßnahmen veranlassen.

Die Richtlinien werden von der Geschäftsführung verbindlich gemacht, so dass sie von den jeweiligen Adressaten der Richtlinie einzuhalten sind und Verstöße ggf. sanktioniert werden können.

Das DST berichtet direkt an die Geschäftsführung.

2.5 Maßnahmen

Die Maßnahmen zur Umsetzung dieser Leitlinien 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.

2.6 Verantwortlichkeiten

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

Die **Informationssicherheitsbeauftragte** hat die Aufgabe der Initiierung, Planung, Umsetzung und Steuerung des Informationssicherheitsprozesses im Unternehmen. Sie ist Ansprechpartner für Informationssicherheit im Unternehmen.

Die **Datenschutzbeauftragte** ist Ansprechpartnerin für das Thema Datenschutz im Unternehmen. Sie berät, kontrolliert und unterstützt die Unternehmensleitung und Beschäftigten hinsichtlich der Verarbeitung von personenbezogenen Daten im Unternehmen. Ihre Aufgaben ergeben sich aus den datenschutzrechtlichen Vorschriften der Bundesrepublik Deutschland.

Das **Datenschutz- und Informationssicherheitsteam** unterstützt die Datenschutzbeauftragte und die Informationssicherheitsbeauftragte bei der Planung, Koordinierung und Umsetzung von Datenschutz und Informationssicherheit im Unternehmen. Dieses Team trifft sich mit der Datenschutzbeauftragten und Informationssicherheitsbeauftragten in regelmäßigen Abständen, um den Prozess der kontinuierlichen Verbesserung zu gewährleisten

Die **IT-Verantwortliche** setzt die Richtlinien und sonstigen Vorgaben zu Datenschutz und Informationssicherheit in ihrem Verantwortungsbereich um. Sie stimmt Maßnahmen, die Auswirkungen auf die Informationssicherheit haben, mit der Informationssicherheitsbeauftragten ab.

Die **Administrator*innen** führen die technischen Maßnahmen in Abstimmung mit der 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.

Jede **Mitarbeiter*in** trägt durch ihr Verhalten zur Gewährleistung von Datenschutz und Informationssicherheit bei. Alle Beschäftigten sind verpflichtet, diese Leitlinie und die Richtlinien zu Datenschutz und Informationssicherheit einzuhalten. Um Datenschutz und Informationssicherheit im Un-

ternehmen ist jede Mitarbeiter*in verpflichtet, Störungen, Sicherheitsvorfälle und Notfälle im Bereich der Informationssicherheit unverzüglich und direkt an die Informationssicherheitsbeauftragte zu melden. Vorfälle im Bereich des Datenschutzes sind von allen Beschäftigten unverzüglich nach Kenntnisnahme an die Datenschutzbeauftragte zu melden. Sollten Beschäftigte Zweifel haben, ob ein Vorfall an die Informationssicherheitsbeauftragte oder an die Datenschutzbeauftragte zu melden ist, soll in diesen Fällen eine Meldung an die Datenschutzbeauftragte erfolgen. Die Datenschutzbeauftragte wird die Meldung ggf. an den Informationssicherheitsbeauftragten weiterleiten.

Projekt oder Prozessverantwortliche müssen die Datenschutzbeauftragte bei allen Projekten mit Auswirkung auf die Verarbeitung personenbezogener Daten konsultieren, um sicherzustellen, dass datenschutzrechtliche Vorschriften eingehalten werden können. Ferner sind alle Projekt- oder Prozessverantwortliche verpflichtet, den Informationssicherheitsbeauftragten bei allen Projekten zu konsultieren, die Auswirkung auf die Informationssicherheit im Unternehmen haben.

Lieferant*innen, externe Dienstleister*innen und sonstige Auftragnehmer*innen 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.

2.7 SANKTIONEN

Ein Verstoß gegen diese Leitlinie kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden.

Für Lieferant*innen, externe Dienstleister*innen und sonstige Auftragnehmer*innen sollten bei besonderen Risiken Vertragsstrafenregelungen vereinbart werden.

Berlin, 22.6.2018