Leitlinie zu Datenschutz und Informationssicherheit

Einleitung

Die w3 GmbH 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 Kunden, Vertragspartnern, Dienstleistern, 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.

Geltungsbereich

Diese Leitlinie gilt für die w3 GmbH. Sie erstreckt sich auf alle Standorte der w3 GmbH. Diese Leitlinie verpflichtet alle Beschäftigten der w3 GmbH zur Einhaltung der hier festgelegten Pflichten. Die Leitlinie wird den Beschäftigten in der jeweils geltenden Fassung über das „Datenschutz-Wiki“ der w3 GmbH zugänglich gemacht.

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, vor allem den Richtlinien des Datenschutzhandbuches der w3 GmbH konkretisiert. Bei der konkreten Umsetzung der Ziele müssen die getroffenen Schutzmaßnahmen in einem wirtschaftlich vertretbaren Verhältnis zum Schutzbedarf der verarbeiteten Daten und Informationen stehen.

Organisation von Datenschutz und Informationssicherheit

Informationssicherheitsbeauftragter

Zur Erreichung der Ziele dieser Richtlinie wurde ein Informationssicherheitsbeauftragter von der Unternehmensleitung benannt. Dabei handelt es sich um **Herrn Frank Hochdorfer**.

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. Diese Einbindung kann auch durch eine frühzeitige Einbindung des Datenschutz- und Informationssicherheitsteams (DST, s.u.) erfolgen, wenn sichergestellt ist, dass der ISB Mitglied des DST ist.

Datenschutzbeauftragter

Die w3 GmbH 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. Die Einbindung des DSB kann auch im Zusammenhang mit der Einbindung des DST erfolgen.

Der Datenschutzbeauftragte und der Informationssicherheitsbeauftragte informieren und unterstützen sich gegenseitig durch gegenseitigen Informationsabgleich, soweit keine gesetzlichen oder vertraglichen Pflichten entgegenstehen. Der Informationsaustausch kann über das DST erfolgen.

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.

Datenschutz- und Informationssicherheitsteam [DST]

Es wird ein Datenschutz- und Informationssicherheitsteam (DST) gebildet, das die Planung, Umsetzung und Evaluierung von Datenschutz im Unternehmen Informationssicherheit im

Unternehmen begleitet und unterstützt. Das DST wird die für die Umsetzung der Ziele dieser Leitlinie erforderlichen Richtlinien planen, mit der Unternehmensleitung abstimmen und regelmäßig auf ihre Wirksamkeit überprüfen und erforderlichenfalls 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 Unternehmensleitung vortragen. Die Unternehmensleitung wird dann entscheiden und die erforderlichenfalls Maßnahmen veranlassen.

Die Richtlinien, insbesondere die im Datenschutzhandbuch der w3 GmbH enthaltenen Richtlinien, werden von der Unternehmensleitung 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 Unternehmensleitung.

Die Unternehmensleitung wird die Mitglieder des DST bestimmen. Zwingend dem DST gehören der Datenschutzbeauftragte und – soweit vorhanden – der Informationssicherheitsbeauftragte an. Weitere Mitglieder wird die Unternehmensleitung im Einvernehmen mit den jeweiligen Personen bestimmen.

Das DST berät über Sachfragen und wird der Unternehmensleitung über das Ergebnis der Erörterung berichten. Sollte das DST keine einheitliche Meinung zu einer Sachfrage haben, wird der Meinungsstand offen an die Unternehmensleitung berichtet.

Die Unternehmensleitung kann Entscheidungen an das DST durch Weisungen in Textform delegieren. Bei dieser Delegierung hat die Unternehmensleitung zu bestimmten, ob für eine Entscheidung des DST ein einheitlicher Beschluss des DST oder eine Mehrheitsentscheidung ausreichend ist.

Das DST wird sich mindestens einmal jährlich treffen, um die getroffenen Maßnahmen zu Datenschutz und Informationssicherheit im Hinblick auf ihre Wirksamkeit zu überprüfen und Anpassungen vorzunehmen.

Das DST wird sich ansonsten anlassbezogen im Hinblick auf Treffen oder Entscheidungsfindungen koordinieren, um anstehende Sachfragen zu erörtern und zu entscheiden. Maßnahmen und Entscheidungen können auch telefonisch oder in Textform erörtert werden, also z.B. durch Telefonkonferenzen, Online-Meetings und/oder E-Mail-Diskussionen.

Das DST kann selbst eigene Rollen an Mitglieder verteilen. So kann z.B. die Pflege und das Führen von Verarbeitungsverzeichnissen oder die Planung der Durchführung von Datenschutz-Folgenabschätzungen an einzelne Mitglieder zu weiteren Koordination delegiert werden. Das DST wirkt jedoch gemeinschaftlich, und die Mitglieder des DST unterstützen sich gegenseitig bei der Erfüllung ihre Aufgaben. Dem DST können Aufgaben und Befugnisse von der Unternehmensleitung übertragen werden. Dies kann auch durch entsprechende Vorgaben im Datenschutzhandbuch der w3 GmbH erfolgen.

Für das DST wird eine Sammel-E-Mail-Adresse unter dst@w3.de eingerichtet, unter der das DST für alle Beschäftigten der w3 GmbH und die Unternehmensleitung elektronisch erreichbar ist. Die E-Mail-Adresse wird allen Beschäftigten in geeigneter Weise mitgeteilt und muss für alle Mitarbeiter leicht aufzufinden sein. Dies kann z.B. durch Aushänge (analog/digital) erfolgen.

Aufgabe des DST ist es, das Wissen im Bereich Datenschutz und Informationssicherheit aufzubauen und aufrechtzuerhalten. Das DST pflegt hierzu Kontakte zu geeigneten Arbeitskreisen, Gremien oder Verbänden.

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.

Verantwortlichkeiten

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

Die Verantwortlichkeiten von DSB, ISB und IST sind bereits oben 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 ur 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, diese Leitlinie und die Richtlinien zu Datenschutz und Informationssicherheit, insbesondere die Richtlinien aus dem Datenschutzhandbuch der w3 GmbH, einzuhalten. Um Datenschutz und Informationssicherheit im Unternehmen ist jeder Mitarbeiter verpflichtet, Störungen, Sicherheitsvorfälle und Notfälle im Bereich der Informationssicherheit unverzüglich und direkt an das DST zu melden. Vorfälle im Bereich des Datenschutzes sind von allen Beschäftigten unverzüglich nach Kenntnisnahme an das DST zu melden. Es gelten die jeweiligen Richtlinien aus dem Datenschutz-Wiki der w3 GmbH.

Projekt oder Prozessverantwortliche müssen das DST 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, das DST 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.

Sanktionen

Ein Verstoß gegen diese Leitlinie kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden. Für Lieferanten, externe Dienstleister und sonstige Auftragnehmer sollten bei besonderen Risiken Vertragsstrafenregelungen vereinbart werden.

Zur Umsetzung der Ziele aus der Leitlinie sind die nachfolgenden Richtlinien von den Beschäftigten einzuhalten. Der Geltungsbereich ergibt sich aus der jeweiligen Richtlinie.

Dieses Datenschutzhandbuch wird regelmäßig aktualisiert. Die Änderungen sind der Versionshistorie zu entnehmen. Gleiches gilt für Änderungen der Richtlinien. Es gilt die jeweils aktuelle Fassung der Richtlinien in diesem Datenschutzhandbuch.