Leistungsbeschreibung Datenschutz

UIMC®

Datenschutz von A bis Z

Datenschutz mit Effektivität und Effizienz schrittweise und nachhaltig verbessern

In Datenschutz und Informationssicherheit stets gut beraten!

UIMC Dr. Vossbein GmbH & Co KG
Nützenberger Straße 119
42115 Wuppertal
E-Mail: consultants@uimc.de
Tel: 0202 / 265 74 - 0
Fax: 0202 / 265 74 - 19
Internet: www.UIMC.de

Die Anforderungen

Der Gesetzgeber legt Unternehmen durch diverse gesetzliche Regelungen umfassende Vorgaben im Umgang mit personenbezogenen Daten auf.

Kernanforderung Datenschutzbeauftragter

Gemäß § 4f BDSG hat jedes Unternehmen einen Beauftragten für den Datenschutz schriftlich zu bestellen, sofern **mehr als 9 Personen** personenbezogene Daten verarbeiten (dies ist bspw. schon dann erreicht, wenn 10 Mitarbeiter einen E-Mail-Account haben).

Hierbei darf **nur zum Beauftragten** bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Die fachliche Eignung muss hierbei kontinuierlich durch Fortbildungen aufgebaut und aufrecht erhalten werden.

Umfassende Aufgaben in der Umsetzung

Es existiert eine Vielzahl an Forderungen, die (**unabhängig von Unternehmensgröße und Mitarbeiteranzahl**) erfüllt werden müssen. Hierbei seien folgende Aufgaben genannt:

» Aufbau einer **Datenschutz-Organisation** mit entsprechenden Prozessen und Richtlinien
» Information und Beratung der Geschäftsführung
» Prüfung der Rechtmäßigkeit der Datenverarbeitung
» Beratung der Mitarbeiter und Fachbereiche
» **Überwachung** der ordnungsgemäßen Anwendung der EDV
» Schulung und **Sensibilisierung** der Mitarbeiter
» Überwachung der Übersicht der verwendeten Verfahren (**Verfahrensverzeichnis**)
» Prüfung/Auditierung der Dienstleister (Auftragsdatenverarbeitung)
» Hinwirken auf Einhaltung der **technisch-organisatorischen Maßnahmen** unter Berücksichtigung der Angemessenheit
» Durchführung einer **Vorabkontrolle** usw.

Firmen-Know-How und sichere IT-Systeme

Auch die Bedeutung der Sicherheit von Informationen sowie der IT-Systeme steigt mit zunehmender Abhängigkeit von der IT. Eine Geschäftstätigkeit ohne IT ist heutzutage nicht mehr denkbar. Auch die Beeinträchtigung der Systeme oder gar der Vertraulichkeitsverlust von Know How kann folgenschwer für den Fortbestand Ihres Hauses sein.

Nicht nur Technik!

Hierbei bedeutet Informationssicherheit nicht nur die technische Verhinderung von Virenbefall, von Verlust der Daten durch Serverdefekte oder von Angriffen durch Hacker, sondern auch

» Prozesse zur Berechtigungsvergabe
» Verschlüsselung von (mobilen) Datenträgern
» Arbeitsplatzgestaltung
» Sichere und ordnungsgemäße Gestaltung von Dienstleistungsverhältnissen
» Verfahren/Vorgehensweisen im „Fall der Fälle“ (Notfall-Management)
» Sensibilisierung der Mitarbeiter usw.

Bildquelle: pixelio.de / Rainer Sturm

Probleme und Lösungsansätze

Externe Anforderungen

Ferner existieren diverse externe Anforderungen:

» Einhaltung von Gesetzen,
» Sicherstellung eines adäquaten Qualitätsmanagements,
» Wirtschaftsprüfer (Prüfung der Ordnungsmäßigkeit),
» Anforderungen von Kunden (z. B. Lieferantenbedingungen),
» Normanforderungen für Auditierung/Zertifizierung und
» Schutz von vertraulichen Informationen und Firmen-Know-How.

Es ist keine Seltenheit, dass eine ordnungsgemäße Informationsverarbeitung und IT-Sicherheit in punkto Verfügbarkeit, Integrität und Vertraulichkeit nicht gewährleistet ist, da Voraussetzungen wie

» angemessene Kapazitäten zur Erstellung von Regelungen/Konzepten (Datenschutz-Konzept und/oder Informationssicherheits-Managementsystem/ISMS),
» Sensibilisierung der Geschäftsleitung und der Mitarbeiter,
» informationssicherheitsbezogenes Know-how und/oder
» Transparenz von Regelungen und Maßnahmen

nicht gegeben sind.

Probleme: Kompetenz und Ressourcen

Dies stellt die Betriebe vor Herausforderungen, weil hierfür zum einen eine „geeignete“ Person gefunden werden muss und zum anderen neue Strukturen geschaffen werden müssen. Einen geeigneten Mitarbeiter für die Funktion des Datenschutzbeauftragten zu finden, ist nicht leicht. Insbesondere die Zuverlässigkeit des Datenschutzbeauftragten bereitet zumeist Probleme, da eine Interessenkollision in vielen Fällen gegeben ist. Zum Beispiel geraten Geschäftsführer, Personalleiter, IT-Leiter und Vertriebs-/Marketingleiter oftmals in Konflikt, wenn sie ihre Interessen und Aufgaben mit den Tätigkeiten des Datenschutzbeauftragten vereinbaren und sich selbst kontrollieren würden.

Somit bereitet die Bestellung eines betrieblichen Datenschutzbeauftragten häufig „praktische Schwierigkeiten“. Analoges gilt erfahrungsgemäß auch für die Informationssicherheit.

Das Rad nicht neu erfinden: Best Practice nutzen

Nicht nur, dass sich die UIMC entsprechender Best-Practice-Normen bedient, vielmehr werden auch langjährige Erfahrungen aus einer Vielzahl von Projekten sowie Tools und interne Standards bei der Umsetzung der Informationssicherheit und des Datenschutzes berücksichtigt.

Wir bieten Betreuung von **A** bis **Z** aus einer Hand: Von der

A usbildung der Mitarbeiter oder des internen Datenschutzbeauftragten:

» E-Learning-Lösungen
» klassische Schulungen
» Coaching des intern bestellten Datenschutzbeauftragten

B egutachtung der aktuellen Situation mit Hilfe einer toolgestützten Schwachstellenanalyse,

C omputergestütztes Lernen mittels E-Learning (webbasiertes eCollege)

D atenschutz-Konzepts bzw. -Handbuchs

bis zur Übernahme **aller** Funktionen als

E xterner Datenschutzbeauftragter;

des Weiteren bieten wir ein an die

K MU-spezifischen Anforderungen für Klein-, Mittel- oder Tochterunternehmen angepasstes Konzept;

bis hin zu

Z ertifizierungsvorbereitungen für ihre Datenschutzorganisation runden das Angebot ab.

U. V. M.

Outsourcing des Beauftragten

Ist-Analyse als erster Schritt

Ausgangspunkt ist stets ein Datenschutz-Checkup, um eine Bewertung der aktuellen Ist-Situation vorzunehmen. Dies tun wir stets mit Hilfe des UIMC-Tools für Analyse und Berichterstellung (UTAB). Innerhalb eines Interviews bzw. Workshops werden die Informationen anhand eines computergestützen Fragenkatalogs erfasst sowie durch die UIMC.austria ausgewertet und in Form eines Status-Quo-Berichts inkl. Schwachstellen und eines Maßnahmenkatalogs zur Verbesserung dokumentiert.

Maßnahmenplanung zur struktruierten Verbesserung

Die vorgeschlagenen Maßnahmen können durch die UIMC innerhalb einer Aktivitätenliste so vorpriorisiert werden, dass eine sukzessive Abarbeitung der Schwachstellen vorgenommen werden kann. Dies ist erforderlich, weil Erfahrungswerte zeigen, dass ein gleichzeitiges Beseitigen verschiedenster Schwachstellen u. a. aus Effizienz-, Akzeptanz- und Effektivitätsgründen nicht sinnvoll ist.

Optimale Organisation

Zentrales Instrument für die Umsetzung des Datenschutzes ist das Datenschutzhandbuch. Es enthält alle wesentlichen Anweisungen, Vorgaben, Formblätter etc. und umfasst alle aufbau- und ablauforganisatorischen Fragestellungen, welche allgemein verbindlich sind.

Das Handbuch ist ein auf langjähriger Erfahrung und den Datenschutzgesetzen basierendes Regelwerk. Es ist modular aufgebaut, wodurch es an jede Institution spezifisch anpassbar ist. Neben der Einzellösung (Datenschutz oder Informationssicherheit) kann/sollte diese Lösung aufgrund der großen Nähe der beiden Gebiete sinnvollerweise auch in Form eines integrierten Informationssicherheits- und Datenschutz-Handbuchs eingesetzt werden.

Faktor Mensch berücksichtigen

Ferner ist es unerlässlich, die Mitarbeiter im Hinblick auf die Risiken zu sensibilisieren und auf die Maßnahmen zu schulen. Aus unserer langjährigen Erfahrung sind vor allem folgende Formen zielführend, welche wir auch umsetzen und zumeist auch sinnvoll miteinander kombinieren, wobei wir gerne ein individuelles Schulungskonzept erstellen:

» Präsenz-Schulungen durch einen erfahrenen Referenten und/oder
» eLearning zur Selbstschulung mittels eCollege.

Kontinuierliche Verbesserung

Durch regelmäßige Besuche, Revisionsgespräche und Audits sowie durch die kontinuierliche Anpassung der Hilfsmittel wie Handbuch und Schulungen an technische und rechtliche Änderungen werden wir den Datenschutz und die Informationssicherheit laufend optiminieren. Auch Veränderungen des Unternehmens können berücksichtigt werden, indem Regelungen, Prozesse usw. entsprechend modifiziert werden.

Bildquelle: pixelio.de / Alexander Klaus

Betreuung und Beratung

Durch Synergien aufgrund von **Mehrfachbestellungen** können die Aufgaben als Datenschutzbeauftragter oftmals nicht nur fachkundiger, sondern auch wesentlich **effizienter** erfüllen. Analoges gilt natürlich auch für den Informationssicherheitsbeauftragten.

Ihr Experten-Team

Wie stellen einen fachkundigen und zuverlässigen Datenschutzbeauftragten und/oder Informationssicherheitsbeauftragten (in Anlehnung an die ISO 27002) und übernimmt die wesentlichen Funktionen.

Unsere Mitarbeiter, die bei einer externen Beauftragung zum Einsatz kommen, verfügen über die erforderliche Fachkunde und langjährige **Erfahrung**. Sie werden darüber hinaus durch UIMC-interne Spezialisten, wie z. B. auf Datenschutzrecht **spezialisierte Juristen** oder **Experten** auf dem Gebiet von IT-Systemen und der Informationssicherheit unterstützt.

Intern ist bei Ihnen lediglich ein Ansprechpartner zu benennen, der als Anlaufstation des UIMC-Teams dient und Anliegen intern weiterleitet.

Aufgabenwahrnehmung

Die Aufgaben werden durch unser Team wahrgenommen, indem es sowohl reaktiv auf Anfragen reagiert als auch proaktiv Empfehlungen ausspricht und Maßnahmen anstößt. Hierbei werden grundsätzlich Lösungen und Hilfestellungen angeboten. Die Aufgaben im Einzelnen sind auf der Seite 2 dargestellt und im Betreuungsvertrag transparent definiert.

Hierbei legen wir großen Wert auf Effizienz und Praxisnähe. So wird die Low-Budget-Idee unter Berücksichtigung der gesetzlichen Angemessenheit umgesetzt, indem unnötige Vor-Ort-Zeiten vermieden sowie Tools, Standards und Best Practice genutzt und auf umfassende Erfahrungen aus anderen Bestellungen zurückgegriffen werden.

Externe Beauftragung

- Sehr hohe Fachkompetenz
- Einkauf umfassender Erfahrungen
- Synergien aus Mehrfachbestellungen
- Kostenersparnis und kalkulierbare Kosten
- Keine Betriebsblindheit
- Neutralität bei „brisanten“ Themen (Mediator)
- Nutzung der „geliehenen“ Autorität eines Externen

Nutzen aus dem Outsourcing

- Kurzfristige Verfügbarkeit
- Berücksichtigung von pragmatischer Umsetzbarkeit („angemessener Datenschutz“)
- Kein Schulungsaufwand und Einarbeitungszeit für einen intern bestellten Datenschutzbeauftragten
- „Das Rad nicht neu erfinden“ (Best Practice)
- Effiziente Aufgabenerfüllung & effektive Lösungen
- Umfangreiches Datenschutz- und „Spezial“-Wissen

Vertrauen ist gut, Kontrolle ist besser

Nicht nur im Datenschutz ist es aufgrund der o. g. Rechtsgrundlage stets sinnvoll, zunächst den Status quo zu erheben, wodurch nicht nur Schwachstellen erkannt, sondern auch nur so strukturiert begegnet und behoben werden können.

Mit Hilfe des Analyse-Tools „UTAB“ (UIMC-Tool zur Analyse und Berichterstellung) werden die Anforderungen an Datenschutz und/oder Informationssicherheit computergestützt abgeprüft und Schwachstellen erkannt. Diese Form der Schwachstellenanalyse gestattet es, eine Bewertung der Ist-Situation vorzunehmen. Prüfungsinhalte sind entweder die gesetzlichen Anforderungen an den Datenschutz (Zulässigkeitsfragestellungen, technische und organisatorische Maßnahmen etc.) bzw. an die Informationssicherheit (u. a. Sicherungsmaßnahmen, die Sensibilisierung der Geschäftsführung und der Mitarbeiter).

Ergebnis: Status-Quo-Feststellung

Das Ergebnis wird in einem Status-Quo-Bericht mit Positiv- und Negativbefunden zusammengefasst. Für einen schnellen Einstieg befindet sich eine Management Summary mit farblicher Ampelkennzeichnung zu Beginn des Dokuments.

Eine quantitative Auswertung ermöglicht nicht nur eine zusammenfassende grafische Darstellung der Erhebungsergebnisse, sondern auch die Möglichkeit des Benchmarkings (z. B. Vergleich verschiedener Unternehmensbereichen) und der Trendanalyse, um den Fortschritt im Zeitverlauf zu erkennen.

Maßnahmenplanung

Die vorgeschlagenen Maßnahmen zur Schwachstellenbeseitigung werden durch die UIMC innerhalb einer Aktivitätenliste so vorpriorisiert, dass eine sukzessive Abarbeitung der Schwachstellen festgelegt werden kann. Dies ist erforderlich, weil Erfahrungswerte zeigen, dass ein gleichzeitiges Beseitigen verschiedenster Schwachstellen u. a. aus Effizienz-, Akzeptanz- und Effektivitätsgründen nicht sinnvoll ist.

§ 11 Absatz 2 BDSG [Auftragsdatenverarbeitung]: „Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. [...] Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.

Durch ein Dienstleister-Audit können Sie sich strukturiert, einfach und effizient von der Einhaltung der geforderten Maßnahmen beim Dienstleister überzeugen. Hierbei werden entsprechende Defizite gekennzeichnet, was Ihre Compliance und die Qualität der Dienstleistung verbessert.

Bildquelle: pixelio.de / Claudia Hautumm

Analyse und Auditierung

Folgende Leistungen können Sie im Rahmen der Auditierung und Analyse in Anspruch nehmen:

◆ Software-Tool

Sie erhalten unser Analyse-Tool als installierbare Software, die einen Fragenkatalog enthält und Sie sukzessive durch die Befragung führt. Es sind Hilfefunktionen (wie bspw. „Glossar“, „Flags”) integriert, die die Erhebung und Auswertung vereinfachen.

◆ Begleiteter Checkup

Die Analyse kann auch in Form eines Workshops durch einen Berater moderiert werden, der mediatorisch in Diskussionen eingreifen und Erfahrungen aus anderen Institutionen einbringen kann. So können relevante Themengebiete auch tiefergehend geprüft werden. Fehlbewertungen aufgrund unzureichender Erfahrungen und Kenntnisse können so vermieden werden.

◆ Regelmäßige Re-Audits

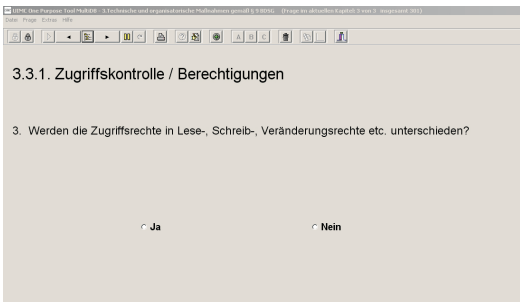
Die Ergebnisse der ersten Ist-Analyse sollte regelmäßig überprüft werden. Dies berücksichtigt nicht nur technische und rechtliche Änderungen, sondern auch Veränderungen innerhalb des Unternehmens. Nur durch eine regelmäßige Auditierung kann eine nachhaltige Umsetzung gewährleistet werden.

◆ Dienstleister-Auditierung

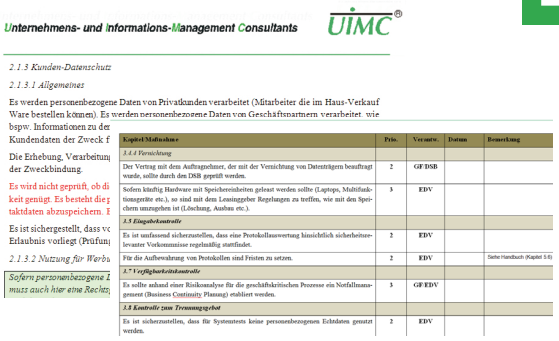
Durch eine Dienstleister-Auditierung, die individuell oder pauschal vereinbart werden kann, werden die Dienstleister nach den Vorgaben der §§ 11 BDSG geprüft; sei es im Rahmen des Auswahlverfahrens oder des „Sich-Überzeugens”. Auch hier erhalten Sie sowohl einen Bericht mit einem Risiko-Überblick als auch einen Maßnahmenkatalog, der vom Dienstleister umgesetzt werden sollte.

◆ Strategie- und Zielfindungs-Workshop

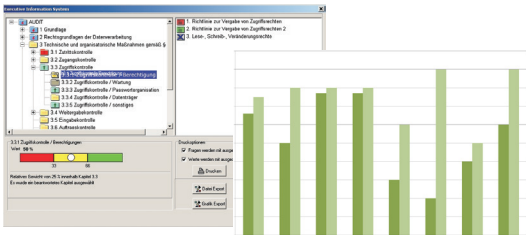
Für ein zielgerichtetes Arbeiten sollte am Anfang eine Datenschutzstrategie sowie die Datenschutzziele festgelegt werden. Hierdurch entsteht eine Norm, an der die Angemessenheit von zu realisierenden Maßnahmen beurteilt werden kann. Der Workshop wird computergestützt mit Hilfe der Szenariomethode abgewickelt. Die Ergebnisse werden in einem Zielpapier zusammengefasst und der Institution zur Verfügung gestellt. Hierauf sollten dann weitere Aktivitäten aufbauen



Während des Checkups beantworten Sie strukturiert die vorgebenen Fragen; trotz Multiple-Choice haben Sie mittels der Bemerkungsfunktion gute Individualisierungsmöglichkeiten.



Im **Status-Quo-Bericht** werden die Positiv- und Negativbefunde farblich dargestellt; in einem **Maßnahmenkatalog** können alle Empfehlungen priorisiert und einem Verantwortlichen zugeorndet werden.



Durch die quantitative Komponente erhalten Sie nicht nur einen **schnellen Überblick**, sondern können auch weitere Auswertungen erstellen und die Ergebnisse z. B. mittels Excel grafisch darstellen.

Verbindlichkeit und Transparenz

Neben Schulung und Sensibilisierung der Mitarbeiter kann der Datenschutz und die Informationssicherheit sinnvoll nur mit der Schaffung transparenter, verbindlicher Regelungen erreicht werden. Dies ist auch deswegen wichtig, weil die Geschäftsführung als Verantwortliche für den Datenschutz nur so ihrer **Organisationsschuld** ausreichend nachkommen kann.

Wer schreibt, der bleibt...

Aufgrund der fehlenden Weisungsbefugnis des Datenschutzbeauftragten ist ein verbindliches Regelwerk zu schaffen. Dies ist erforderlich, da fehlende verbindliche organisatorische Regelungen immer wieder innerhalb von Institutionen dazu führen, dass technische Maßnahmen zur Gewährleistung des Datenschutzes unterlaufen werden.

Verbindlichkeit und Transparenz

Das Regelwerk sollte alle aufbau- und ablauforganisatorischen Fragestellungen beachten, welche allgemein verbindlich sind. Das Handbuch ist hierfür eine ideale Basis. Das standardisierte, auf langjährige Erfahrung, den Datenschutzgesetzen und etablierten Sicherheitsnormen (beispielsweise der ISO 27002) basierende Regelwerk ist modular aufgebaut, wodurch es an jede Institution spezifisch anpassbar ist.

Zentrales Regelwerk

Die übergeordneten Ziele des Handbuchs sind generell die Unterstützung der Schaffung von Informationssicherheit und Datenschutz sowie die Dokumentation aller diesbezüglichen Entscheidungen. Das Organisations-Kit ist von seinen Zielen her:

» Organisationsmittel,
» Informationsquelle,
» Schaffung von Transparenz der organisatorischen Tatbestände,
» Führungsinstrument,
» Kontrollgrundlage für Vorgesetzte und Mitarbeiter,

sowie

» Hilfe für Mitarbeiter bei ihrer Arbeit sowie bei der Beantwortung von Zweifelsfragen,
» Bezugspunkt für das gesamte Problem des Datenschutzes bei der täglichen Arbeit.

Verzahnung: Umsetzung des Schwachstellenbeseitigungs-Konzepts

Sämtliche unserer Produkte und Leistungen sind miteinander verzahnt. Die Abweichungen auf Basis der Ist-Analyse werden organisatorisch durch das Organisations-Kit abgedeckt. Mit Hilfe des Maßnahmenkatalogs im Sinne eines Schwachstellenbeseitigungs-Konzepts und des Organisations-Kits kann somit relativ schnell der Datenschutz verbessert und die kritischen Schwachstellen beseitigt werden.

Das Datenschutz-Handbuch bildet die Basis für die Arbeit des Beauftragten und für die sukzessive Umsetzung bei Ihnen.

Bildquelle: pixelio.de / Rainer Sturm

Datenschutz-Handbuch

Handbuch und Formulare

Im Standard-Handbuch sind all jene Regelungen und Richtlinien als Muster enthalten, die für die Umsetzung des Datenschutzes und/oder der Infomationssicherheit erforderlich sind. Ferner sind Formulare wie z. B.

» rechtskonforme Muster-Einwilligungserklärungen,
» Verpflichtungserklärungen,
» Richtlinien für die Nutzung spezieller IT (wie beispielsweise Smartphones oder Laptops),
» Checklisten,
» Informationsblätter für verschiedene Fachbereiche (wie beispielsweise Personalwesen, IT- und Marketing-Abteilung)
» Muster-Verträge usw.

zur schnellen Umsetzung enthalten.

Eine Anpassung an das Unternehmen findet nicht statt. Modifikationen sind im Rahmen von zusätzlichen Beratungsleistungen aber möglich.

Informationssicherheit integrieren

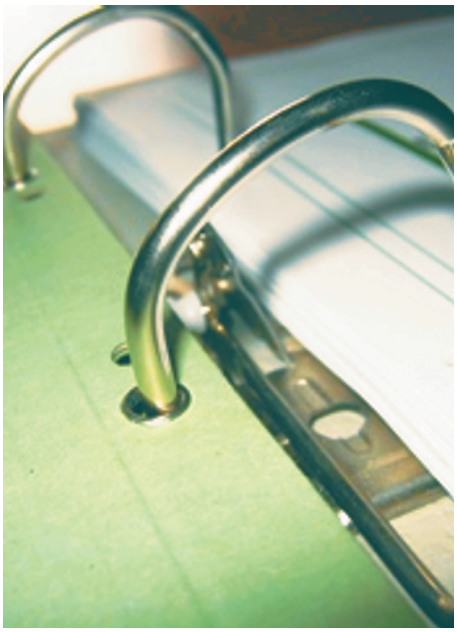
Aufgrund der hohen Schnittmenge von Datenschutz und der Informationssicherheit ist eine integrierte Regelung in Form eines integrierten Handbuchs zu empfehlen. Dies schafft noch mehr Akzeptanz und nutzt Synergien. Redundanzen und Widersprüche werden vermieden.

Basis für eine Zertifizierung

Ganz nach dem Motto „Tue Gutes und sprich darüber“ ist es bisweilen für die Außen-, aber auch Innenvermarktung sinnvoll, eine Zertifizierung anzustreben. Unser Handbuch bietet eine ideale Basis für die erforderliche Dokumentation im Zertifizierungsprozess.

Auszug aus dem Muster-Datenschutzhandbuch

1 Einleitung
2 Strukturorganisatorische Regeln
3 Übergreifende Richtlinien
3.1 Klassifizierung von Informationen
3.2 Schulungsrichtlinie
3.3 Personalrichtlinie
4 Verwaltung des IT-Systems
5 Berechtigungen
6 Arbeitsplätze
6.1 IT-unterstützte Arbeitsplätze
6.2 Mobile Devices
6.3 Telearbeit (Home Office)
7 Kommunikation
8 Notfall-Management
9 Datenschutzrelevante Richtlinien
10 Gesetzesspezifische Richtlinien
11 Vertragsspezifische Richtlinien
12 Formale Richtlinien



Organisation

Die Vorteile

» Umfassendes Regelwerk
» Allgemein verbindlich geltende Regelungen und Führungsinstrument
» Bewährung durch langjährige Praxiserfahrungen der UIMC
» In Anlehnung an anerkannte Normen
» Übersichtlichkeit durch Unterteilung im allgemeinen Regelungs- und Formularteil

Ihr Nutzen

» Gesetzeskonformität
» Schaffung von Transparenz
» Verbesserung des Datenschutzes
» Praxisgerechte Umsetzung des Datenschutzes
» Kostengünstiger im Vergleich zur eigenständigen Erstellung eines Regelwerks
» Effiziente Zertifizierungsvorbereitung

Berücksichtigung des „Faktors Mensch“

„[Der Datenschutzbeauftragte hat] die mit der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz und mit den jeweiligen Erfordernissen des Datenschutzes vertraut zu machen.“

Zur effektiven Umsetzung von Anforderungen ist es unerlässlich, die Mitarbeiter zu sensibilisieren und auf die zu ergreifenden Maßnahmen zu schulen (dies gilt nicht nur aufgrund der o. g. Gesetzesanforderung für den Datenschutz, sondern auch für die Informationssicherheit). Die Erfahrung zeigt, dass Vorgaben nur eingehalten werden, wenn Mitarbeiter die Hintergründe verstehen. Andernfalls werden entweder bewusst Regeln umgangen, weil sie als „lästig“ empfunden, oder unbewusst aus Unwissen gegen diese verstoßen.

Wie bieten hierzu verschiedene Möglichkeiten, die alternativ oder ergänzend im Unternehmen umgesetzt werden können. Gerne erstellen wir ein individuelles Schulungskonzept.

Seminare und Workshops

Die Mitarbeiter werden durch uns im Rahmen eines ca. 1,5-stündigen Seminars persönlich geschult. Hierbei können Fragen direkt mit dem Referenten diskutiert werden.

Auch spezielle Schulungen und Workshops für einzelne Bereiche oder Teams sind denkbar, wie z. B. Personal- und IT-Bereich, Betriebsrat oder Geschäftsführung bzw. Management.

Awareness-Kampagne

Je nach Bedeutung und/oder Risiken, kann es erforderlich sein, die Mitarbeiter so umfassend zu sensibilisieren, dass „gewöhnliche“ Schulungsmaßnahmen nicht mehr ausreichend sind. Hierbei können wir gemeinsam mit Ihnen eine zugeschnittene Kampagne entwickeln, um die Mitarbeiter in ihrem Arbeitsalltag auch für diese Themen zu erreichen.

eCollege als browsergestütztes E-Learning

E-Learning kann eine sinnvolle Alternative oder Ergänzung zu klassischen Schulungen sein. Gerade in dezentral organisierten Institutionen kann E-Learning eine effiziente Umsetzungsmethodik sein. Über den Browser kann auf die Selbstschulungen via Internet zugegriffen werden (auch ohne VPN-Zugang des Mitarbeiters).

Je nach gewähltem Modul bzw. Paket (näheres auf der Folgeseite) können verschiedene Lerninhalte durchgearbeitet sowie zusätzliche Inhalte und auch Funktionen genutzt werden.

Bildquelle: pixelio.de / C. Nöhren

Schulung und Sensibilisierung

Nachfolgend geben wir Ihnen einen Überblick über die Funktionen des eCollege (Weiterführende Informationen finden Sie in unserer eColege-Broschüre):

◆ Wissensvermittlung und -management

Neben den Lerninhalten können weitere Informationen hinterlegt werden, wie beispielsweise das Handbuch, Richtlinien, Betriebsvereinbarungen oder Formulare. Somit wird das eCollege als Wissensmanagement-System (auch zur Qualitätssicherung) zum zentralen Informationsstandort werden.

◆ Bestätigung mit wenigen „Klicks“

Alternativ zur schriftlichen Bestätigung, bei der die Mitarbeiter ein PDF-Formular ausdrucken und dies dann unterschrieben an den Personalbereich weiterleiten, kann die Bestätigung auch elektronisch geschehen. Hierbei wird eine vorkonfigurierte E-Mail erzeugt, die nach einer kurzen Ergänzung nur noch abgeschickt werden muss.

◆ Nachhaltigkeit durch Selbst-Tests

Durch die Möglichkeit eines Selbst-Tests wird den Mitarbeitern die Chance geboten, erlerntes Wissen selbst zu überprüfen. So können Multiple-Choice-Fragen bearbeitet werden, auf die eine sofortige Rückmeldung gegeben wird, ob die Frage korrekt oder (teilweise) fehlerhaft ist. Durch Lernerfolge kann eine höhere Motivation geschaffen werden.

◆ Modular und skalierbar

Das eCollege bietet in verschiedenen Paketen unterschiedliche Funktionen, die wir im Block auf der rechten Seite darstellen. Auch können weitere Wissensgebiete, wie bspw. Informationssicherheit bzw. der Datenschutz oder eigene Themen jederzeit problemlos ergänzt werden.

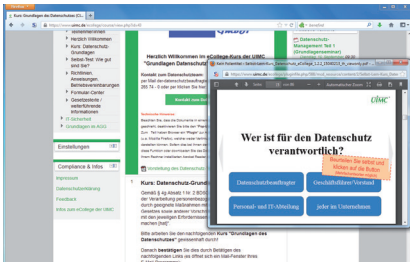
Modul Basic

- Einheitlicher Zugang für alle Mitarbeiter (Gruppenaccount)
- Grundlagen-Schulungsunterlagen in eigenem Kursraum
- allgemeine weiterführende Informationen
- Formular-Center mit Muster-Formularen

Modul Classic

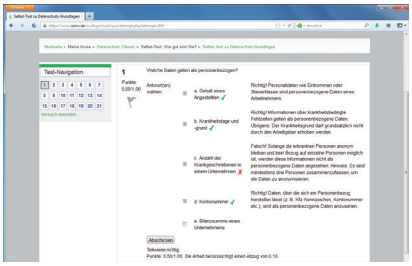
- wie Basic
- personalisierter Zugang für jeden Mitarbeiter
- Möglichkeit zum Selbsttest
- Vorstellung der Ansprechpartner (wie z. B. DSB)
- Automatisierung durch elektronische Bestätigung durch User
- Veröffentlichung von internen Formularen, Richtlinien und weiterer Informationen

Abb.: Inhalte der Module/Pakete



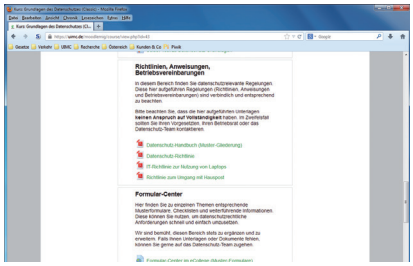
Vielfältige Themenangebote

Im eCollege haben wir verschiedene Themengebiete bereits aufbereitet, wie bspw. Datenschutz (zu allen Rechtsgrundlagen) und Informationssicherheit. Weitere Themen erarbeiten wir gerne, auch gemeinsam mit Ihnen.



Testen von Erlernten

Hierzu bietet die UIMC im eCollege verschiedene vorgefertigte Schulungspakete, die sich nach Umfang, Detailtiefe und -breite sowie Branchenfokus unterscheiden. Ferner haben Sie die Möglichkeit, weitere Inhalte selbst zu erstellen oder individuell durch die UIMC erarbeiten zu lassen.



Organisationsschuld und Effektivität verbessern

Die organisatorischen Regelungen müssen, um der Organisationsschuld der Geschäftsführung nachkommen zu können, nicht nur verständlich, sondern auch leicht auffindbar sein. Wir veröffentlichen an gleicher Stelle auch wichtige Richtlinien.

Low-Budget-Idee für KMU

Auch wenn die gesetzliche Basis in Form der datenschutzrelevanten Gesetze für alle Unternehmen generell gleich ist, so erfordert die Umsetzung eine jeweils passende Lösung. Gerade in kleinen und mittleren Unternehmen (KMU), deren Kerngeschäft nicht maßgeblich durch den Datenschutz beeinflusst wird, sind angemessene Lösungen notwendig.

Die Low-Budget-Idee

Im Outsourcing sind die Vor-Ort-Leistungen des beratenden Unternehmens die teuersten Leistungen. Es ist aus Effizienzgründen Ziel, diese Leistungen zu reduzieren. Durch Nutzung

- moderner Kommunikationstechniken,
- standardisierter Organisationsmittel mit Best Practice sowie
- computergestützter Verfahren und Tools (z. B. für die Analyse und Schulung)

werden hoch individuelle und Vor-Ort-Leistungen reduziert und optimiert. Dadurch werden der interne Aufwand und die externen Kosten für Sie optimiert. Der Bedeutung des Datenschutzes wird dabei durch uns und unsere Organisationsmittel Rechnung getragen, aber nicht überbetont und überbewertet.

Externe bieten Neutralität

„Der Prophet im eigenen Land“ wird oftmals nicht erhört. Deshalb kann ein Externer in der Regel unvoreingenommener an Fragestellungen herangehen und notwendige Maßnahmen vorantreiben kann. Auch wird ein extern bestellter Datenschutzbeauftragter vom eigenen Betriebsrat vielfach als neutraler wahrgenommen. So treten wir auch als „Sachverständiger“ gemäß § 80 BetrVG auf und berät Arbeitnehmer- und Arbeitgebervertreter gleichermaßen fachlich kompetent und nicht politisch.

Pauschalen bringen Planungssicherheit

Gerade in KMU und Mittelstand ist eine hohe Planungssicherheit im Hinblick auf die Kosten sehr wichtig. Daher ist ein zentrales Element der Low-Budget-Idee, die Leistungen pauschaliert abzurechnen. Hierbei werden niedrige monaltliche Pauschalen genutzt.

Die Paket-Idee

Die Bedürfnisse und Anforderungen an eine Umsetzung sind oft sehr unterschiedlich. In Form von Paketen haben wir sinnvolle Leistungen und Produkte so zusammengefasst, dass diese auf unterschiedliche Rahmenbedingungen und Anforderungen zutreffen. Von einer standardisierten Basis-Betreuung bis hin zur umfassenden, individuellen Betreuung haben Sie die Wahl der für Sie passenden Unterstützung.

Nichtsdestotrotz bleiben Sie vollkommen flexibel: Sei es durch eine situative Zusatzleistung („Wir brauchen Unterstützung bei einem Audit!“) oder das grundsätzliche Hinzubuchen von anderen Paketbestandteilen (z. B. der Wunsch nach regelmäßigen Vor-Ort-Besprechungen).

Bildquelle: pixelio.de / Illustration Marcus Stark

Informationssicherheit mit System

Mit zunehmender Durchdringung der Unternehmen durch die Informationsverarbeitungstechnologie erhöht sich auch die Abhängigkeit. Dies führt dazu, dass die Anforderungen an die Sicherheit des Informationssystems stetig wachsen. Um sowohl das Risiko, gravierende Sicherheitsprobleme zu übersehen, zu minimieren als auch möglichst schnell, effektiv und effizient auf neue Probleme eingehen zu können, muss die Informationssicherheit in all ihren Facetten betrachtet werden.

In einer modernen Institution ist es deshalb notwendig, ein Informationssicherheitskonzept zu erarbeiten, das technische, organisatorische und personelle Fragen berücksichtigt. Als Basis hierfür können verschiedene Normen herangezogen werden, die einem bei dem Aufbau eines Informationssicherheits-Managementsystems (ISMS) Hilfestellung leisten.

Aufbau eines ISMS

Um ein ISMS in einem Unternehmen aufzubauen, hat sich eine stufenweise aufeinander aufbauende Vorgehensweise bewährt:

Dieses Vorgehensmodell orientiert sich an den gängigen Normen zum Informationssicherheits-Managementsystem (ISO/IEC 27001 und 27002) und ist seit Jahren aufgrund seiner Praktikabilität anerkannt. Im Ergebnis entsteht ein Managementsystem, durch das sichergestellt werden kann, dass die Informationssicherheit im Unternehmen gelebt wird, dass sie auf die Bedürfnisse des Unternehmens angepasst ist und dass alle wichtigen Aspekte erfasst werden.

Business Continuity / Notfallmanagement

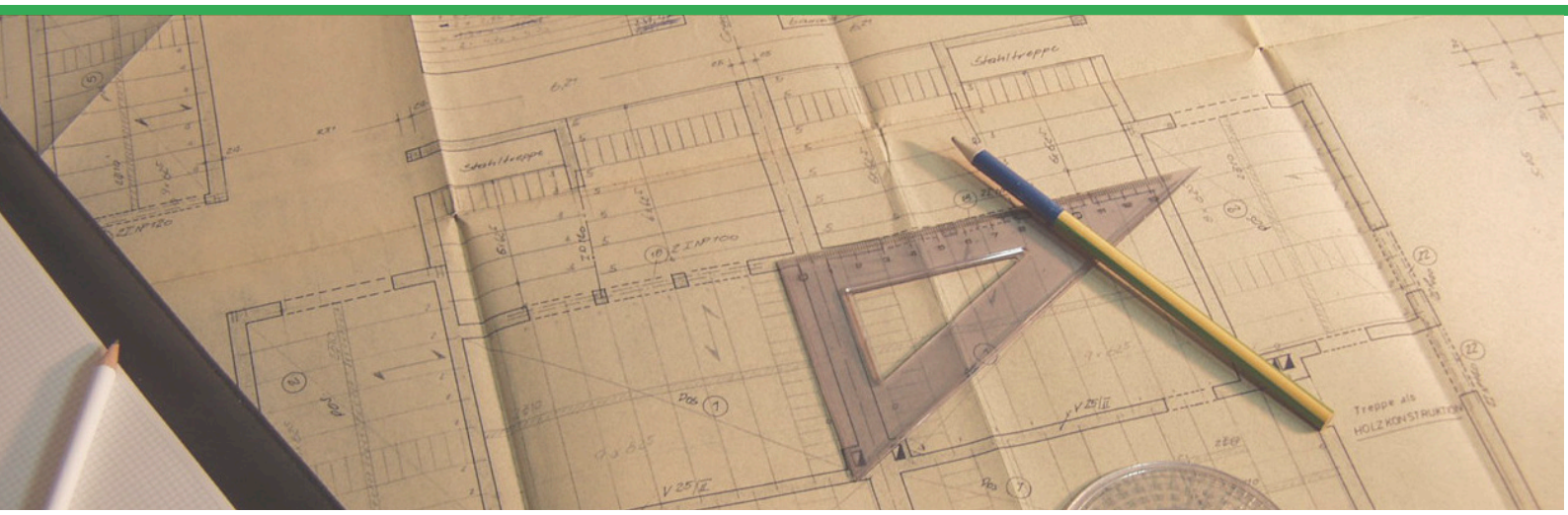
Aufgrund der stetig zunehmenden Abhängigkeit aller Institutionen von der Informationsverarbeitung ist die Aufrechterhaltung des Geschäftsbetriebs auch bei gravierenden Störungen der Informationsverarbeitung von ganz besonderer Bedeutung. Dies sicherzustellen ist Aufgabe der Business Continuity, die dafür Sorge trägt, dass auch im Falle gravierender Störungen die kritischen Geschäftsprozesse in ihrer Funktionsfähigkeit erhalten bleiben. Somit ist das Business-Continuity-Management (BCM) eine Tätigkeit, die über die reine Betrachtung der Informationsverarbeitung hinausgeht und die organisatorischen Prozesse im Fokus hat.

Das Notfallmanagement wie auch Business-/Disaster-Recovery-Management sind häufig verwendete Begriffe, die in der Regel einen stärkeren informationstechnischen Schwerpunkt setzen, und somit als Teile des BCM angesehen werden können.

Penetrationstest

Um möglichen Gefährdungen entgegenzuwirken und vorzubeugen, sind Maßnahmen zur kontinuierlichen Verbesserung der IT-Sicherheit zu ergreifen. Sicherheit definiert sich durch Sicherheitsorganisation und Eskalationsvorschriften, technische und organisatorische Maßnahmen, wie Zugriffsschutzmechanismen und Mitarbeitersensibilisierung, Verschlüsselung und Firewallsysteme, mit dem Ziel, ein bestimmtes IT-Sicherheitsniveau zu etablieren. Diese und weitere Aspekte sollten in einer unternehmensweiten IT-Sicherheitsleitlinie („IT-Security Policy“) bzw. in einem organisationsweiten IT-Sicherheitskonzept zusammengeführt werden.

Präzise Prüfungen bis zum Zertifikat



UIMCert® GmbH

Wir, die UIMCert GmbH, sind eine Schwestergesellschaft der UIMC Dr. Vossbein GmbH & Co KG. Gesellschafter der UIMCert sind die UIMC Dr. Vossbein Betriebs-GmbH und Dr. Heiko Haaz. Wir haben einen Fachbeirat, der die Geschäftsführung in wichtigen Fragen im Bereich IT-Management, IT-Sicherheit sowie Datenschutz und Zertifizierung berät.

Wir verfügen über qualifiziertes Personal für die Auditierung und Zertifizierung in den genannten Bereichen. Wir sind **bei der DAkkS für den Standard ISO 27001** und beim **Unabhängigen Landeszentrum für den Datenschutz (ULD) für Datenschutzauditierung** akkreditiert. Wir haben darüber hinaus eigene Prüfsysteme für IT-Sicherheit und Datenschutz (datenverarbeitende Stellen und Produkte) entwickelt, innerhalb derer wir nach erfolgreicher Auditierung gemäß prüfbaren standardisierten Normen ein eingetragenes Gütesiegel verleihen.

UIMCollege®

Wir führen Schulungen und **Fortbildungsmaßnahmen** auf den Sektoren Auditierung, Revision, Datenschutz und IT-Sicherheit durch und entwickeln Lernprogramme und -software. Durch die Verbindung mit der UIMC stehen uns die von der UIMC entwickelten Tools zur Verfügung, die eine hohe Effizienz durch das computerisierte Arbeiten insbesondere bei der Auditierung ermöglichen.

Informationssicherheit

- ISO 27001 (nativ)
- ISO 27001 auf Basis IT-Grundschutz
- Umsetzung des Best Practice ISO 27002
- interne Audits /Analysen (SiSSA)

Informationsmanagement

- ISO 20000 (Service-Management)
- Auswahl & Prüfung einzelner Bausteine

Datenschutz

- ULD-Gütesiegel
- UIMCert-Gütesiegel [Stellen, Produkte und Verfahren]
- Audit von Dienstleistern (Datenschutz und Informationssicherheit)
- Vorabkontrollen
- interne Audits /Analysen (Datenschutz-Checkup)

Bildquelle: pixelio.de / Siegried Fries

Wir stellen uns vor: Die UIMC

Wir sind eine gesellschaftergeführte, mittelständische Unternehmensberatung mit den Kerngebieten **Datenschutz** und **Informationssicherheit**. Schon bei der Gründung 1997 haben wir einen Schwerpunkt unserer Beratungstätigkeit auf die Konzeptionierung und Umsetzungsunterstützung auf Basis von Best-Practice-Normen gelegt.

Vollsortimenter

Im Datenschutz gehören wir zu den Marktführern und bieten als Vollsortimenter von einzelnen Tools und Stellungnahmen bis hin zum Komplett-Outsourcing in Form einer externen Datenschutzbeauftragung sämtliche Unterstützungsmöglichkeiten der Analyse, Beratung, Umsetzung und Schulung/Sensibilisierung an.

Pragmatische Lösungen

Durch unsere vielfältigen Fach-, Branchen- und Methodenkompetenz arbeiten wir stets an pragmatischen Lösungen, mit denen Sie Ihrer Verantwortung gerecht werden und die Risiken maßgeblich reduzieren. Hierbei profitieren Sie von unserer Größe, durch die wir einerseits umfangreichere Projekte ohne Abhängigkeit von einzelnen Mitarbeitern durchführen und andererseits flexibel auf Ihre individuellen Bedürfnisse eingehen können.

Auch die breit gefächerten Spezialisierungen unserer Mitarbeiter sowie die Nähe zu unserer „Zertifizierungsschwester“ bringen wir zu Ihrem Nutzen ein.

Nachhaltigkeit

Die aufgrund der hohen Qualität und Zufriedenheit langfristigen Kundenbeziehungen haben zu einer stetigen Ausdehnung unseres regionalen und fachlichen Tätigkeitsgebiets geführt. Hierbei legen die Inhaber nicht nur Wert auf solides, sondern auch nachhaltiges Wachstum.

Datenschutz von A bis Z

Wir bieten eine **Betreuung von A bis Z** aus einer Hand: Von der Ausbildung der Mitarbeiter oder des internen Beauftragten, der Begutachtung des Unternehmens oder von Geschäftspartner/Dienstleistern über das Computergestützte Lernen (E-Learning) sowie die Übernahme aller Aufgaben als Externer Datenschutzbeauftragter bis hin zur Zertifizierungsvorbereitung.

IT-Sicherheit mit System

Die Notwendigkeit zum Aufbau eines Informationssicherheits-Managementsystems ist mittlerweile allgemein erkannt, doch bestehen oftmals Probleme in der Umsetzung. Hierbei zeigt sich, dass die ISO 27002 ideal ist, um die Situation der **Informationssicherheit** im Unternehmen zu analysieren und zu verbessern, was eine wesentliche Säule für eine verbesserte Compliance-Situation darstellt.

Management und mehr

Die UIMC weist auch Referenzen im Bereich verschiedenster organisatorischer Fragestellungen auf. Von **vorstrukturierten Problemen** wie der Erstellung eines Archivierungskonzepts oder Erarbeitung von Betriebsvereinbarungen **bis hin zu individuellen Problemstellungen** wie die Effizienzverbesserung von Geschäftsabläufen: Die UIMC kann Sie unterstützen.

Unsere Leistungsgebiete:

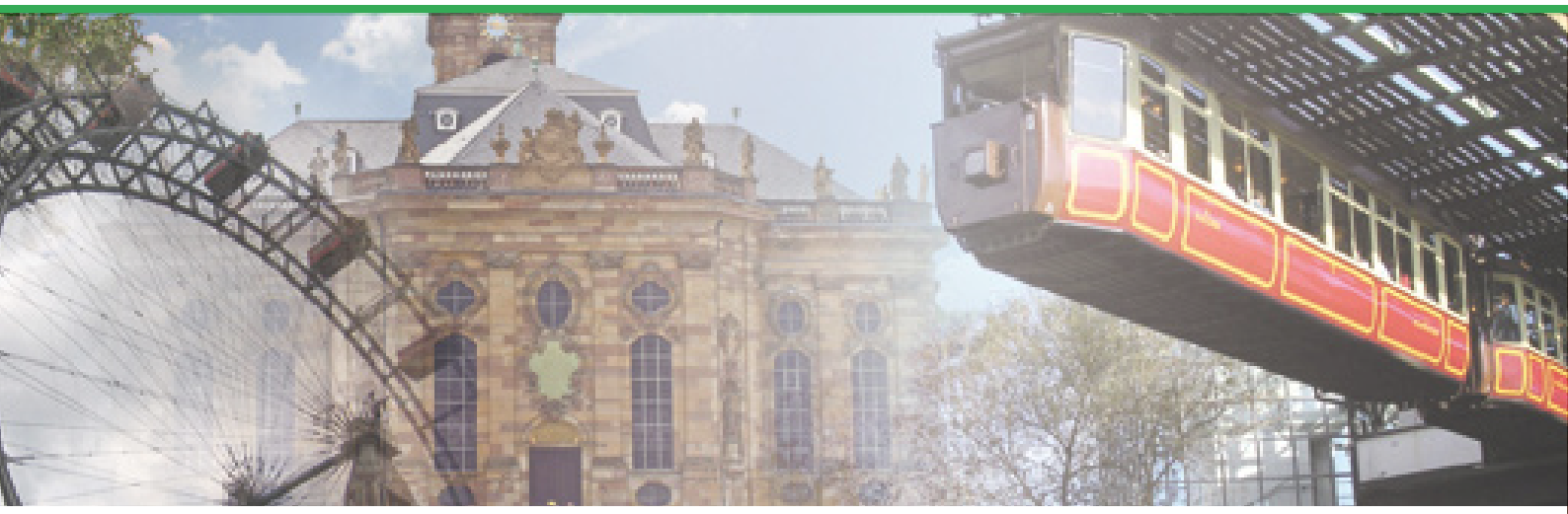
Datenschutz
Von einzelnen Stellungnahmen und Tools bis zur Übernahme der externen Datenschutzbeauftragung

Informationssicherheit
Aufbau eines Informationssicherheits-Managementsystems auch bis zur Zertifizierungsreife

Organisation/ Strategie
Beratungsleistungen in konzeptionellen und strategischen Fragestellungen

Analyse / Auditierung | Planung & Beratung | Konzept-Erarbeitung | Schulung & Sensibilisierung | Umsetzung (mit Tools)

Unsere Leistungen im Datenschutz



Wir sind eine gesellschaftergeführte, mittelständische Unternehmensberatung mit den Kerngebieten **Datenschutz** und **Informationssicherheit**. Schon bei der Gründung 1997 haben wir einen Schwerpunkt unserer Beratungstätigkeit auf die Konzeptionierung und Umsetzungsunterstützung auf Basis von Best-Practice-Normen gelegt.

Vollsortimenter

Im Datenschutz gehören wir zu den Marktführern und bieten als Vollsortimenter von einzelnen Tools und Stellungnahmen bis hin zum Komplett-Outsourcing in Form einer externen Datenschutzbeauftragung sämt-liche Unterstützungsmöglichkeiten der Analyse, Beratung, Umsetzung und Schulung/ Sensibilisierung an.

Datenschutz von A bis Z

Wir bieten eine **Betreuung von A bis Z** aus einer Hand: Von der **A**usbildung der Mitarbeiter oder des internen Beauftragten, der **B**egutachtung des Unternehmens oder von Geschäftspartner/Dienstleistern über das **C**omputergestützte Lernen (E-Learning) sowie die Übernahme aller Aufgaben als Externer **Datenschutzbeauftragter** bis hin zur **Z**ertifizierungsvorbereitung.

- Datenschutz-Checkup
- Umsetzungsplanung und -beratung
- Etablierung eines Konzepts
- Schulung und Sensibilisierung
- Umsetzung (u. a. mit Hilfe von Tools)
- (regelmäßige) Auditierung

Bilder: Gecko, LucB7, Susanne Wetzel / pixelio.de

UIMC®
UIMC Dr. Vossbein GmbH & Co KG
Nützenberger Straße 119, 42115 Wuppertal
consultants@uimc.de, Tel: 0202 / 265 74 - 0

Vorteile und Nutzen

- Praxisgerechte Umsetzung des Datenschutzes und Erfüllung gesetzlicher Vorgaben
- Individuelle Unterstützung entsprechend Ihrer Wünsche und Anforderungen sowie flexibles „Hinzubuchen“ von weiteren Leistungen
- Nutzung von bewährtem, effizientem „Best Practice“
- Nutzung von aufeinander abgestimmten Komponenten
- Synergiepotentiale durch integrierte Betreuung von Datenschutz und Informationssicherheit möglich
- Hohe interne Akzeptanz aufgrund optimierter Lösungen
- Hohe externe Akzeptanz durch „Datenschutz-Profis“
- Hohe Fachkompetenz und Synergien aus Mehrfachbestellungen
- Keine Betriebsblindheit
- Kurzfristige Verfügbarkeit ohne Schulungsaufwand
- Effiziente Aufgabenerfüllung