Security - Das Dienstleistungspaket für rundum Datensicherheit in Ihrem Unternehmen.

IT-Sicherheit Datenschutzbeauftragter aktive Schutzmaßnahmen

Sehr geehrter Kunde und Interessent,

wir freuen uns das Sie sich für das IT-Outsourcing Modell (flexpo-security) interessieren und damit die F&M Consulting als einen IT- Full Service Partner für sich gewinnen möchten.

Anbei einige Grundlagen zum Thema Datenschutz und Datensicherheit sowie das F&M Leistungspaket für Ihre sichere und hochverfügbare IT Landschaft.

Datenschutz und Informationssicherheit

Informationssicherheit ist eine wesentliche Voraussetzung zur Umsetzung des Datenschutzes in Unternehmen. Sie umfasst neben der Sicherheit von IT-Systemen und den damit verarbeiteten und darin gespeicherten Daten auch die Sicherheit von nicht-elektronisch verarbeiteten Informationen. Ein wesentlicher Bestandteil der Informationssicherheit ist die **Datensicherheit**.

Was ist Datensicherheit und welche Anforderungen bestehen ?

Die Datensicherheit verfolgt das Ziel, im Prozess der Datenverarbeitung vor Verlust, Zerstörung, Verfälschung, unbefugter Kenntnisnahme und unberechtigter Verarbeitung der Daten zu schützen.

Es muss gewährleistet sein, dass insbesondere

- der Zugriff auf die Daten und somit deren Kenntnisnahme ausschließlich durch **autorisierte Benutzer** erfolgt; das Gleiche gilt für die Modifikation (Ändern und Löschen) von Daten,

Tiergartenstraße 54g
D-47053 Duisburg
☎ : +49 (0)203/ 608499-10
Fax : +49 (0)203 / 608499-11

- Daten **nicht unbemerkt** verändert werden können, sondern Änderungen **nachvollziehbar** sind,
- der **Zugriff auf Daten** innerhalb eines festgelegten Zeitraums für entsprechend autorisierte Nutzer gewährleistet ist und die **Funktionalität der IT-Systeme** nicht beeinträchtigt ist.

Welche Maßnahmen sind zu treffen ?

In Deutschland sind alle Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten oder nutzen, gesetzlich verpflichtet, die erforderlichen und angemessenen **technischen und organisatorischen Maßnahmen** zum Erzielen und Aufrechterhalten der Datensicherheit zu treffen. Dies ergibt sich insbesondere aus § 9 des Bundesdatenschutzgesetzes (BDSG) in Verbindung mit der Anlage zu § 9 Satz 1 BDSG.

Der Anforderungskatalog listet eine Reihe von Maßnahmen auf, um das Ziel Datensicherheit zu erreichen. Die gesetzlichen Anforderungen an die erforderlichen Datensicherungsmaßnahmen sind im Gesetz jedoch flexibel gehalten, da sie u.a. unabhängig von einem bestimmten Stand der Technik und verwendeten Medien beschrieben werden.

Generell gilt, dass sich die zu treffenden Maßnahmen an den zu schützenden Unternehmenswerten zu orientieren haben. Hierfür bietet sich zunächst die Durchführung einer **Schutzbedarfsanalyse** als Grundlage eines **Sicherheitskonzepts** an, um zu ermitteln, welcher Schutz für die Informationen und die eingesetzte Informationstechnik erforderlich sowie angemessen ist.

Besonderes Augenmerk sollte hierbei vor allem auch in Bezug auf den Einsatz privater mobiler Endgeräte zu Unternehmenszwecken liegen.

Welche technischen und organisatorischen Maßnahmen sind konkret gemeint ?

Die Anlage zu § 9 Satz 1 BDSG listet in den Nummern 1 bis 8 Maßnahmen auf:

Maßnahmen zur Zutrittskontrolle

Zutrittskontrollmaßnahmen sollen Unbefugten den physischen Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehren. Beispiele für die Umsetzung der Maßnahme sind die Verwendung von Berechtigungsausweisen ggf. mit integriertem Zutrittstransponder (RFID) oder der Einsatz von Alarmanlagen oder Überwachungseinrichtungen.

Tiergartenstraße 54g
D-47053 Duisburg
☎ : +49 (0)203/ 608499-10
Fax : +49 (0)203 / 608499-11

Maßnahmen zur Zugangskontrolle

Zugangskontrollmaßnahmen sollen verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Zur Umsetzung dieser Kontrollmaßnahme kommt beispielsweise ein effektives Passwortmanagement – ggf. mit Zwei-Faktor-Authentifikation – sowie eine entsprechende Protokollierung der Passwortnutzung in Betracht.

Maßnahmen zur Zugriffskontrolle

Zugriffskontrollmaßnahmen sollen gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer **Zugriffsberechtigung** unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Demnach können solche Maßnahmen z.B. in Form von rollenbasierten Berechtigungskonzepten umgesetzt werden.

Maßnahmen zur Weitergabekontrolle

Mit der Weitergabekontrolle soll verhindert werden, dass personenbezogene Daten bei der elektronischen Übertragung, während ihres Transports oder ihrer Speicherung auf Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können. Es soll zudem überprüft und festgestellt werden können, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Als Maßnahmen kommen u.a. Regelungen zur Datenträgervernichtung, Taschenkontrollen etc. in Betracht.

§ 9 Satz 2 BDSG stellt explizit heraus, dass die Verwendung eines dem Stand der Technik entsprechenden **Verschlüsselungsverfahrens** eine Maßnahme für die Zugangs-, Zugriffs- sowie Weitergabekontrolle ist.

Maßnahmen zur Eingabekontrolle

Die Eingabekontrolle soll gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben, verändert, d. h. auch gelöscht und entfernt worden sind. In Betracht kommt hier die Protokollierung von Dateneingaben sowie -löschungen.

Tiergartenstraße 54g
D-47053 Duisburg
☎ : +49 (0)203/ 608499-10
Fax : +49 (0)203 / 608499-11

Maßnahmen zur Auftragskontrolle

Im Rahmen der Auftragskontrolle hat der Auftragnehmer zu gewährleisten, dass die im Auftrag zu verarbeitenden Daten nur entsprechend den Weisungen des Auftraggebers verarbeitet werden. Der Auftraggeber hat dem Auftragnehmer im Rahmen der Auftragsdatenverarbeitung daher entsprechende **Weisungen** zu erteilen und die Einhaltung dieser durch den Auftragnehmer regelmäßig zu **kontrollieren**. Die entsprechenden Abreden hierzu, insbesondere auch die Befugnis zur Unterbeauftragung weiterer Dienstleister sind **schriftlich** zu treffen.

Maßnahmen zur Verfügbarkeitskontrolle

Die Kontrollmaßnahmen zur Verfügbarkeit sollen gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind, insbesondere durch Vorfälle wie Stromausfall, Blitzschlag, Feuer- und Wasserschäden. Sicherungsmaßnahmen wie z.B. Einsatz einer unterbrechungsfreien Stromversorgung (USV) oder von Notstromaggregaten, Erstellung von Backups sowie deren Auslagerung etc. sollten in einem Notfallplan festgehalten werden.

Maßnahmen zur Erfüllung des Trennungsgebots

Ziel des Trennungsgebots ist, zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Umgesetzt werden kann dieses Ziel z.B. durch die Verwendung von mandantenfähiger Software und entsprechend konzipierten Zugriffsberechtigungen. Eine Herausforderung zur Einhaltung des Zweckbindungsgrundsatzes stellt sich bei der Verwendung von CRM-Systemen.

IT-Grundschutz

Insbesondere hinsichtlich der im Unternehmen verwendeten IT-Systeme bieten die IT-Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI) eine Auswahl an geeigneten Maßnahmen zur Erreichung und Aufrechterhaltung der Datensicherheit. Das Konzept der IT-Grundschutzvorgehensweise besteht in der Zugrundelegung pauschaler Gefährdungen und hält für diese entsprechende technische und organisatorische Schutzmaßnahmen bereit.

Tiergartenstraße 54g
D-47053 Duisburg
☎ : +49 (0)203/ 608499-10
Fax : +49 (0)203 / 608499-11

Leistungen von F&M Consulting

- **Aufbau, Optimierung und Überprüfung der IT-Sicherheit nach anerkannten Standards**
- **Vorbereitung auf eine Zertifizierung nach ISO 27001 oder IT-Grundschutz**
- **Bereitstellung eines externen IT-Sicherheitsbeauftragten**
- **Aktive Gestaltung und Sicherung der gesamten System- und Datenstruktur**
- **Kontinuierliche Überwachung und Aktualisierung der Sicherheits- und Sicherungssysteme**
- **Aktives Management der Hard- und Softwaresysteme (Infrastruktur, Server, Applikationen, mobile Endgeräte)**
- **Migration und Hosting von Inhouse IT und Cloud Lösungen**
- **Prävention: Sicherheitsanalyse und kontinuierliche Systemlösungen**
- **Abwehr: Monitoring und Sicherheitsshutdown**
- **Nachsorge: IT-Forensik, Wiederherstellung von Intranet, Hardware und Softwareapplikationen, Datenträger sowie mobile Endgeräte.**

Dieses Dienstleistungskonzept ist gezielt auf den produzierenden Mittelstand abgestimmt und wurde bereits mehrfach für die angewandte Methodik mit Innovationspreisen ausgezeichnet.

Weitere Leistungsmerkmale sind dem F&M Leistungskatalog „IT-Outsourcing“ zu entnehmen.

Tiergartenstraße 54g
D-47053 Duisburg
☎ : +49 (0)203/ 608499-10
Fax : +49 (0)203 / 608499-11