comdatis
it-consulting

Markus Olbring
Deventer Weg 8
48683 Ahaus

Telefon +49 (0) 2561/7569986
Mobil +49 (0) 173/979 989 7
E-Mail m.olbring@comdatis.de
Internet http://www.comdatis.de

USt.-IdNr. DE295839603

Informationssicherheit für KMU

Mit technischen und organisatorischen Maßnahmen müssen Unternehmen gem. Art. 32 der Datenschutz-Grundverordnung dafür Sorge tragen, dass personenbezogene Daten hinreichend geschützt sind.

Nachfolgende Aufstellung stellt einige Beispiele für mögliche Maßnahmen zur Informationssicherheit dar. Die konkrete Ausgestaltung ist stets abhängig von der Unternehmensgröße und des Risikos der vom Unternehmen verarbeiteten Daten.

1. Sicherstellung der Vertraulichkeit von Daten
    - Zutrittskontrolle
        - Serverraum bzw. Serverschrank ist stets verschlossen und nur berechtigte Mitarbeiter haben Zutritt.
        - Generell verfügen nur berechtigte Mitarbeiter über einen Schlüssel. Eine Schlüsselliste wird im Unternehmen geführt. Mitarbeiter sind verpflichtet, den Verlust eines Schlüssels umgehend zu melden.
        - Alarmanlage
        - Kennwörter sind nicht notiert und auf Bildschirm / Tastatur aufgeklebt. Als Backup kann eine Kennwortliste im Tresor hinterlegt sein.
        - Schränke in der Personal- und Finanzbuchhaltung sind bei Abwesenheit der Mitarbeiter verschlossen. Generell werden sensible / vertrauliche Dokumente sicher aufbewahrt, sie liegen nicht offen auf den Tischen herum.
    - Zugangskontrolle
        - Die PC-Arbeitsplätze sind durch ein sicheres Kennwort (Klein-/Großbuchstaben, Zahlen, Sonderzeichen) geschützt. Kennwörter sollten mindestens für kritische Dienste regelmäßig geändert werden bzw. eine 2-Faktor-Authentifizierung wird verwendet.
        - Sofern möglich, hat jeder Mitarbeiter mit PC-Zugriff einen eigenen Benutzernamen und ein eigenes Kennwort.
        - Für verwendete Onlinedienste (z.B. Onlineshops) ist sichergestellt, dass unterschiedliche und ausreichend sichere Kennwörter verwendet werden. Mitarbeiter sind dahingehend sensibilisiert, dass im privaten und beruflichen Umfeld unterschiedliche Kennwörter verwendet werden.
        - PC-Arbeitsplätze werden bei Verlassen des Arbeitsplatzes gesperrt und zur Entsperrung ist eine Kennworteingabe notwendig.
        - Wird der PC nicht vom Mitarbeiter gesperrt, erfolgt nach spätestens15 Minuten eine automatische Sperre.
        - Mobile Endgeräte (Tablet, Smartphone) sind ebenfalls gesperrt und mit einer Zugangskontrolle gesichert (z.B. PIN, Fingerabdruck).
        - E-Mails usw. werden ausschließlich über verschlüsselte Verbindungen abgerufen.
        - Lokale Administrationsrechte an Windows-Arbeitsplätzen sind eingeschränkt.
        - Die Administration von Software erfolgt ausschließlich durch berechtigte Mitarbeiter.
    - Zugriffskontrolle
        - Mitarbeiter verfügen ausschließlich über die Rechte am PC-Arbeitsplatz, die zur Aufgabenerledigung notwendig sind.
        - Externe (z.B. Systemhäuser, Softwarehersteller) können auf die Systeme nicht über unverschlüsselte Leitungen zugreifen. Entweder besteht ein personifizierter VPN-Zugriff oder für den Fernzugriff muss die Verbindungsherstellung explizit bestätigt werden.

comdatis
it-consulting

Markus Olbring
Deventer Weg 8
48683 Ahaus

Telefon +49 (0) 2561/7569986
Mobil +49 (0) 173/979 989 7
E-Mail m.olbring@comdatis.de
Internet http://www.comdatis.de

USt.-IdNr. DE295839603

2. Sicherstellung der Integrität von Daten
    - Weitergabekontrolle
        - Verschlüsselter Zugriff für Smartphones und Tablets (z.B. zum Mailabruf).
        - Dienste mit der Eingabenotwendigkeit von Benutzernamen und Kennwort werden ausschließlich über verschlüsselte Verbindungen genutzt (https).
        - WLAN im Unternehmen ist mit per WPA2 verschlüsselt und der Code ist mindestens 20 Stellen lang.
        - Gäste und Mitarbeiter erhalten mit nicht betriebseigenen Geräten keinen Zugriff auf das interne WLAN, ggf. kann ein Gäste-WLAN eingerichtet werden.
        - Der Speicher mobiler Endgeräte ist verschlüsselt. Dies gilt für Notebooks mit betrieblichen Daten sowie Smartphones und Tablets mit Android-Betriebssystem. Apple-Geräte sind systemseitig bereits verschlüsselt.
        - Papierbasierte Datenträger werden geschreddert, wenn diese nicht mehr benötigt werden. Hierbei kommt die Stufe P-4 der DIN66399 zum Einsatz.
        - IT-Datenträger werden physisch zerstört oder über einen zertifizierten Dienstleister vernichtet.
        - Daten auf USB-Sticks oder anderer Hardware werden sicher gelöscht, wenn diese Datenträger wiederverwendet werden.
        - Das Kontaktformular auf der Homepage ist zur Sicherstellung der Anforderungen des Telemediengesetzes (TMG) verschlüsselt (https).
        - Mitarbeiter sind schriftlich zur Verschwiegenheit verpflichtet.

3. Sicherstellung der Verfügbarkeit und Belastbarkeit von Daten
    - Verfügbarkeitskontrolle
        - Einsatz aktueller Lösungen zum Virenschutz.
        - Einsatz einer Firewall (Software und/oder Hardware).
        - Regelmäßige Datensicherungen werden durchgeführt. Dabei ist sichergestellt, dass es stets eine Offlinesicherung (z.B. externe, nicht angeschlossene USB-Festplatte).
        - Softwareaktualisierungen werden regelmäßig durchgeführt. Neben den Windows-Updates werden auch die Virenschutzsoftware sowie Hilfsprogramme (PDF-Programm, Java, Flash usw.) aktualisiert.
    - Wiederherstellbarkeit
        - Die Funktionsfähigkeit der Datensicherung einschl. der Wiederherstellbarkeit wird regelmäßig getestet, um sicherzustellen, dass das Backup auch eine Wiederherstellung der Daten im Ernstfall erlaubt.

4. Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung
    - Datenschutz-Management
        - Prüfung im Unternehmen, ob eine gesetzliche Verpflichtung zur Bestellung eines Datenschutzbeauftragten besteht. Sofern eine Ernennungspflicht vorliegt, erfolgt eine Meldung an die zuständige Aufsichtsbehörde.
        - Erfüllung der Informationspflichten, die sich aus dem Datenschutz ergeben
            - Einfach erreichbare Datenschutzerklärung auf der Homepage.
            - Erfüllung der notwendigen Informationspflichten auch bei Offline-Datenerhebung.
        - Etablierung eines Verfahrens zur Geltendmachung von Betroffenenrechten.
        - Erstellung eines Verzeichnisses der Verarbeitungstätigkeiten im gesetzlich vorgeschriebenen Umfang.
        - Dokumenten der Maßnahmen zur Informationssicherheit (techn. und org. Maßnahmen, wie in diesem Dokument exemplarisch dargestellt).

comdatis
it-consulting

Markus Olbring
Deventer Weg 8
48683 Ahaus

Telefon +49 (0) 2561/7569986
Mobil +49 (0) 173/979 989 7
E-Mail m.olbring@comdatis.de
Internet http://www.comdatis.de

USt.-IdNr. DE295839603

  - Schriftliche Regelung des erlaubten Umfangs bzw. Verbots der Privatnutzung.
  - Einholung einer Einwilligung von Mitarbeitern oder anderen Personen, wenn z.B. auf der Homepage oder in Prospekten Bildmaterial der Personen gezeigt wird.
- Auftragskontrolle
  - Sorgfältige Auswahl externer Dienstleister.
  - Verpflichtung der externen Dienstleister auf den Datenschutz.