Technische und Organisatorische Maßnahmen

gemäß §64 BDSG neu

01. Zugangskontrolle

Verwehrung des Zugangs zur Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird für Unbefugte gemäß § 64 BDSG neu:

Zutritt zu den Geschäfts-/IT-Räumen

- die Geschäftsräume der SConsultIT sind außerhalb der Geschäftszeiten verschlossen
- zu den Geschäftszeiten ist der Zutritt nur mittels Schlüssel möglich
- Zutritt zum Serverraum ist nur autorisierten Mitarbeitern möglich
- Zugang zu den Datenverarbeitungsanlagen
  - das Firmennetzwerk ist durch eine Firewall gesichert
  - der Zugriff von extern auf das Intranet ist nur via VPN möglich
  - zu in der DMZ befindlichen Diensten, mit denen personenbezogene Daten verarbeitet werden, sind ausschließlich verschlüsselte Verbindungen möglich
  - alle Arbeitsplatzrechner wie auch Server, auf denen personenbezogene Daten verarbeitet werden, sind verschlüsselt
  - der Zugriff ist nur mit benutzerspezifischer Authentifikation (Benutzername und Kennwort) möglich
  - für den Schutz vor Schadsoftware kommen entsprechende Produkte zum Einsatz

Es existieren interne Richtlinien zum Umgang mit personenbezogenen Daten wie Kundendaten/Kundendatenbanken, wie auch zum Umgang mit den gestellten IT-Systemen. Diese beinhalten z.B. Kennwortrichtlinien, Richtlinien zur Verarbeitung von Kundendatenbanken, Einschränkungen zur Speicherung von Kundendatenbanken.

02. Datenträgerkontrolle

Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern, gemäß § 64 BDSG neu:

- personenbezogene Daten dürfen gemäß internen Richtlinien nur auf verschlüsselten Datenträgern gespeichert werden
- alle intern in Geräten eingesetzten wie auch andere externe Datenträger sind verschlüsselt
- vor der Weitergabe oder Entsorgung von Datenträgern werden diese sicher gelöscht

03. Speicherkontrolle

Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten gemäß § 64 BDSG neu:

- Systeme müssen gemäß internen Richtlinien bei Abwesenheit gesperrt werden
- alle intern in Geräten eingesetzten wie auch andere externe Datenträger sind verschlüsselt
- Benutzer müssen sich auf allen Systemen mit ihren persönlichen Zugangsdaten authentifizieren
- Protokollierung von Zugriffen/Änderungen
- Trennung von Produktiv- und Testsystemen

04. Benutzerkontrolle

Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerprotokolle), gemäß § 64 BDSG neu:

- nur berechtigte Personen haben Zugriff auf Datenverarbeitungsanlagen
- Benutzer müssen sich auf allen Systemen mit ihren persönlichen Zugangsdaten authentifizieren
- Werden personenbezogene Daten übertragen, so geschieht dies ausschließlich über verschlüsselte Übertragungswege
- Protokollierung der Zugriffe/Änderungen
- Produktiv- und Testsysteme sind strikt getrennt

05. Zugriffskontrolle

Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben, gemäß § 64 BDSG neu:

- der Zugriff auf Systeme ist nur mit benutzerspezifischer Authentifikation (Benutzername/Kennwort) möglich
- jeder Mitarbeiter hat unterschiedliche Berechtigungsstufen auf einzelne Systeme (wie z.B. ERP-/CRM-System, Mailserver, Telefonanlage, Fileserver, FTP-Server)
- Zugriffsverletzungen durch fehlerhafte Logins werden – abhängig vom jeweiligen System – protokolliert und direkt an die Administration gemeldet

06. Übertragungskontrolle

Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können, gemäß § 64 BDSG neu;

- jeder Zugriff wie auch die Übermittlung von Daten werden protokolliert
- jeder Zugriff auf den FTP-Server wird unmittelbar per E-Mai an die IT-Abteilung gemeldet, so ist direkt nachvollziehbar, wer wann auf welche Daten zugegriffen hat
- für die Übertragung von vom Kunden bereitgestellte Daten gibt es streng definierte Übermittlungswege und interne Prozesse
- personenbezogene Daten der Kunden werden im ERP-/CRM-System verarbeitet, hier findet keine Übertragung an andere Systeme statt

07. Eingabekontrolle

Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert wurden, gemäß § 64 BDSG neu:

- die Erfassung und Änderung von personenbezogenen Daten wird mit Zeitstempel vom jeweiligen Benutzer protokolliert

08. Transportkontrolle

Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport und Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden, gemäß § 64 BDSG neu:

- für die Übertragung von vom Kunden bereitgestellte gibt es streng definierte Übermittlungswege und interne Prozesse

- personenbezogene Daten der Kunden werden im ERP-/CRM-System verarbeitet, hier findet keine Übertragung an andere Systeme statt
- alle externen/internen Datenträger, auf denen personenbezogene Daten verarbeitet werden, sind verschlüsselt
- Einsatz aktueller Verschlüsselungsverfahren auf den Serversystemen wie SFTP, TLS (vormals SSL), HTTPS, SMTPS, IMAPS, etc.

09. Wiederherstellbarkeit

Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellbarkeit), gemäß § 64 BDSG neu:

- für alle Systeme existieren mehrstufige Backups mit individuell angepassten Backup-Konzepten
- Backups von verschlüsselten externen/internen Datenträgern sind ebenfalls verschlüsselt

10. Zuverlässigkeit

Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden, gemäß § 64 BDSG neu:

- Ausfälle werden in der Praxis sofort bemerkt
- ein Monitoring-System ist geplant

11. Datenintegrität

Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können, gemäß § 64 BDSG neu:

- Festplatten, Datenbanken etc. können auf Integrität geprüft werden
- Kundendatenbanken werden nur in archivierter Form angenommen und zurückübertragen, da die darin enthaltene CRC-Prüfung Integritätsverluste erkennen kann

12. Auftragskontrolle

Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können (Auftragskontrolle), gemäß § 64 BDSG neu:

- in den AV-Verträgen mit Kunden sind Weisungsempfänger und Weisungsbefugter explizit angegeben
- Mitarbeiter sind in Bezug auf den Datenschutz geschult und gemäß internen Richtlinien angehalten, Weisungen zu befolgen

13. Verfügbarkeitskontrolle

Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle), gemäß § 64 BDSG neu:

- Siehe hierzu Punkt 09. Wiederherstellbarkeit
- für alle Systeme existieren mehrstufige Backups mit individuell angepassten Backup-Konzepten

14. Trennbarkeit

Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (Trennbarkeit), gemäß § 64 BDSG neu:

- Intern genutzte Systeme bieten die Möglichkeit, Personen nach Status getrennt zu verarbeiten (ERP-/CRM-System)
- Produktiv- und Testsysteme sind strikt getrennt