Anlage 1: Technische und organisatorische Maßnahmen

1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten.

- Büroräume befinden sich innerhalb einer Passage. Diese ist außerhalb der Geschäftszeiten komplett verschlossen.
- Schlüsselrechtekonzept für Gebäude und Räume
- Verschließbarer Serverschrank, Schlüsselausgabe nur an Berechtigte
- Admin-Passwort separat verschlossen gelagert
- VPN-Verbindung mittels zertifikatsgesicherter OpenVPN-Verbindung
- Verschließbare Aktenschränke, Schlüsselausgabe an Berechtigte
- Verschließbare Personalakten, Schlüsselausgabe an Berechtigte
- Einsatz von Aktenvernichtern bzw. Dienstleistern zur Dokumentenvernichtung
- Nach Verlassen des Arbeitsplatzes Bildschirm und Tastatur/Maus gesperrt
- Domäneninfrastruktur mit zentraler Benutzer- und Gruppenverwaltung (Active Directory)
    - Ordner- und Dateifreigaben
    - Steuerung von Lese- und Schreibzugriffen
    - lediglich Mitarbeiter der IT-Abteilung besitzen Administratorberechtigung
    - Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)
- Einsatz von zwei unabhängigen Virenscannern
- Einsatz von Spamfiltern
- Verschlüsselung des WLAN mit WPA-2 PSK
- Einsatz einer DMZ

2 Integrität

Die Integrität beschreibt, ob Sie sich darauf verlassen können, dass alle Daten am richtigen Ort zum richtigen Kunden zugeordnet sind.

- Web- und E-Mailserver (Im Rechenzentrum)
    - RAID zur automatischen Korrektur von Datenfehlern
    - Verwendung von ECC-RAM
    - regelmäßige Backups auf File- und Backupserver
    - Verwendung von USVs und redundanten Netzteilen
- Fileserver
    - Verwendung von USVs und redundanten Netzteilen
    - RAID
- Windowsserver
    - Virtualisierung der produktiven Windowsserver-Betriebsumgebungen mit Snapshotfunktion
    - Verwendung von ECC-RAM
    - Verwendung von USVs und redundanten Netzteilen
- Führung einer Inventarliste für Clients
- Datenübertragungen von E-Mailsystemen sind mittels TLS gesichert und werden protokolliert
- Einschränkung des Zugriffs auf bestimmte Datensätze im Kundenverwaltungssystem

- Protokollierung von Änderungen und Löschung im Kundenverwaltungssystem
- Vergabe von Lese- und Schreibrechten auf Dateiebene und per Netzwerkfreigabe (Berechtigungskonzept)
- Einsatz von verschlüsselten Verbindungen bei externen Datenübertragungen

3 Verfügbarkeit

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige und mutwillige Zerstörung oder Verlust geschützt sind.

- Serversysteme
    - virtualisiert
    - mit unterbrechungsfreier Stromversorgung (USV) ausgestattet
    - mit Überspannungsschutz ausgestattet
    - mit RAID-System ausgestattet
    - Mehrstufiges Backup-Konzept
    - SMART-Monitoring
- Clients
    - Automatische Datensicherung durch servergespeicherte Benutzerprofile (Roaming Profiles)
    - Erhöhte Datensicherheit durch Nutzung netzwerkbasierter Angebotsprogramme
    - Automatische Windows-Updates
    - Virenscanner kommen in zwei Bereichen zum Einsatz. Direkt auf dem E-Mail-Server und auf Dateiebene der Clients und Domainserver. Es handelt sich um zwei unterschiedliche Antivirenhersteller
    - Einsatz von Firewalls
- Wartungsvertrag Maklerverwaltungsprogramm inkl. Notfall-Support-Hotline

4 Belastbarkeit der Systeme

IT-Systeme müssen im Alltagsbetrieb einwandfrei funktionieren und gegenüber automatisierten Angriffen und Belastungen solide arbeiten.

- Wartungen, bei denen mit Ausfallzeiten zu rechnen ist, werden außerhalb der Geschäftszeiten durchgeführt
- zentrale Verwaltung der Antivirensoftware auf Windows-Clients und -servern (mehrfache Aktualisierung der Signaturdatenbank, zentrales Monitoring/Reporting)
- Regelmäßige Prüfung und Installation von
    - Firewall-Soft-/Firmware-Updates
    - Server Betriebssystem-Updates
    - Client-Updates
- Firewall (IDS, DoS, IP-Filter; Standardregel: Paket verwerfen)
- Backup läuft außerhalb der Geschäftszeiten

5 Wiederherstellung

Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können

- IT-Dienstleister auf Abruf
- Wartungsvertrag mit Notfall-Hotline Maklerverwaltungsprogramm
- Notfallplan Wiederherstellung Maklerverwaltungsprogramm
- Tägliches Backup aller Daten
- Vorhalten von Ersatzteilen
- Business-Notfallhotline der Telekom bei Störungen oder Ausfällen der Telefonanlage

6 Datenvernichtung

Umsetzung des Rechts auf „Vergessenwerden“

- Implementierung von Fernlöschung, insbesondere auf mobilen Endgeräten
- Zerstörung von Datenträgern vor der Entsorgung
- Schreddern / mechanische Deformierung von Datensätzen auf Papier / DVD / CD oder sonstigen Datenträgern
- Sorgfältige Auswahl von Entsorgungsdienstleistern

7 Überprüfung / Evaluierung der Wirksamkeit

Durch folgende Maßnahmen wird eine Bewertung und Evaluierung der Wirksamkeit der o.g. Maßnahmen sichergestellt

- Automatische Information bei Backup-Komplikationen
- Reporting Virenscanner
- Jour-Fix für Mitarbeiter: Regelmäßige Diskussionen zu Maßnahmen und deren Wirksamkeit
- Mitarbeiter sind angehalten, bei Verdachtsmomenten Ihren Vorgesetzten oder den Datenschutzbeauftragten zu informieren
- eindeutige Vertragsgestaltung gemäß individueller Leistungsvereinbarung
- formalisierte Auftragserteilung durch schriftliche und unterzeichnete Auftragsverarbeitungsvereinbarung
- Möglichkeit der Durchführung von Kontrollen durch den Auftraggeber zur Vertragsausführung
- Führung eines Verzeichnisses aller Auftragnehmer
- Verpflichtungen der Mitarbeiter/innen des Auftragnehmers auf das Datengeheimnis bzw. zur Vertraulichkeit
- Durchführung von regelmäßigen Unterweisungen zum Datenschutz
- schriftliche Bestellung eines externen Datenschutzbeauftragten