1. Technische und organisatorische Maßnahmen

1. Die im Anhang beschriebenen technischen und organisatorischen Maßnahmen werden als verbindlich festgelegt.
2. An der Erstellung der Verfahrensverzeichnisse hat der Auftragnehmer mitzuwirken. Er hat die erforderlichen Angaben dem Auftraggeber zuzuleiten.
3. Der Auftragnehmer beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung. Er gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen.
4. Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Wesentliche Änderungen sind schriftlich zu vereinbaren.
5. Soweit die beim Auftragnehmer getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich. Entsprechendes gilt für Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie bei Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten.

2. Allgemeine technische und organisatorische Maßnahmen der Hornetsecurity GmbH

2.1. Zutrittskontrolle

Ein unbefugter Zutritt zum Rechenzentrum (physisch) wird verhindert. Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten sind:

- Kontrolle der Identität per amtlichem Ausweis; wird durchgeführt durch das Personal des jeweiligen Rechenzentrums im Kontrollraum vor dem Zutritt in das RZ.
- Überwachung der RZ-Räume erfolgt per Videosystem (Tageslicht- und Infrarotkameras).
- Zugang zum RZ erfolgt über zwei Zugangskontrollen:
- Tür-Gegensprechanlage zum Kontrollraum mit el. Türöffner
- Tür-Schließsystem mit Magnetkarte.
- Zusätzlich sind die Racktower von Hornetsecurity mit eigenem Schließsystem versehen.
- Der Zugang wird mit Vermerk von Zugangszeitpunkt, Name und Firma, sowie mit Zugangsende protokolliert.

2.2. Zugangskontrolle

Das Eindringen Unbefugter in die DV-Systeme wird durch Hornetsecurity verhindert.

- Kennwortpolicy: mind. 8 Zeichen, mind. 3 von 4 Kriterien (Großbuchstabe, Kleinbuchstabe, Ziffer, Sonderzeichen), Wechselintervall alle 6 Monate
- Pro Mitarbeiter ein Benutzerstammsatz
- Benutzerrechte eingeschränkt auf Tätigkeitsbereiche
- Alle Systeme werden durch geeignete Firewallsysteme vor unerlaubten Zugriffen geschützt, Zugänge bei Systemen sind auf eng definierte IP-Adressbereiche beschränkt
- Festplatten in Computersystemen sind grundsätzlich verschlüsselt.

2.3. Zugriffskontrolle

Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen werden verhindert. Es gibt eine bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie für deren Überwachung und Protokollierung:

- Zugangsberechtigungen nur für Bereiche, die für spezifische Tätigkeiten benötigt werden (rollenbasierte Berechtigung)
- Kontrollen bzgl. unberechtigter Zugangsversuche (IDS/IPS)
- Transaktionsprotokollierung jeglicher Systemänderungen
- 4-Augenprinzippflicht für Softwareänderungen.

2.4. Weitergabekontrolle

Regelung der Weitergabe personenbezogener Daten (Elektronische Übertragung, Datentransport, Übermittlungskontrolle). Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der Nachträglichen Überprüfung:

- Externe Zugriffe auf Daten erfolgt ausschließlich über VPN
- Offlinearbeitsdateien (Notebooks, etc.) liegen ausschließlich auf verschlüsselten Datenträgern vor.

2.5. Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege wird gewährleistet. Jegliche Datenveränderung wird transaktionsorientiert protokolliert. Ein Verändern des Protokolls ist nicht möglich. Dadurch kann jederzeit auch nachträglich festgestellt werden, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind.

2.6. Auftragskontrolle

Die Verarbeitung von Kundendaten wird von Hornetsecurity selber durchgeführt und nicht an Dritte vergeben. An Dritte vergeben werden lediglich Basisleistungen (RZ-Dienste, Internetanbindung, Transport und Einbau von Systemen und Datenträgern).

2.7. Verfügbarkeitskontrolle

Die Daten werden gegen zufällige Zerstörung oder Verlust geschützt. Maßnahmen zur Datensicherung (physikalisch / logisch):

- Hornetsecurity setzt bei der Datenverarbeitung mindestens zwei unabhängige und räumlich weit getrennte Rechenzentren ein. Jedes dieser Rechenzentren verfügt für sich allein über:
- redundante Stromversorgung
- redundante Netzwerkversorgung
- redundante Klimatisierung
- redundante Löschanlagen
- Die Datenverarbeitung wird vollständig bereits mit dem Betrieb eines einzelnen RZ gewährleistet. Das zweite und weitere RZ werden zur Erhöhung der Redundanz eingesetzt.
- Daten werden grundsätzlich auf gespiegelten Datenträgern durch geeignete RAID-Verfahren gespeichert.
- Zentrale Datensysteme sind zusätzlich gedoppelt mit automatischer Replikation sowie Hot-Fail-Over-Funktionalitäten ausgestattet.
- Daten werden zusätzlich regelmäßig auf ein Bandsystem gesichert um ältere Datenstände wiederherstellen zu können.

2.8. Trennungskontrolle

Alle Daten werden nach Mandanten getrennt in dedizierten Datenbanken gespeichert. Für interne Zwecke (z.B. Entwicklung, Test und Backup) werden getrennte Systeme mit eigener Datenstruktur genutzt.