Anlage 1 - Unterauftragsverhältnisse

Aktuell bestehen die nachfolgenden Unterauftragsverhältnisse im Zusammenhang mit der Auftragsverarbeitung:

Ablesung

Ggf. ein externes Unternehmen für die Wintermonate, derzeit ist keines beauftragt

IT-Dienstleister

Ceos Solutions GmbH

Heizkörpererkennungs- und Bewertungssystem

Thermosoft2000

Datenvernichtung

Bellersheim Abfallwirtschaft

HeiKoTec
Gehrer GmbH

Anlage 2
Technische organisatorische Maßnahmen / Datenschutzkonzept

Der Auftragsverarbeiter sichert zu, dass er die nachfolgend beschriebenen Mindestanforderungen im Rahmen seines Datenschutzkonzeptes einhält. Es beschreibt die im Rahmen der Auftragsverarbeitung erforderlichen Maßnahmen beim Auftragsverarbeiter zum sicheren Umgang mit personenbezogenen Daten. Die Grundlage für dieses Datenschutz-Konzept bilden die EU-Datenschutzgrundverordnung DS-GVO und ggf. weitere von den interessierten Parteien geforderten Maßnahmen. Hierbei orientiert sich der Auftragsverarbeiter im Wesentlichen an den Vorgaben der Artikel 24, 25 und 32 DS-GVO.
Auf Anforderung weist der Auftragsverarbeiter die Einhaltung entsprechend nach.

1. Vertraulichkeit (Art. 32 Abs. 1 lit b DS-GVO)

Maßnahme	*Umsetzung der Maßnahme*
• Zutrittskontrolle Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z. B. Magnet- oder Chipkarten, Schlüssel, elektronische Türöffner, Werkschutz bzw. Pförtner, Alarmanlage, Videoanlage	- Kein Zugang für Unbefugte zu den Datenverarbeitungsanlagen - Während der Geschäftszeiten ist der Zutritt zu den Geschäftsräumen durch die Mitarbeiter kontrolliert - Regelung für Betriebsfremde - Alarmanlage mit Meldestelle zur Polizei
• Zugangskontrolle Keine unbefugte Systembenutzung, z. B. (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern	- Zugang zu Systemen nur mit individuellen Benutzernamen und Kennwörtern - Definierter Kreis von Zugangsberechtigten
• Zugriffskontrolle Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z. B. Berechtigungs-Konzepte und bedarfsgerechte Zugriffsrechte. Protokollierung von Zugriffen	- Berechtigte können nur auf für sie berechtigte Daten zugreifen - Personenbezogene gespeicherte Daten können nur im Rahmen des Berechtigungskonzeptes gelesen, kopiert, verändert oder entfernt werden - Gestaffeltes Berechtigungskonzept anhängig von der Funktion der jeweiligen Person zur Erfüllung des Auftrags - Verwendung fortlaufend aktualisierter Virenschutzsoftware - Schutz des E-Mail-Verkehrs vor Viren - Firewall-System - Passwortschutz

• Trennungskontrolle Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z. B. Mandantenfähigkeit, Sandboxing	- Trennung der Daten durch getrennte Datenbanken, welche durch unterschiedliche Mandanten getrennt werden - Berechtigte können nur auf für sie berechtigte Daten zugreifen
• Pseudonymisierung Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen	- Mieter- und/oder Eigentümername alleine reicht nicht aus, um relevante Daten zu erkennen - Mieterbezogene Daten können nur mit Mehrfachabfrage extrahiert werden (Name, Straße und/oder Ort, Abrechnungsjahr)

2. Integrität (Art. 32 Abs. 1 lit b DS-GVO)

Maßnahme	*Umsetzung der Maßnahme*
• Weitergabekontrolle Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z. B. Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur	- Verschlüsselung - Nutzung von VPN-Tunnel bei Übertragung - Regelung des Systemkommunikationsverkehrs
• Eingabekontrolle Feststellung, ob und von wem personenbezogene in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z. B. Protokollierung, Dokumentenmanagement	- Berechtigungskonzept - Personenbezogene Daten können nur im Rahmen des Berechtigungskonzeptes eingeben, verändert oder entfernt werden - Schriftwechsel erfolgt über Dokumentenmanagement

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit b DS-GVO)

Maßnahme	*Umsetzung der Maßnahme*
• Verfügbarkeitskontrolle Schutz gegen zufällige oder mutwillige Zerstörung bwz. Verlust, z. B. Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne	- Personenbezogene Daten sind während der Geschäftszeiten verfügbar - Daten werden täglich durch mehrfache Datensicherung gegen zufällige oder mutwillige Zerstörung oder Verlust geschützt - tägliche Sicherheitskopien auch außerhalb des Gebäudes auf externer Festplatte beim GF - Überwachungs- und Meldesystem für die Datensicherung
• Rasche Wiederherstellbarkeit	- Daten können aufgrund der täglichen Datensicherung innerhalb eines Tages komplett wieder hergestellt werden

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Maßnahme	*Umsetzung der Maßnahme*
• Auftragskontrolle Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z. B. eindeutige Vertragsgestaltung, formalisiertes Auftrags-management, strenge Auswahl des Dienstleisters, Vorab-überzeugungspflicht, Nachkontrollen	- Verarbeitung nur entsprechend der dokumentierten Weisung des Auftragsgebers - Weisungen erfolgen zwischen dafür ausdrücklich abgestimmten Kontaktpersonen - eingesetzte Personen sind über datenschutzrechtliche Anfor-derungen informiert und schriftlich auf das Datengeheimnis nach § 5 BDSG verpflichtet
• Datenschutzmanagement • Incident-Response-Management • Datenschutzfreundliche Voreinstellung (Art. 25 Abs. 2 DS-GVO)	