Anlage zur Auftragsverarbeitungsvereinbarung

Technisch-organisatorische Maßnahmen zur Umsetzung von Art. 32 Abs. 1 DS-GVO der RHC GmbH

RHC GmbH
Neue Wiese 12
98597 Fambach

Telefon: 036848 / 40930
Fax: 036848 / 409379
www.rhc-edv.de
datenschutz@rhc-edv.de

Zur Sicherung der Datensicherheit, die bei der Datenverarbeitung gewährleistet werden muss, werden folgende technische und organisatorische Maßnahmen entsprechend § 9 BDSG und Anlage verbindlich festgelegt:

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

▪ Zutrittskontrolle:

Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.
Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten durch:
Zutrittskontrollsystem, Ausweisleser, Magnetkarte, Chipkarte

- Sicherung der Büroräume durch Schließsystem
- Überwachungseinrichtung Alarmanlage, Video-/Fernsehmonitor

▪ Zugangskontrolle:

Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern.
Technische (Kennwort-/Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

- Zugang ist kennwortgeschützt (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)
- Automatische Sperrung (z.B. Kennwort oder Pausenschaltung)
- regelmäßig kein Publikumsverkehr in Büroräumen

▪ Zugriffskontrolle:

Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen
sind zu verhindern.
Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts für die autorisierten Mitarbeiter und deren Zugriffsrechte sowie deren Überwachung und Protokollierung:
Berechtigungen (Profile, Rollen, Transaktionen und Objekte)
Auswertungen

- Zugriffe werden bei Bedarf vom Auftraggeber freigegeben und vom Auftragnehmer protokolliert
- Kenntnisnahme, Veränderung, Löschung

▪ Verarbeitungskontrolle:

- Daten sind während der Verarbeitung durch Verschlüsselung geschützt

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

▪ Weitergabekontrolle:

Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

- Verschlüsselung/Tunnelverbindung (VPN = Virtual Private Network),
- Protokollierung (ist manuell vorzunehmen),
- Transportsicherung: FTP-Übertragung, ZIP-Archiv mit Passwortschutz, Übermittlung des
- Passwortes über Telefon.

▪ Eingabekontrolle:

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.
Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:
Protokollierungs- und Protokollauswertungssystem – Systeminternes Protokollierungsverfahren für Datenbewegungen und Datenzugriffe.

▪ Auftragskontrolle:

Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten.
Der Auftragnehmer weist seine Mitarbeiter in den Umfang und Inhalt der vom Auftraggeber erteilten Weisungen ein. Der Auftraggeber ist berechtigt, dies durch unangekündigte Kontrollen vor Ort zu kontrollieren.

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

▪ Verfügbarkeitskontrolle:

Verfügbarkeit und Stabilität der Systeme ist durch technische und organisatorische Maßnahmen sichergestellt:

- Backup-Konzept
- Firewall und Virenschutz
- Spiegeln von Festplatten, z.B. RAID-Verfahren
- Unterbrechungsfreie Stromversorgung (USV)
- Überspannungsschutz (FI)
- rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO) ist gewährleistet

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

- Datenschutzrichtlinie
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)