Technische und organisatorische Sicherheitsmaßnahmen gemäß Art. 32 DS-GVO

Zum Schutz der in Bezug auf die Verarbeitung personenbezogener Daten bestehenden Rechte und Freiheiten natürlicher Personen ist es erforderlich, dass geeignete technische und organisatorische Maßnahmen getroffen werden und die Anforderungen dieser Verordnung damit erfüllt werden. Um die Einhaltung der Verordnung nachweisen zu können, legt der Auftragnehmer interne Strategien fest und ergreift Maßnahmen, die insbesondere den Grundsätzen des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge tun.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Dabei sind der Stand der Technik, die Implementierungskosten, die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 DS-GVO zu berücksichtigen. Wesentliche Änderungen sind zu dokumentieren. Insgesamt handelt es sich um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme, die je nach Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind, herzustellen. Zur Erfüllung der gesetzlichen Anforderungen setzt der Auftraggeber in seinem Einflussbereich auf diese Vereinbarung wie folgt um:

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

1.1. Zutrittskontrolle

Keinen unbefugten physischen Zutritt zu Datenverarbeitungsanlagen, wie Serverräume, Netzwerkverkabelungen oder Arbeitsräume, in denen Arbeitsplatzrechner stehen, zu verschaffen. Der Auftragnehmer trägt dafür Sorge, dass weder das Betreten, der Einblick oder der mögliche Zugriff erlangt werden kann.

Der Auftragnehmer hat folgende Maßnahmen getroffen:

- Schlüsselverwaltung mit Dokumentation der Schlüsselvergabe
- Einbruchmeldeanlage nach VDS Standard
- Besucher- und Personenkontrolle
- Videoüberwachung des Betriebsgeländes
- Türsicherung des Serverraums mit elektronischer Zutrittskontrolle
- Fensterloser Serverraum

1.2. Zugangskontrolle

Es ist zusätzlich zur Zutrittskontrolle zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden. Der Zugang zu Anlagen mit denen personenbezogene Daten verarbeitet werden, ist mittels Benutzer-Identifikation zu versehen.

Der Auftragnehmer hat folgende Maßnahmen getroffen:

- Persönlicher Userlogin mit Berechtigungskonzept bei Anmeldung am Unternehmensnetzwerk
- Kennwortverfahren und Kontrolle des Verfahrens
- Regelmäßige Änderung der Userpasswörter
- Geeignete Antivirenschutzlösung mit aktuellen Updates auf Server und Clients
- Redundantes Firewall System auf Hardwarebasis
- Automatische Sperrung des Clients nach Zeitablauf ohne Useraktivität
- Digitales System für sämtliche Passwörter und Verschlüsselungen
- Verschlüsselte Übertragungswege sind mittels VPN abgesichert
- Festplatten von mobilen Geräten wie Notebooks und Tablets sind verschlüsselt
- Sämtliche Arbeitsplatzsysteme, fest oder mobil, sind mit einem Bios Passwort versehen
- Vereinbarungen zur sicheren Nutzung mobiler Endgeräte sowie Home-Office

1.3. Zugriffskontrolle

Berechtigte erhalten ausschließlich, auf Basis ihrer Zugriffsberechtigung unterliegenden Daten, Zugriff, so dass kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen von personenbezogenen Daten möglich ist.

Der Auftragnehmer hat folgende Maßnahmen getroffen:

- Persönlicher Userlogin mit Berechtigungskonzept und dedizierten Userrechten
- Passwortidentifikation und Passwortrichtlinie
- Zugriffsbeschränkung auf IP-Ebene und Fernzugriff mittels verschlüsselten VPN
- Protokollierungen auf Anwendungsebene
- Verbot der privaten Nutzung der Clients sowie eigener mobiler Endgeräte
- Verwendete Datenträger werden vor Neuverwendung gelöscht
- Geräte mit SIM Karten Funktion werden mit PIN gesichert
- Festplatten von mobilen Geräten wie Notebooks und Tablets sind verschlüsselt
- Alt Akten und Altdatenträger werden mit zertifizierten Schreddern oder Lochern vernichtet
- An allen Arbeitsplatzsystemen sind die USB Anschlüsse gesperrt

1.4. Trennungsgebot

Die zu unterschiedlichen Zwecken erhobenen Daten sind getrennt zu verarbeiten. Die Trennung ist so durchzuführen, dass eine Vermischung mit Daten anderer Auftraggeber sowie auch der Zugriff unbefugter Dritter nicht möglich ist.

Der Auftragnehmer hat folgende Maßnahmen getroffen:

- Getrennte Datenbanken und Verarbeitungssysteme
- Getrennte Produktiv- und Testsysteme
- Zugriffsberechtigungskonzept
- Mandantentrennung in eingesetzten Softwareprodukten

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

2.1. Weitergabekontrolle

Es ist zu gewährleisten, dass kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder während des Transports und Speicherung auf externe Datenträger möglich ist. Eine Überprüfung und Feststellung muss durchgeführt werden können, an welchen Stellen eine Übermittlung personenbezogener Daten durch die Einrichtung zur Datenübertragung vorgesehen ist.

Der Auftragnehmer hat folgende Maßnahmen getroffen:

- Verschlüsselte Email Übertragung personenbezogener Daten bei Emails
- Gesichertes Wireless LAN (WLAN)
- Verschlüsselte Übertragungswege sind mittels VPN abgesichert
- Verschlüsselung von Datenträgern bei Transport
- Geeignete Antivirenschutzlösung mit aktuellen Updates auf Server und Clients
- Redundantes Firewall System auf Hardwarebasis
- Verpflichtung aller Beschäftigten zur Einhaltung datenschutzrechtlicher Anforderungen nach Art. 5 DS-GVO

2.2. Eingabekontrolle

Ermöglichung einer nachträglichen Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, mit Protokollierungssystem.

Der Auftragnehmer hat folgende Maßnahmen getroffen:

- Dokumentenmanagement mit Revisionierung und Historie
- Protokollierungseinrichtungen bei Eingabe, Änderung und Löschung
- Zugriffsrechte werden limitiert vergeben
- Eingeschränkter Personenkreis zur Änderung der firmenweiten bbCore Software

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

3.1. Verfügbarkeitskontrolle

Ein geeigneter Schutz gegen zufälligen, mutwilligen oder unvorhersehbaren Verlust von personenbezogenen Daten ist einzurichten.

Der Auftragnehmer hat folgende Maßnahmen hierzu getroffen:

- Datensicherungskonzept mit regelmäßiger Überprüfung
- Notfallhandbuch mit Notfallplänen vorhanden
- Datensicherung in getrennten Feuerabschnitt
- Verschlüsselte Backupdatenträger
- Datenträgeraufbewahrung mit Sicherheitskopien außerhalb des Betriebes
- Unterbrechungsfreie Stromversorgung (USV)
- Einbruchmeldeanlage nach VDS Standard
- Geeignete Feuerlöschsysteme in Serverraum und Betriebsgelände
- Regelmäßiger E-Check nach DGUV3 aller elektronischen Anlagen
- Getrennte elektronische Sicherungen der Stromkreisläufe

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

4.1. Auftragskontrolle

Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Sobald beim Auftragnehmer Unterauftragnehmer eingesetzt werden, sind diese in gleicher Art zur Erfüllung der Weisungen und auf die Einhaltung des Datenschutzes zu verpflichten.

Der Auftragnehmer hat folgende Maßnahmen hierzu getroffen:

- Schriftlicher Vertrag zur Auftragsdatenverarbeitung mit dem Auftragnehmer
- Überprüfung und Auswahl des Auftragnehmers insbesondere auf Datensicherheit
- Verpflichtung aller Beschäftigten zur Einhaltung datenschutzrechtlicher Anforderungen nach Art. 5 DS-GVO
- Prüfung des Auftragnehmers ob ein Datenschutzbeauftragter bestellt ist
- Fortlaufende Prüfung und Kontrollrechte in Hinsicht auf den Auftragnehmer