Anlage 2 zum ADV

Technische und organisatorische Maßnahmen der 1blu AG

1. Pseudonymisierung, Datenminimierung

(Art. 32 Abs. 1 lit. a DSGVO, Art. 25 Abs. 1 DSGVO)

Maßnahmen zur Verarbeitung personenbezogener Daten in einer Weise, dass diese ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und den entsprechenden technischen und organisatischen Maßnahmen unterliegen:

- IP-Adressen werden in Logdateien nur vollständig erfasst, sofern dies zum ordnungsgemäßen Betrieb der Server erforderlich ist (d.h. zur Abwehr von Angriffen, zur Feststellung missbräuchlicher Verwendung von Diensten oder der Herausgabe bei Anfragen durch Strafverfolgungsbehörden, usw.).
- Logdateien, welche unverfremdete IP-Adressen enthalten, werden auf unseren Systemen automatisch rotiert.
- Über längere Zeit gespeicherte IP-Adressen (z.B. als Grundlage zur Erstellung von Statistiken für unsere Kunden) sind durch Unkenntlichmachung eines Oktetts (IPv4) bzw. eines Hextetts (IPv6) nicht mehr eindeutig einer bestimmten Person zuzuordnen.
- Es werden nur solche persönlichen Daten unserer Kunden erhoben, die für die Erbringung unserer Dienstleistung notwendig sind. Mitarbeiter sind zur Datensparsamkeit gehalten.

2. Vertraulichkeit

(Art. 32. Abs. 1 lit. b DSGVO)

2.1 Maßnahmen, die Unbefugten den physischen Zugriff auf Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehren (Zutrittskontrolle):

- Das Rechenzentrum verfügt über einbruchshemmende Türen und Lüftungsklappen.
- Es besteht eine Schlüsselregelung samt dokumentierter Schlüsselvergabe.

- Das Rechenzentrum ist durch ein personalisiertes biometrisches Zutrittskontrollsystem abgesichert.
- Eine Richtlinie regelt den Zutritt und die Überwachung von Besuchern. Der Zutritt zu den Serverräumen ist gesondert geregelt.
- Besucher im Rechenzentrum werden protokolliert.
- Videoüberwachung ist im Rechenzentrum installiert.
- Es besteht eine Alarmanlage, deren Auslösung eine automatische Benachrichtigung des Bereitschaftsdienstes nach sich zieht.
- Das Rechenzentrum weist keine Fenster auf.

2.2 Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle):

- Alle DV-Systeme, die Zugang zu personenbezogenen Daten gewähren, erfordern mindestens eine Authentifikation mittels Benutzername und Kennwort.
- Benutzerzugänge sind personalisiert.
- Die Vergabe von Zugangsberechtigungen erfolgt rollenbasiert und wird dokumentiert.
- Es erfolgt ein Entzug von Berechtigungen, sofern diese nicht mehr benötigt werden. Dieser Vorgang wird dokumentiert.
- Die Authentifikation der Benutzer erfolgt durch Verwendung digitaler Zertifikate.
- Administrative Zugänge dürfen sich nur von bestimmten, festgelegten IPs aus anmelden.
- Bei wiederholten Authentifizierungsfehlern erfolgt eine automatische Sperrung von Zugängen.
- Es existiert eine Richtlinie zur datenschutzkonformen Konfiguration der Arbeitsplatzrechner.
- Vorgeschrieben ist für alle Arbeitsplatzrechner das Einrichten einer automatischen Bildschirmsperre mit Kennwortschutz bei Untätigkeit.
- Es erfolgt eine zentrale Speicherung von Protokolldateien auf einem dezidierten Logserver.

2.3 Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, sowie dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen,

kopiert, verändert oder entfernt werden können (Zugriffskontrolle):

- Es gelten rollenbasierte Zugriffsregelungen.
- Administrative Tätigkeiten werden protokolliert.
- Privilegierte Aktionen werden zusätzlich auf einem dedizierten Logserver protokolliert.
- Protokollierung von Kenntnisnahme, Veränderung und Löschung von personenbezogenen Daten auf den Kundenservern.

2.4 Maßnahmen, die sicherstellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden (Trennungskontrolle):

- Auftragsdaten werden getrennt (auf anderen Maschinen) von den Daten aus laufenden Systemanwendungen der Kunden gespeichert.
- Personenbezogene Daten werden ausschließlich zweckgebunden verarbeitet.

3. Integrität

(Art. 32. Abs. 1 lit. b DSGVO)

3.1 Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektrischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Weitergabekontrolle):

- Entfernter Zugriff ist nur unter Verwendung verschlüsselter Verbindungen möglich (z.B. VPN / SSH).
- Wo dies möglich ist, wird Datenverschlüsselung eingesetzt (z.B. PGP für Email).
- Personenbezogene Daten werden standardmäßig nicht an Dritte übermittelt.
- Es besteht ein dokumentierter Prozess zur Vernichtung von Daten und Datenträgern.
- Die physische Vernichtung der Datenträger erfolgt durch einen zertifizierten Dienstleister.

- Transport der Datenträger zur Vernichtung erfolgt in eigens dafür vorgesehenen abschließbaren Behältern.

3.2 Maßnahmen, die eine nachträgliche Überprüfung ermöglichen, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle):

- Eine Protokollierung aller Vorgänge im Bereich der eingesetzten Verwaltungssoftware wird durchgeführt.
- Für essentielle Systeme kommen Versionsverwaltungssysteme zum Einsatz.

4. Verfügbarkeit und Belastbarkeit

(Art. 32 Abs. 1 lit. b und c DSGVO)

Maßnahmen, welche gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und verfügbar bleiben (Verfügbarkeitskontrolle):

- Um die Daten nach einem Ausfall wiederherstellen zu können, existiert ein vollständiges Backup- & Recovery-Konzept.
- Es wird eine tägliche Datensicherung automatisch durchgeführt.
- Um größtmögliche Verfügbarkeit der Daten zu erzielen, werden in den Servern RAID-Systeme eingesetzt.
- Auf Wunsch werden Hochverfügbarkeitslösungen umgesetzt.
- Im Rechenzentrum wird Gebrauch von unterbrechungsfreier Stromversorgung gemacht.
- Das Rechenzentrum verfügt über einen automatisch anlaufenden Dieselgenerator, um Stromausfälle überbrücken zu können, welche über die Batteriekapazität der eingesetzten USV-Anlagen gehen.
- Der Dieselgenerator wird regelmäßig mittels durchgeführter Testläufe auf Betriebsbereitschaft hin überprüft.
- Es besteht eine mehrfach-redundante Anbindung an Backboneprovider.

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

(Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Maßnahmen zur Sicherstellung eines technisch und organisatorisch angemessenen Standes bei der Erbringung der vertraglich vereinbarten Leistungen:

- Die TOM werden nach einem definierten Prozess regelmäßig auf Wirksamkeit und Einhaltung eines angemessenen technischen Standes überprüft.
- Der sichere Betrieb des Rechenzentrums und die sachgemäße Dokumentation der diesbezüglichen Prozesse werden mittels eines durch einen anerkannten externen Dienstleister ausgestellten Zertifikates nachgewiesen.

6. Datenschutzbeauftragter und Auftragsdatenverarbeitung (Art. 32. Abs. 4 DSGVO; Art. 29 DSGVO; Art. 37 Abs. 4 DSGVO)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle):

- Die 1blu AG hat einen Datenschutzbeauftragten bestellt und sorgt durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten Prozesse.
- Verpflichtung der Beschäftigten auf das Datengeheimnis (vormals § 5 BDSG).
- Abschluss von Verträgen zur Verarbeitung von personenbezogenen Daten im Auftrag unter Berücksichtigung der jeweiligen Anforderungen, wenn diese vom Auftraggeber mitgeteilt werden.
- Serverstandorte sind – sofern nicht anderweitig vereinbart – Rechenzentren in Deutschland.