Anlage 2 zur Vereinbarung zur Auftragsverarbeitung

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Vertraulichkeit Bezüglich Umgang mit personenbezogenen Daten	**Maßnahmen**
1. Zutrittskontrolle (Räume und Gebäude) Unbefugten den Zutritt zu Datenverarbeitungsanlagen verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden bzw. in denen personenbezogene Daten gelagert werden.	**Standort Berlin, Kastanienallee 32:** Die Räumlichkeiten der Campusspeicher GmbH in der Kastanienallee 32 in 10435 Berlin befinden sich in einem geschäftlich genutzten Hinterhaus im 3. OG. Sämtliche Zugänge sind ausreichend gegen den unbefugten Zutritt abgesichert, das bedeutet: ▪ Zugänge zu den Büroräumen grundsätzlich verschlossen ▪ Zentrales Schließsystem mit Sicherheitsschlössern ▪ Öffnen der Zugangstüren nur mit Schlüssel ▪ Besucherregelung: Abholung von Besuchern (nach Klingeln) am Eingang zum Bürotrakt. ▪ Dokumentierte Verfahrensweise für Ausgabe und Rückgabe von Zugangsmitteln ▪ Dokumentierte Verfahrensweise für die Meldung des Verlusts eines Zugangsmittels ▪ Spezielle Räume abschließbar. Regelung über Arbeitsanweisung **Rechenzentren Nürnberg, Karlsruhe, Frankfurt und Straßburg:** ▪ Sicherheitsbereich mit Eingangskontrolle ▪ Eingezäuntes Gelände inkl. Videoüberwachung ▪ Regelmäßige Kontrollgänge durch Sicherheitspersonal ▪ Zutrittskontrollsystem mit Chipkarten ▪ Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
2. Zugangskontrolle (IT-Systeme, Anwendungen) Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	**Allgemein:** ▪ Zugang zu DV-Geräten mit persönlicher Benutzer-ID und Kennwort ▪ Dokumentierte Vergabe-Richtlinie für Benutzer-IDs und Kennworte ▪ Zusätzliche Logins für spezielle Applikationen ▪ Kennwortrichtlinie ▪ Protokollierung der Logins und Kennwortfehleingaben ▪ Verschlüsselte Festplatten der Arbeitsrechner ▪ Verbindung von außerhalb der Büroräume nur über VPN

	Bei „Root Server“, „Virtual Server” und “Cloud Server” Verträgen: ▪ Server-Passwörter, die nur vom Auftraggeber nach erstmaliger Inbetriebnahme von ihm selbst geändert werden und dem Auftragnehmer nicht bekannt sind ▪ Passwörter zur Administrationsoberfläche werden vom Auftraggeber selbst vergeben und müssen vordefinierten Richtlinien entsprechen **Bei „Managed Server“, „Managed Hosting“ und „Webhosting” Verträgen:** ▪ Zugang ist passwortgeschützt. Zugriff nur für berechtigte Mitarbeiter vom Auftragnehmer, verwendete Passwörter müssen Mindestlänge haben
3. Zugriffskontrolle (auf Daten) Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.	Bei **internen Verwaltungssystemen** des Auftragnehmers: ▪ Benutzerrollen-/Gruppenkonzept ▪ Passwortrichtlinie inkl. Passwortlänge und Passwortwechsel ▪ Regelmäßige Überprüfung/Aktualisierung der Berechtigungen ▪ Regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) ▪ Zeitgesteuerte Bildschirmsperre mit Wiederanmeldung ▪ Einsatz von Verschlüsselung und Firewalls ▪ Papier-Shredder für Dokumentenvernichtung **Bei „Root Server“, „Virtual Server” und “Cloud Server” Verträgen:** ▪ Die Verantwortung der Zugriffskontrolle obliegt dem Auftraggeber **Bei „Managed Server“, „Managed Hosting“ und „Webhosting” Verträgen:** ▪ Regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) ▪ Regelmäßige Überprüfung/Aktualisierung der Berechtigungen ▪ Benutzerrollen-/Gruppenkonzept
4. Datentrennungskontrolle (zweckbezogen) Gewährleistung, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	▪ Getrennte Verarbeitung zweckgebundener Daten ▪ Trennung von Entwicklungs- und Produktivumgebungen ▪ Ausgesonderte Datenträger werden datenschutzkonform gelöscht oder physikalisch gelöscht ▪ Für die Pseudonymisierung ist der Auftraggeber verantwortlich

Integrität Bezüglich Umgang mit personenbezogenen Daten	**Maßnahmen**
5. Weitergabekontrolle (von Daten) Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.	Die Aspekte der Weitergabe personenbezogener Daten wird durch folgende Maßnahmen umgesetzt: ▪ VPN-Technologie (SSL/TLS) zur Datenkommunikation ▪ Verschlüsselte Übertragung ▪ Identifizierung / Authentifizierung ▪ Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung
6. Eingabekontrolle (in Datenverarbeitungssystemen) Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind.	Die Kontrolle von Eingaben bei **internen Verwaltungssystemen** des Auftragnehmers erfolgt durch: ▪ Protokollierung und Nachvollziehbarkeit von Eingaben, Änderungen und Löschung von Daten (durch Logfiles) ▪ Regelungen zum Zugriff und zur Löschung der Protokolle **Bei „Root Server", „Virtual Server" und "Cloud Server" Verträgen** ▪ Die Verantwortung der Eingabekontrolle obliegt dem Auftraggeber **Bei „Managed Server", „Managed Hosting" und „Webhosting" Verträgen** ▪ Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst. ▪ Änderungen der Daten werden protokolliert
Verfügbarkeit, Belastbarkeit, Wiederherstellbarkeit Bezüglich Umgang mit personenbezogenen Daten	**Maßnahmen**
7. Verfügbarkeitskontrolle (von Daten) Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.	Bei **internen Verwaltungssystemen** des Auftragnehmers: ▪ Backup-Recovery-Strategie mit täglicher Sicherung aller relevanten Daten ▪ Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogrammen, SPAM-Filter) ▪ Einsatz von Festplattenspiegelung (RAID) bei allen relevanten Servern ▪ Monitoring aller relevanter Server ▪ Protokollierung und Auswertungen von Störungsvorfällen ▪ Unterbrechungsfreie und redundante Stromversorgung (USV) ▪ Aktiver DDoS-Schutz ▪ Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt wer im Fehlerfall zu informieren

	ist, um die betroffenen Systeme schnellstmöglich wiederherzustellen **Bei „Root Server“, „Virtual Server” und “Cloud Server” Verträgen** ▪ Datensicherung obliegt dem Auftraggeber ▪ Unterbrechungsfreie und redundante Stromversorgung (USV) ▪ Brandschutzeinrichtungen (Feuer- und Rauchmeldeanlagen, Feuerlöscher) ▪ Ersatz- und Austauschkomponenten vorhanden **Bei „Managed Server“, „Managed Hosting“ und „Webhosting” Verträgen** ▪ Backup- und Recovery Konzept mit täglicher Sicherung der Daten je nach gebuchten Leistungen des Auftrages ▪ Einsatz von Festplattenspiegelung (RAID) bei allen Servern ▪ Unterbrechungsfreie und redundante Stromversorgung (USV) ▪ Brandschutzeinrichtungen (Feuer- und Rauchmeldeanlagen, Feuerlöscher) ▪ Ersatz- und Austauschkomponenten vorhanden ▪ Einsatz von Software-Firewalls und Portreglementierungen
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung	**Maßnahmen**
8. Auftragskontrolle Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.	▪ Sorgfältige Auswahl von Dritten (insb. wegen Datensicherheit) in Zusammenarbeit mit dem Datenschutzbeauftragten (soweit möglich nur ISO/IEC- 27001:2005 zertifizierte Unternehmen/ Rechenzentren), ▪ Sofern die Campusspeicher GmbH Subunternehmen mit Aufgaben betraut, gelten für diesen die gleichen Regelungen und Bestimmungen wie für die Campusspeicher GmbH selbst.
9. Sonstiges Anpassung der innerbetrieblichen Organisation an die besonderen Anforderungen des Datenschutzes.	▪ Die Leistungen von Campusspeicher orientieren sich soweit möglich an den Vorgaben der Normen der ISO-27001 Zertifizierung ▪ Erarbeitung eines IT-Sicherheits- und Datenschutzkonzepts ▪ Ein Incident-Response-Management ist vorhanden ▪ Datenschutzfreundliche Voreinstellungen werden bei Softwareentwicklungen berücksichtigt