

Technische und organisatorische Maßnahmen

Organisationssicherheitsrichtlinien der kubus IT

Der Auftragnehmer sichert zu, die Organisationssicherheitsrichtlinien der kubus IT (Auftraggeber) einzuhalten. Er weist deren Umsetzung durch Ausfüllen und Übermittlung des von der kubus IT dafür bereitgestellten Nachweismusters¹ nach. Die Organisationssicherheitsrichtlinien gehen allen anderen Vertragsbestandteilen vor.

Die in den Anforderungen der Organisationssicherheitsrichtlinien der kubus IT enthaltenen Standards können nur insoweit wirksam unterschritten werden, als dies gemeinsam von den Parteien ausdrücklich und unter Bezugnahme auf die jeweilige konkrete Anforderung sowie mit Darstellung der resultierenden Risiken und der stattdessen umzusetzenden Maßnahmen vereinbart wird.

Auditrecht

Der Auftragnehmer gewährt (i) dem Auftraggeber, (ii) den Gesellschaftern des Auftraggebers, (iii) vom Auftraggeber oder den Gesellschaftern des Auftraggebers beauftragten, zur Berufsverschwiegenheit oder anderweitig zu Verschwiegenheit verpflichteten Dritten, (iv) den für den Auftraggeber zuständigen Aufsichtsbehörden und Prüfdiensten, und (v) den für die Begünstigten zuständigen Aufsichtsbehörden und Prüfdiensten (die vorstehend genannten Personen und Einrichtungen jeweils einzeln der „Auditor“, sowie gemeinsam die „Auditoren“) auf Anforderung des Auftraggebers und/oder eines Auditors jederzeit (im Regelfall aber im Rahmen der üblichen Geschäftszeiten, anders bei Dringlichkeit, insbesondere bei anlassbezogenen bzw. sicherheitsvorfallbezogenen Prüfungen) unmittelbar Zugriff auf Unterlagen, Systeme und Daten des Auftragnehmers sowie Zugang zu seinen Einrichtungen. Die vorstehenden Auditrechte enden 5 (fünf) Jahre nach Beendigung dieses Vertrags. Nach Ablauf der vorstehenden fünf Jahre sind Audits nur noch möglich, soweit ausnahmsweise rechtliche oder vertragliche Anforderungen zu erfüllen sind. Soweit Gesetzliche Bestimmungen weitergehende Anforderungen an Audits stellen, gehen diese den vorstehenden Regelungen vor und sind vom Auftragnehmer zu erfüllen.

Gesetzliche Anforderungen an die technischen und organisatorischen Maßnahmen

Die vom Auftragnehmer einzuhaltenden technischen und organisatorischen Maßnahmen müssen neben den sonstigen gesetzlichen und vertraglichen Anforderungen geeignet, angemessen und wirksam sein, um Betriebs- und Geschäftsgeheimnisse im Sinne des Geschäftsgeheimnisgesetzes (GeschGehG), personenbezogene Daten im Sinne der Datenschutzgrundverordnung (DSGVO) sowie im Sinne des Sozialgesetzbuches (SGB) zu schützen sowie den sicheren Betrieb der kritischen Infrastrukturen (BSIG) zu gewährleisten. Für den Fall, dass es an einer spezifischeren Regelung fehlt, vereinbaren die Parteien, dass

¹ i.d.R. Organisationssicherheitsrichtlinien der kubus IT (Externe.pdf, Vorlage Nachweisdokument.xlsx)

alle Informationen im Kontext der Leistungserbringung für den Auftraggeber der Geheimhaltung durch den Auftragnehmer unterliegen.

Folgende **gesetzliche Mindestanforderungen** müssen daher erfüllt sein:

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

- Zutrittskontrolle
Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, Gegenmaßnahmen sind insbesondere: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pfortner, Alarmanlagen, Videoanlagen;
- Zugangskontrolle
Keine unbefugte Systembenutzung, Gegenmaßnahmen sind insbesondere: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- Zugriffskontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, Gegenmaßnahmen sind insbesondere: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;
- Trennungskontrolle
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, Maßnahmen sind insbesondere: Mandantenfähigkeit, Sandboxing;
- Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO) 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 entsprechenden technischen und organisatorischen Maßnahmen unterliegen;

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

- Weitergabekontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, Gegenmaßnahmen sind insbesondere: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;

- Eingabekontrolle
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, Maßnahmen sind insbesondere: Protokollierung, Dokumentenmanagement;

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

- Verfügbarkeitskontrolle
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, Gegenmaßnahmen sind insbesondere: Backup-Strategie
- (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Viren-schutz, Firewall, Meldewege und Notfallpläne;
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO).

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

- Datenschutz-Management;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
- Auftragskontrolle