Grundlegende Anforderungen zu Informationssicherheit

Für Verträge mit IT-gestützter Verarbeitung von Daten von cellcentric.

1. Der Auftragnehmer verpflichtet sich alle Informationen und Daten, die der Auftragnehmer für den Auftraggeber erhebt oder verarbeitet, oder auf die er Zugriff hat, stets nach dem jeweils aktuellen Stand der Technik wirksam gegen unberechtigten Zugriff, Veränderung, Zerstörung oder Verlust, unerlaubte Übermittlung, anderweitige unerlaubte Verarbeitung und sonstigem Missbrauch zu sichern. Dafür verfügt der Auftragnehmer über ein geeignetes Sicherheitskonzept.

2. Der Auftragnehmer stimmt sein Sicherheitskonzept mit dem Auftraggeber ab. Insbesondere sind die im Lastenheft oder in anderen schriftlichen Spezifikationen definierten Anforderungen und Vorgaben für die Informationssicherheit einzuhalten und für das Sicherheitskonzept zu berücksichtigen. Der zuständige Informationssicherheitsbeauftragte des Auftraggebers unterstützt dabei. Der Auftraggeber kann einen geeigneten, regelmäßig schriftlichen Nachweis über die Umsetzung und Einhaltung des Sicherheitskonzepts verlangen. Bei Anlass zu Zweifeln ermöglicht der Auftragnehmer dem Auftraggeber auch eine Besichtigung vor Ort und erteilt notwendige Auskünfte.

3. Der Auftragnehmer benennt einen mit hinreichenden Befugnissen ausgestatteten Ansprechpartner für Security Management, der für sämtliche Themen zur Informationssicherheit zur Verfügung steht, z.B. für Incident Management (Management von Informationssicherheitsvorfällen).

4. Der Auftragnehmer hat den Auftraggeber über wesentliche Änderungen der Datenverarbeitung in Textform zu informieren. Änderungen sind insbesondere dann wesentlich, wenn sie das Sicherheitskonzept betreffen. Die Mitteilung muss den Umfang der Änderung und die Auswirkung auf das Sicherheitskonzept beschreiben. Bei einer absehbaren Minderung der Schutzwirkung ist vor der Änderung die Zustimmung des Auftraggebers in Textform einzuholen.

5. Die Informationen und Daten des Auftraggebers dürfen vom Auftragnehmer nur für die vertraglich vereinbarten Zwecke und soweit dies zur Vertragserfüllung erforderlich ist genutzt werden. Bei Verarbeitung von Daten verschiedener Auftraggeber ist deren Trennung nachprüfbar zu gewährleisten (Mandantentrennung).

6. Ein Zugriff auf Datenverarbeitungsanlagen („DV-Anlagen“) des Auftraggebers oder dessen Unterauftragnehmer darf nur mit Erlaubnis des Auftraggebers im erlaubten und für die Vertragserfüllung erforderlichen Umfang durch die dazu berechtigten Personen erfolgen. Der Auftragnehmer verpflichtet sich, keinem Unbefugten die ihm zur Nutzung des Systems zugeteilten Zugriffsberechtigungen bekannt zu geben. Dem Auftragnehmer ist es nur nach Zustimmung des Auftraggebers gestattet, etwaigen Subunternehmern oder freien Mitarbeitern im vertragserforderlichen Umfang den Zugriff auf die DV-Anlagen des Auftraggebers, seiner Beauftragten oder Subunternehmer zu ermöglichen. Der Auftragnehmer muss dem Auftraggeber unverzüglich mitteilen, wenn Mitarbeiter des Auftragnehmers, Subunternehmers oder freie Mitarbeiter mit Zugangs- oder Zugriffsberechtigungen für DV-Anlagen des Auftraggebers, seiner Beauftragten oder Subunternehmer nicht mehr mit der Erfüllung der vertragsgegenständlichen Leistung befasst sind, damit der Auftraggeber bestehende Zugangs- und Zugriffsberechtigungen entziehen kann.

7. Alle vom Auftraggeber als vertraulich oder geheim eingestufte Informationen des Auftraggebers sind vom Auftragnehmer durch geeignete kryptographische Maßnahmen nach aktuellem Stand der Technik bei der Übertragung sowie bei einer Speicherung auf mobilen Datenträgern zu schützen; bei einer Übertragung oder Speicherung innerhalb einer gesicherten Umgebung ist dies nicht erforderlich. Der Auftragnehmer weist auf Anforderung des Auftraggebers nach, dass die Umgebungen für die Verarbeitung vertraulicher oder geheimer Daten nach dem jeweils aktuellen Stand der Technik ausgelegt sind.

8. Der Auftragnehmer hat den Auftraggeber bei Kenntniserlangen oder begründetem Verdacht auf Datenschutzverletzungen, Sicherheitsverletzungen und anderen Manipulationen des Verarbeitungsablaufs, die cellcentric-Daten und -Services betreffen, unverzüglich zu informieren und sofort – in Abstimmung mit dem Auftraggeber – alle erforderlichen Schritte zur Aufklärung des Sachverhalts einzuleiten und zur Schadensbegrenzung einzuleiten.

9. Findet die Datenverarbeitung bei cellcentric oder im Datenaustausch mit cellcentric-Systemen statt, so wird der Auftragnehmer, sofern erforderlich, geeignete Maßnahmen ergreifen, damit es zu keiner Beeinträchtigung der cellcentric-Infrastruktur (und von Dritten aus der cellcentric-Umgebung heraus) kommt. Der Auftragnehmer hat die jeweils gültigen Informationssicherheitsanforderungen des Auftraggebers zu befolgen.

10. Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, falls durch Pfändung, Beschlagnahme oder sonstigen behördlichen Zugriff, in einem Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter die Gefahr besteht, dass nicht berechtigte Personen auf Daten von cellcentric zugreifen. Der Auftragnehmer wird die Dritten darüber informieren, dass es sich um Daten von cellcentric handelt.

11. Der Auftragnehmer informiert regelmäßig seine Mitarbeiter, Subunternehmer oder freien Mitarbeiter mit Zugangs- oder Zugriffsberechtigungen für DV-Anlagen des Auftraggebers über relevante Themen der Informationssicherheit im Zusammenhang mit der Leistungserbringung für den Auftraggeber.