Security AGBs für IT-Beschaffungen des Landes Steiermark zur Wahrung der Informationssicherheit

Die Security AGBs für IT-Beschaffungen des Landes Steiermark zur Wahrung der Informationssicherheit dienen der Sicherstellung der Geheimhaltung von schutzwürdigen Informationen und Daten und der Verschwiegenheit zwischen den jeweiligen Stellen des Landes Steiermark (Auftraggeber) und deren Geschäftspartnern (Auftragnehmer) sowie der Qualitätssicherung im Bereich der Informationssicherheit.

Insbesondere sollen die Berücksichtigung und Umsetzung der relevanten Bestimmungen der Datenschutz-Grundverordnung (DSGVO) in Zusammenhang mit vom Auftragnehmer für den Auftraggeber durchgeführten Auftragsverarbeitungen gewährleistet werden.

Die Security AGBs gelten insoweit, als diese nicht ausdrücklich festgelegten Sicherheitsbestimmungen in den Vereinbarungen zuwiderlaufen, denen sie beigelegt sind (z.B. projektbezogene Ausschreibungsunterlagen, Verträge).

1 Datenschutz - Personenbezogene Daten

Für den Fall, dass der Auftragnehmer personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Z 2 und Art. 28 DSGVO verarbeitet, werden alle Datenverarbeitungstätigkeiten ausschließlich innerhalb der EU bzw. des EWR durchgeführt.

1.1 Rechte und Pflichten des Auftraggebers

- Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen gemäß Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich.
- Der Auftraggeber hat dem Auftragnehmer unverzüglich und vollständig mitzuteilen, wenn in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen festgestellt werden.
- Der Auftraggeber hat das Recht, Weisungen und Aufträge zur Sicherstellung der rechts- und auftragskonformen Auftragserfüllung sowie betreffend Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung zu erteilen. Alle Aufträge, Teilaufträge und Weisungen ergehen grundsätzlich schriftlich (dem ist ein dokumentiertes elektronisches Format gleichzuhalten). Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen.

1.2 Rechte und Pflichten des Auftragnehmers (Art. 28 Abs. 3 DSGVO)

- Der Auftragnehmer verpflichtet sich, Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers zu verarbeiten, außer es liegt ein Ausnahmefall gemäß Art. 28 Abs. 3 lit. a DSGVO (z.B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden) vor. Eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers bedarf eines schriftlichen Auftrags; Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.
- Der Auftragnehmer hat geeignete Maßnahmen zu ergreifen, um die Einhaltung der Verschwiegenheitspflicht sicherzustellen und damit nur befugte Personen (Auftragnehmer, befasste MitarbeiterInnen und andere erforderliche beigezogene Personen) Zugang zu den verfügbaren Daten haben. Der Auftragnehmer garantiert, dass er sämtliche Personen, die Zugang zu diesen Daten haben, vor Aufnahme der Tätigkeit zur Verschwiegenheit verpflichtet hat oder diese einer gesetzlichen Verschwiegenheitspflicht

unterliegen. Die Verschwiegenheitsverpflichtung bleibt auch nach Beendigung ihrer Tätigkeit und nach dem Ausscheiden beim Auftraggeber aufrecht.

- Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung gem. Art. 32 DSGVO ergriffen hat. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und 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 Abs. 1 DSGVO zu berücksichtigen.
- Der Auftragnehmer ergreift alle erforderlichen technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Personen nach Kapitel III DSGVO (Information, Auskunft, Berichtigung, Löschung, Datenübertragbarkeit, Widerspruch sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Frist jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen.
  Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken.
  Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragssteller ihn irrtümlich für den Verantwortlichen der von ihm betriebenen Datenanwendung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.
- Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Personen, Datenschutz-Folgeabschätzung, vorherige Konsultationen).
- Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder seiner Mitarbeiter (Sub-Auftragsverarbeiter) sowie Verstöße gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen bei der Verarbeitung personenbezogener Daten mit.
- Der Auftragnehmer ist nach der Beendigung der Erbringung der Verarbeitungstätigkeit verpflichtet, alle personenbezogenen Daten, erstellten Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftragnehmer bekannt zu geben. Nach Bestätigung durch den Auftraggeber hat er diese Daten je nach Vorgabe des Auftraggebers entweder zu übergeben und/oder zu vernichten. Er hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber unverzüglich vorzulegen.
- Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm übergebenen personenbezogenen Daten das Recht auf jederzeitige Einsichtnahme und Kontrolle (Inspektion) - sei es auch durch von ihm beauftragte Dritte - eingeräumt. Der Auftragnehmer verpflichtet sich, an diesen Kontrollen umfassend mitzuwirken und dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind .
- Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Auffassung ist, dass eine Weisung des Auftraggebers gegen Datenschutzbestimmungen der Union oder nationales Recht verstößt.
- Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er – sofern gesetzlich zulässig – den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen.
- Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften (DSGVO und nationalen Vorschriften) bekannt sind.
- Dem Auftraggeber ist bewusst, dass er die Auftragsverarbeitung in ein Verarbeitungsverzeichnis nach Art. 30 DSGVO aufzunehmen hat.

2 Schutz nicht-personenbezogener Daten und Informationen

Sämtliche Daten des Landes Steiermark, die im Zuge des Auftrages außerhalb des Landesbereiches verfügbar wurden, sind nach erfolgter Erledigung der Aufgabe und/oder bei Beendigung des Vertragsverhältnisses mit dem Auftraggeber sofort zu löschen bzw. zu vernichten.

Insbesondere nimmt der Auftragnehmer zur Kenntnis, dass

- es untersagt ist, unbefugten Personen oder unzuständigen Stellen Daten oder Informationen mitzuteilen oder ihnen die Kenntnisnahme zu ermöglichen, sowie Daten zu einem anderen als dem zur Erfüllung des Auftrages gehörenden Zweck zu verwenden,
- automationsunterstützt verarbeitete Daten, die aufgrund der Erfüllung des Auftrages dem Auftragnehmer anvertraut wurden, von diesem nur aufgrund ausdrücklicher Anordnung des Auftraggebers übermittelt werden dürfen,
- eine über den Auftragszweck hinausgehende weitere Verarbeitung dieser Daten durch den Auftragnehmer unzulässig ist,
- die gegenständlichen Verpflichtungen auch nach Auftragsbeendigung bzw. Ausscheiden eines Mitarbeiters aus der Firma des Auftragnehmers fortbestehen.

3 Sub-Auftragsverarbeiter

Der Auftragnehmer ist berechtigt einen Sub-Auftragsverarbeiter zu beauftragen. Der Auftragsverarbeiter ist jedoch verpflichtet, den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter zu informieren, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber dem Sub-Auftragsverarbeiter gelten. Die Aufgaben sind so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Sub-Auftragsverarbeiters deutlich voneinander abgegrenzt werden können. Kommt der Sub-Auftragsverarbeiter seinen vertraglichen Verpflichtungen nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters. Änderungen des Sub-Auftragsverarbeiters bedürfen der ausdrücklichen schriftlichen Zustimmung des Auftraggebers.

4 Sicherheitsanforderungen für IT-Lösungen

4.1 Lieferung von securitygeprüfter Software

Der Auftragnehmer erklärt, für die von ihm gelieferte bzw. bereitgestellte Software (bzw. Updates) zumindest einen der folgenden Web-Application-Security-Industriestandards- wie OWASP Top 10 Liste , CWE / SANS Top 25 oder WASC Threats – in der zum Zeitpunkt der Lieferung aktuellen Version berücksichtigt zu haben.

4.2 Zustimmung für eine nachträgliche Security-Prüfung der Software

Der Auftragnehmer erklärt sich einverstanden, dass die von ihm gelieferte Software vom Auftraggeber selbst oder von einem von ihm beauftragten Security-Test-Unternehmen hinsichtlich der OWASP Top 10 bzw. anderer möglicher Schwachstellen einem Blackbox bzw. Greybox Test unterzogen werden kann. Die dabei evtl. festgestellten Mängel werden vom Auftraggeber (bzw. dem beauftragten Unternehmen) vertraulich behandelt.

4.3 Behebung festgestellter Security-Mängel

Die bei einer Security-Prüfung festgestellten Mängel sind im Zuge der Leistungsabnahme bzw. während der gesetzl. Gewährleistungszeit bzw. der Laufzeit eines allfällig abgeschlossenen Software-Wartungsvertrages vom Auftragnehmer auf seine Kosten umgehend und möglichst rasch zu beheben.

4.4 Haftung

Der Auftragnehmer haftet für Schäden, welche durch die Nichteinhaltung der Sicherheitsanforderungen für IT-Lösungen entstanden sind, im Rahmen der rechtlichen Bestimmungen.

4.5 Zustimmung für die Erstellung einer Software Bill of Materials (SBOM)

Der Auftragnehmer verpflichtet sich zur Erstellung einer Software Bill of Materials (SBOM), für die von ihm gelieferte bzw. bereitgestellte Software (bzw. Updates). In der SBOM sind alle für die Erstellung eines Softwareprodukts verwendeten Komponenten wie Bibliotheken oder Pakete aufgezählt (dazu zählen Open-Source-Softwarepakete oder Softwarekomponenten von Drittherstellern). Eine „Software-Komponente“ im Sinne dieser Security ABGs muss einer einzelnen, ausführbaren Datei entsprechen. Die SBOM muss die folgenden Mindestelemente enthalten:

- Name des Anbieters
- Komponentenname
- Version der Komponente
- Andere eindeutige Identifikatoren
- Abhängigkeitsbeziehung
- Autor der SBOM-Daten
- Zeitstempel

Für jede Softwareversion muss eine neue, eigene SBOM erzeugt werden. Eine neue Version der SBOM zu einer gegebenen Softwareversion muss genau dann erzeugt werden, wenn mehr Informationen zu den eingebundenen Software-Komponenten zur Verfügung gestellt werden oder Fehler in den SBOM-Daten korrigiert werden.

5 Schutz von Speichermedien

Beim Austausch bzw. bei der Rücknahme von Geräten oder Geräteteilen durch den Auftragnehmer ist sicher zu stellen, dass keine Daten an Dritte gelangen. Daher müssen alle Speichermedien (Festplatten, Sticks etc.), auf denen Daten der Steiermärkischen Landesregierung gespeichert waren bzw. gespeichert sind bzw. gespeichert sein könnten, nachweislich derart zerstört werden, dass eine Wiederherstellung von Daten ausgeschlossen ist.

6 Remote-Zugang

Ein allfällig vereinbarter Remote-Zugang zum Landesdatennetz ist ausschließlich den mit dem Support des Auftragsgenstandes betrauten Personen zu ermöglichen.

7 Werbeverbot

Eine Verwertung von Daten über erteilte Aufträge bzw. Zuschläge für Marketingzwecke, wie z.B. Pressemitteilungen, Aussendungen, Prospekten, Referenzlisten und dgl. bedarf einer ausdrücklichen, im Vorhinein schriftlich erteilten Zustimmung des Auftraggebers. Die Angabe von Referenzdaten im Rahmen der Angebotslegungen zu Vergabeverfahren öffentlicher Auftraggeber ist jedoch zulässig.

8 Zustimmung des Auftragnehmers

Die Security AGBs für IT-Beschaffungen des Landes Steiermark zur Wahrung der Informationssicherheit gelten vom Auftragnehmer mit Annahme des jeweiligen Auftrages als akzeptiert.

9 Schlussbestimmungen

Beide Parteien sind verpflichtet, alle im Rahmen der Vereinbarung erlangten Kenntnisse über Geschäftsgeheimnisse und/oder Datensicherheitsmaßnahmen der jeweils anderen Partei vertraulich zu behandeln.
Diese Verpflichtung bleibt auch nach Beendigung der Vereinbarung bestehen.

Änderungen und Ergänzungen dieser Vereinbarung (insb. betreffend Verarbeitungsgegenstand und Verfahrensänderungen) sowie alle auf dieser Vereinbarung bezugshabenden Bestandteile bedürfen zu ihrer Wirksamkeit ausnahmslos der Schriftform. Mündliche Nebenabreden zu dieser Vereinbarung bestehen nicht und sind unzulässig.

Den Anweisungen des Auftraggebers bezüglich der sicheren Nutzung der IT-Infrastruktur des Auftraggebers ist jedenfalls Folge zu leisten.

Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein oder werden, so berührt dies nicht die Wirksamkeit der übrigen Inhalte dieser Vereinbarung. An Stelle der nichtigen, unwirksamen oder rechtsungültigen

Bestimmung gilt jene Regelung als vereinbart, die dem wirtschaftlichen Interesse der Vereinbarungspartner möglichst nahe kommt.

Bei Verstoß des Auftragnehmers gegen die Regelungen dieser Vereinbarung, insbesondere zur Einhaltung des Datenschutzes, ist der Auftraggeber berechtigt, entsprechenden Schadenersatz vom Auftragnehmer zu fordern und das Auftragsverhältnis fristlos zu kündigen.

10 Gerichtsstand und Rechtswahl

Sämtliche Vertragsparteien vereinbaren, dass auf das gegenständliche Rechtsgeschäft einschließlich aller Fragen betreffend sein Zustandekommen ausschließlich österreichisches Recht unter Ausschluss der Anwendbarkeit aller auf fremdes Recht (einschließlich des UN-Kaufrechtes) verweisenden Rechtsnormen anzuwenden ist. Darüber hinaus bestimmen sämtliche Vertragsparteien für alle aus diesem Vertrag etwa entstehenden Rechtsstreitigkeiten gemäß § 104 JN einvernehmlich den ausschließlichen Gerichtsstand des jeweils sachlich zuständigen Gerichtes mit Sitz in Graz-Ost.