

Für den öffentlichen Gebrauch freigegeben

Ergänzende Vertragsbedingungen der Apleona Gruppe zu Anforderungen an die Informationssicherheit für Lieferanten

Inhaltsverzeichnis

1	Präambel.....	3
2	Anforderungen an die Informationssicherheit.....	3
2.1	Management der Informationssicherheit.....	3
2.2	Rollen und Ansprechpartner.....	3
2.3	Sicherheitsüberprüfung.....	4
2.4	Statusbericht.....	4
2.5	Qualifiziertes Personal.....	4
2.6	Verpflichtung Nachunternehmer.....	4
2.7	Verschlüsselung.....	4
2.8	Rechtsräume Hosting.....	4
2.9	Löschung von Daten.....	4
2.10	Endgeräte.....	5
2.11	Meldung Sicherheitsvorfälle.....	5
2.12	Wiederherstellung sicherer Zustand.....	5
2.13	Zugriffe.....	5
2.14	Betriebssicherheit.....	5
3	Bewertung des Reifegrads der Informationssicherheit beim Auftragnehmer.....	6
3.1	Informationen der Sicherheitsorganisation.....	6
3.2	Audit.....	6

1 Präambel

- Der Auftragnehmer unterstützt den Auftraggeber durch mit Informationstechnologie unterstützten Dienstleistungen (z.B. Beratungstätigkeiten), bzw. liefert oder stellt dem Auftraggeber IT (Information Technology) oder OT (Operational Technology) Produkte zur Verfügung, die im Vertrag näher spezifiziert werden.
- Diese Vertragsbedingungen regeln ergänzend Anforderungen an die Informationssicherheit, die vom Auftragnehmer zu erfüllen sind.
- Die vom Vertrag abgedeckten Informationen und Anwendungen unterliegen einem definierten Schutzbedarf (normal, hoch, sehr hoch), aus dem sich die konkrete Ausgestaltung der Maßnahmen zur Informationssicherheit ableitet. Der Schutzbedarf selbst, sowie Details zu Maßnahmen, sind in der Leistungsbeschreibung oder im Vertrag beschrieben.
- Neben diesen Ergänzenden Vertragsbedingungen der Apleona GmbH zu Anforderungen der Informationssicherheit können im Einzelfall Anforderungen an die Informationssicherheit eines Kunden des Auftraggebers an den Auftragnehmer weitergegeben werden. Diese sind Bestandteil des Vertrages zwischen Auftraggeber und Auftragnehmer. Hinsichtlich der Rangfolge von Anforderungen an die Informationssicherheit verschiedener Herkunft gilt folgende: Zunächst die Anforderungen der Kunden des Auftraggebers, danach diese Ergänzenden Vertragsbedingungen der Apleona GmbH zu Anforderungen der Informationssicherheit.
- Soweit nicht ausdrücklich etwas anderes vereinbart wird, sind etwaige dem Auftragnehmer durch die Umsetzung der nachfolgenden Anforderungen entstehenden Aufwände mit der vereinbarten Vergütung abgegolten.

2 Anforderungen an die Informationssicherheit

2.1 Management der Informationssicherheit

Der Auftragnehmer hat in seinem Unternehmen geeignete Prozesse zur Gewährleistung der Informationssicherheit im Rahmen der Leistungserbringung etabliert und hält dieses während der gesamten Vertragslaufzeit aufrecht. Beispielsweise geschieht dies in Form eines angemessenen Informationssicherheitsmanagementsystems (ISMS) oder durch gleichwertige, geeignete Prozesse zur Gewährleistung der Informationssicherheit im Rahmen der Leistungserbringung. Die Informationssicherheitsprozesse des Auftragnehmers entsprechen mindestens den nachfolgend beschriebenen Informationssicherheitsanforderungen und orientieren sich an der ISO/IEC 27001 oder einer gleichwertigen Anforderung.

2.2 Rollen und Ansprechpartner

a) Koordinator Informationssicherheit

Der Auftragnehmer muss dem Auftraggeber für alle Aspekte rund um Informationssicherheit einen sachkundigen Ansprechpartner (z.B. Informationssicherheitsbeauftragten, IT-Sicherheitsmanager bzw. Chief Information Security Officer (CISO)) benennen, der gegenüber dem Auftraggeber in allen Fragen des Managements der Informationssicherheit auskunftsfähig und auskunftsberechtigt ist.

b) Ansprechpartner Regelkommunikation

Der Auftraggeber kann vom Auftragnehmer verlangen, weitere Ansprechpartner / Rollenverantwortliche in allen informationssicherheitsrelevanten Angelegenheiten im Kontext der beauftragten Leistung zu benennen (z.B. fachlich, technisch oder betrieblich Verantwortliche) und die Aufgabenverteilung und den Verantwortungsübergang zweifelsfrei zu klären. Änderungen teilt der Auftragnehmer dem Auftraggeber unverzüglich mit.

c) Ansprechpartner Notfallkoordination

Der Auftragnehmer benennt einen zentralen Ansprechpartner (Single Point of Contact (SPOC)) zur Notfallkommunikation, der dem Auftraggeber zur Verfügung steht. Der SPOC hat im Notfall Zugriff auf alle notwendigen Daten des Auftragnehmers (z.B. Produkt Monitoring, Identity Access Management (IAM) und Konfigurationsdaten) und stellt diese dem Auftraggeber und dessen Notfallteam auf Anforderung und in geeignetem Format (les- und verarbeitbar) zur Verfügung.

2.3 Sicherheitsüberprüfung

Der Auftraggeber behält sich vor, vom Auftragnehmer für Mitarbeiter oder sonstige von ihm im Rahmen der Leistungserbringung eingesetzten Personen, die in Kontakt mit vom Auftraggeber als besonders schützenswert kategorisierten Informationen und Anlagen oder kritischen Infrastrukturen im Sinne der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) kommen, die Durchführung einer Sicherheitsüberprüfung gemäß dem Handbuch für den Geheimschutz in der Wirtschaft des Bundesministeriums für Wirtschaft und Energie („Geheimschutzhandbuch“) zu verlangen. Der Auftragnehmer weist dem Auftraggeber, die erfolgreiche Durchführung der Sicherheitsüberprüfung in Textform nach.

2.4 Statusbericht

Der Auftraggeber kann vom Auftragnehmer einen Statusbericht zur Informationssicherheit der bezogenen Leistung anfordern. Dieser enthält z.B. Informationen zu Abweichungen von vereinbarten Informationssicherheitsanforderungen, Verlaufsstatistiken zu Sicherheitsvorfällen und Sicherheitspatches, Status zum Schwachstellenmanagement und Auditergebnissen, Verfügbarkeit von Security Controls, Aufwände zur Behebung von Incidents und Fakturierung bei gesonderter Vereinbarung von Sicherheitsmaßnahmen.

2.5 Qualifiziertes Personal

Der Auftragnehmer stellt sicher, dass das von ihm eingesetzte Personal die zur Auftragserbringung notwendige Qualifikation und Bewusstsein hinsichtlich der Anforderungen zur Informationssicherheit besitzt und weist dies dem Auftraggeber auf Anfrage nach.

2.6 Verpflichtung Nachunternehmer

Der Auftragnehmer gewährleistet, dass seine in Bezug auf dieses Vertragsverhältnis eingesetzten Nachunternehmer und, so weit im Vertrag vereinbart, deren Nachunternehmer die Anforderungen aus diesem Vertrag, die der ISO/IEC 27001 oder solche einer vergleichbaren Norm erfüllen. Er stellt entsprechende Nachweise auf Anforderung des Auftraggebers zur Verfügung.

2.7 Verschlüsselung

Der Auftragnehmer gewährleistet eine verschlüsselte Übertragung und Speicherung von Daten der Stufen "vertraulich" und "streng vertraulich". Erfolgt die Speicherung nicht beim Auftragnehmer, ist dieses dem Auftraggeber anzuzeigen.

2.8 Rechtsräume Hosting

Der Auftragnehmer verpflichtet sich alle Länder, in denen Daten des Auftraggebers durch den Auftragnehmer oder einen seiner Nachunternehmer verarbeitet oder gespeichert bzw. Anwendungen betrieben werden, zu benennen. Der Auftragnehmer sichert hiermit zu, dass die Daten die benannten Speicherorte nicht verlassen. Umzüge innerhalb der EU sind hiervon ausgenommen, müssen dem Auftraggeber aber unverzüglich in Textform mitgeteilt werden. Ein Verstoß gegen diese Regelung berechtigt den Auftraggeber zur außerordentlichen Kündigung des Vertrags.

2.9 Löschung von Daten

Der Auftragnehmer gewährleistet, sämtliche im Zusammenhang mit dem Auftragsverhältnis stehenden Daten an allen primären und sekundären Standorten des Auftragnehmers und seiner Nachunternehmer bei Beendigung des Vertrags unverzüglich und sicher zu löschen und zu vernichten, so dass diese nicht wiederhergestellt werden können.

Ausnahmen bestehen nur bei Daten, zu deren Aufbewahrung der Auftragnehmer gesetzlich verpflichtet ist oder dies vertraglich geregelt wurde. Der Auftragnehmer weist dies auf Verlangen des Auftraggebers nach.

2.10 Endgeräte

Sofern der Auftragnehmer eigene Endgeräte zur Erbringung der vereinbarten Dienstleistung einsetzt, verpflichtet er sich zur Einhaltung der nachstehend genannten Vorgaben des Auftraggebers. Als Endgerät im Sinne dieser Regelung wird jedes IT-Asset des Auftragnehmers verstanden, das an IT-Applikationen sowie IT-Infrastruktur des Auftraggebers (kabelgebunden oder kabellos) angebunden ist oder zur Verarbeitung von Daten des Auftraggebers eingesetzt wird.

- Die Endgeräte müssen nach dem jeweils aktuellen Stand der Technik abgesichert sein.
- Privilegierte (z.B. administrative) Accounts sind getrennt von Standard-Accounts und dürfen nicht für die reguläre Arbeit genutzt werden.
- Der Auftragnehmer verpflichtet sich die Kompromittierung eines Endgerätes unverzüglich an die Verantwortlichen des Auftraggebers zu melden und dieses umgehend zu deaktivieren und zu sperren.
- Der Einsatz von Hacking-Tools und ähnlichen Anwendungen ist untersagt, sofern dies nicht ausdrücklich zugelassen ist.
- Der Auftragnehmer ist dafür verantwortlich, dass keine Netzkopplung der Datennetze des Auftraggebers und den mit diesem verbundenen Unternehmen mit anderen Datennetzen stattfindet.

2.11 Meldung Sicherheitsvorfälle

Der Auftragnehmer verpflichtet sich, den Auftraggeber über alle Sicherheitsvorfälle oder Datenschutzverletzungen gemäß Art. 33 DSGVO zu informieren, die im Umfeld des Auftragnehmers oder eines seiner Nachunternehmer auftreten und Auswirkungen auf seine unmittelbare oder mittelbare Leistungserbringung haben. Die Meldung hat, sofern der Sicherheitsvorfall relevant für die Daten und Systeme des Auftraggebers und der mit diesem verbundenen Unternehmen ist, unverzüglich zu erfolgen. Sicherheitsvorfälle, die nicht die Daten und Systeme des Auftraggebers berühren, werden dem Auftraggeber im Rahmen des Statusberichts offengelegt.

2.12 Wiederherstellung sicherer Zustand

Im Falle eines für den Auftraggeber und der mit diesem verbundenen Unternehmen relevanten Sicherheitsvorfalls hat der Auftragnehmer neben der Information des Auftraggebers auch unverzüglich alle notwendigen Maßnahmen zu ergreifen, um die gebotene Sicherheit wiederherzustellen. Sofern hierfür ein konzertiertes Vorgehen mit dem Auftraggeber erforderlich ist, wird der Auftragnehmer sich mit detailliertem Maßnahmenkatalog an den Auftraggeber wenden und sich mit diesem abstimmen. Ist zur Bearbeitung der Maßnahmen die Unterstützung Dritter notwendig, gewährt der Auftragnehmer diesen Zugang zu allen notwendigen Informationen, Systemen und Betriebsstätten

2.13 Zugriffe

Ein direkter oder verdeckter Zugang zu den Informationssystemen (z.B. Infrastruktur, Programme, Datenbestände) des Auftraggebers und der mit diesem verbundenen Unternehmen ist dem Auftragnehmer nur dann gestattet, wenn er vom Auftraggeber eine ausdrückliche, dokumentierte Zugriffsberechtigung erhalten hat. Die Zugriffsberechtigung ist auf die eingesetzten und ausdrücklich zugelassenen Mitarbeiter des Auftragnehmers bzw. seiner Nachunternehmer beschränkt. Die Weitergabe der Zugriffsberechtigung an Dritte ist untersagt. Eine erteilte Zugriffsberechtigung darf ausschließlich im Rahmen der vertraglich übernommenen Leistungen genutzt werden.

2.14 Betriebssicherheit

Der Auftraggeber behält sich das Recht vor, Sperrungen und Überwachungen auf Grund behördlicher Anordnungen oder der Nutzungsbestimmungen vorzunehmen. Ebenfalls ist eine Unterbrechung des Netzzugangs jederzeit möglich, wenn durch die an das Netz angeschlossenen Geräte des Auftragnehmers in irgendeiner Weise die Betriebssicherheit bzw. das Betriebsverhalten des Netzes oder daran angeschlossener anderer Geräte oder Software beeinträchtigt werden. Vorgenanntes gilt vorbehaltlich abweichender Regelungen zum Umgang mit personenbezogenen Daten im Auftragsverhältnis.

3 Bewertung des Reifegrads der Informationssicherheit beim Auftragnehmer

3.1 Informationen der Sicherheitsorganisation

Der Auftragnehmer hat dem Auftraggeber auf Anforderung Informationen zu seiner Sicherheitsorganisation offenzulegen, auf deren Basis der Auftraggeber eine Bewertung des Reifegrads der Informationssicherheit durchführen kann. Dies können z.B. eine Management Summary zur Sicherheitsorganisation im Anwendungsbereich der Leistung, Berichte aus einem bestehenden Informationssicherheitsmanagementsystem, ein ISO/IEC 27001-Zertifikat, einschließlich der Erklärung der Anwendbarkeit (Statement of Applicability) bzw. äquivalente Nachweise oder aktuelle Auditergebnisse im Anwendungsbereich der Leistung sein.

3.2 Audit

Der Auftragnehmer stimmt zu, dass der Auftraggeber oder ein durch ihn beauftragter Dritter den Auftragnehmer während der Laufzeit des Vertrages in Bezug auf dessen Informationssicherheit und Einhaltung datenschutzrechtlicher Bestimmungen auditieren darf.

Basis der Audits in der Informationssicherheit ist die ISO/IEC 27001 sowie der jeweils aktuelle Stand der Technik. Geprüft wird die angemessene Umsetzung der vereinbarten Informationssicherheitsanforderungen bezogen auf den Auftrag (Dienstleistung, Produkt) und den Aufbau und die Wirksamkeit der Informationssicherheitsorganisation beim Auftragnehmer. Basis der datenschutzrechtlichen Audits sind die DSGVO sowie das BDSG.

Zwischen anlasslosen Audits sollen grundsätzlich mindestens zwei Jahre liegen. Deren Durchführung erfolgt zu üblichen Geschäftszeiten und die Dauer des Vor-Ort-Auditanteils beschränkt sich nach Möglichkeit auf einen bis zwei Arbeitstage. Der Auftraggeber kündigt ein anlassloses Regelaudit spätestens sechs Wochen vor dessen Durchführung an. Anlassbezogene Audits können in Abhängigkeit von der Schwere des Anlasses bzw. der Dringlichkeit auch kurzfristiger erfolgen.

Der Auftragnehmer stellt rechtzeitig (i.d.R. spätestens drei Wochen vor Durchführungstermin) die benötigten Unterlagen wie z.B. Managementberichte, betriebliche Unterlagen (Konfigurations- und Berechtigungsdaten), Berichte aus dem ISMS zur Verfügung und kommt seinen Mitwirkungspflichten, z.B. Erteilung der notwendigen Zugriffsrechte, Bereitstellen von Dokumentationen und Zugängen, im Rahmen des Audits nach.

Der Auftraggeber stellt dem Auftragnehmer die Ergebnisse des Audits in Berichtsform zur Verfügung. Der Auftragnehmer verpflichtet sich, die als kritisch gekennzeichneten Abweichungen zu beheben und den Fortschritt der Behebungen zu berichten. Auftraggeber und Auftragnehmer vereinbaren Umfang und Zeitplan dieser Verbesserungsprojekte einvernehmlich. Der Auftraggeber behält sich das Recht vor, den Fortschritt der Verbesserungsmaßnahmen vor Ort zu prüfen. Für die Vorbereitung dieser Prüfungen gilt der oben für Regelaudits genannte Zeitrahmen. Die beim Auftraggeber anfallenden Kosten eines anlasslosen Regelaudits werden vom Auftraggeber getragen. Die beim Auftraggeber anfallenden Kosten eines anlassbezogenen, z.B. durch einen Sicherheitsvorfall initiierten Audits werden vom Auftragnehmer getragen.

Soweit ein Audit nachweislich aus berufsrechtlichen Gründen nicht wie vom Auftraggeber geplant durchgeführt werden kann, informiert der Auftragnehmer den Auftraggeber zeitnah über diese Gründe. Die Parteien stimmen dann einen modifizierten Auditplan ab. Dabei werden sowohl das für den Auftragnehmer geltende Berufsrecht als auch die Interessen des Auftraggebers berücksichtigt.