Zusätzliche technische Vertragsbedingungen der HPA und der mit ihr verbundenen Unternehmen zu Anforderungen an die Informationssicherheit (ZTV Informationssicherheit)

1 Präambel

Der Auftragnehmer (AN) liefert dem Auftraggeber (AG) Dienstleitungen, die durch Informationstechnologie unterstützt werden bzw. IT- (Information Technology) oder OT- (Operational Technology) Produkte, die im Vertrag näher spezifiziert werden. IT- und OT-Systeme werden in diesem Dokument einheitlich als „Informationssysteme“ bezeichnet.

1.1 Diese ZTV regeln ergänzend Anforderungen bezüglich der Informationssicherheit, die vom AN zu erfüllen sind und gelten, soweit einschlägig, ergänzend zu den Bestimmungen „Datenschutz, Geheimhaltung und Sicherheit“ der jeweils anzuwendenden EVB-IT-AGB.

1.2 Die vom Vertrag abgedeckten Informationen und Anwendungen unterliegen den Vertraulichkeitsklassen[i] der HPA. Aus der Vertraulichkeitsklasse leitet sich die konkrete Ausgestaltung der Maßnahmen zur Informationssicherheit ab. Diese sind im Anhang aufgeführt.

1.3 Sollte es sich bei den Informationen um Verschlusssachen im Sinne des §4 Hamburgisches Sicherheitsüberprüfungs- und Geheimschutzgesetz (HmbSÜGG) handeln, ist die „Allgemeine Verwaltungsvorschrift zum Geheimschutz“ (HmbVSA) einschlägig. Weiterhin ist eine Speicherung und Verarbeitung nur auf Informationssystemen zulässig, welche in der jeweils aktuellen Fassung der „Liste der zugelassenen IT-Sicherheitsprodukte und -systeme“ des BSI aufgeführt sind.

1.4 Soweit die Parteien nicht ausdrücklich etwas anderes vereinbart haben, sind etwaige dem AN durch die Umsetzung der nachfolgenden Anforderungen entstehenden Aufwände mit der vereinbarten Vergütung abgegolten.

2 Anforderungen an die Informationssicherheit

2.1 Management der Informationssicherheit

Der AN verpflichtet sich, angemessene technische und organisatorische Maßnahmen zum Schutz der Informationen des AG zu ergreifen. Diese sind dem AG auf Verlangen darzulegen.

Als Nachweis dient zum Beispiel die Etablierung eines angemessenen Informationssicherheitsmanagementsystems (ISMS) oder gleichwertiger, vergleichbarer Frameworks zur Gewährleistung der Informationssicherheit im Rahmen der Leistungserbringung.

2.2 Rollen und Ansprechpartner

2.2.1 Ansprechpartner Informationssicherheit

AN und AG müssen mit Vertragsunterzeichnung für alle Aspekte rund um Informationssicherheit einen sicheren Kommunikationskanal vereinbaren sowie jeweils einen sachkundigen Ansprechpartner benennen, der in allen Fragen des Managements der Informationssicherheit auskunftsfähig und auskunftsberechtigt ist.

2.2.2 Ansprechpartner Notfallkoordination

AN und AG benennen zentrale Ansprechpartner / Single Point of Contact (SPoC) zur Notfallkommunikation und -Behandlung, die zu den vertraglich geregelten Fristen zur Verfügung stehen. Die Notfallkommunikation erfolgt über den sicheren Kommunikationskanal, siehe Kapitel 2.2.1.

2.3 Qualifiziertes Personal

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

2.4 Überprüftes Personal

Auf Verlangen des AG ist der AN verpflichtet, nur überprüftes Personal, wie geprüft von nationalen
Behörden, zum Umgang mit sensiblen Informationssystemen (operative Systeme, Netze, Programme, Datenbestände) einzusetzen (z.B. im Fall von Wirtschaftsprüfern), sowohl vor der Integration in das Netzwerk des AG als auch für die Wartung des sensiblen Informationssystems während der gesamten Betriebsphase.

Der AG behält sich vor, vom AN für Mitarbeiter oder sonstige von ihm im Rahmen der Leistungserbringung eingesetzten Personen, die in Kontakt mit Verschlusssachen gemäß §4 HmbSÜGG kommen, eine Sicherheitsüberprüfung zu verlangen oder zu veranlassen. Der AN weist dem AG eine erfolgreiche Sicherheitsüberprüfung nach dem HmbSÜGG oder in vergleichbarer Weise in Textform nach.

2.5 Verpflichtung Nachunternehmer

Der AN gewährleistet, dass seine in Bezug auf dieses Vertragsverhältnis eingesetzten Nachunternehmer ausdrücklich als Nachunternehmer identifiziert sind und stellt sicher, dass diese mindestens dasselbe Sicherheitsniveau wie der AN erreichen. Er stellt entsprechende Nachweise auf Anforderung des AG zur Verfügung.

2.6 Datenverarbeitung

Verarbeitet oder speichert der AN Daten des AG und der mit diesem gemäß §§ 15 ff. AktG verbundenen Unternehmen, so verpflichtet sich der AN sowohl regulatorische und gesetzliche Anforderungen als auch Anforderungen der Leistungsbeschreibung zu beachten und einzuhalten, insbesondere die Regelungen zur Datensicherung.

2.7 Rechtsräume Hosting

Der AN verpflichtet sich, sämtliche Länder, in denen Daten des AG gehostet bzw. Anwendungen betrieben werden, zum Zeitpunkt des Angebots zu benennen. Der AN sichert hiermit zu, dass die Daten die benannten Speicherorte nicht verlassen. Umzüge innerhalb der EU sind hiervon ausgenommen, müssen dem AG aber unverzüglich in Textform mitgeteilt werden.

2.8 Endgeräte

Sofern der AN eigene Endgeräte zur Erbringung der vereinbarten Dienstleistung einsetzt, verpflichtet er sich zur Einhaltung der nachstehend genannten Vorgaben des AG. Als Endgerät im Sinne dieser Regelung wird jedes IT-Endgerät des AN verstanden, dass an IT-Applikationen sowie IT-Infrastruktur des AG (kabelgebunden oder kabellos) angeschlossen oder zur Verarbeitung von Daten des AG eingesetzt wird.

- Nur vom AN aktiv verwaltete Geräte dürfen verwendet werden.
- Die Endgeräte müssen nach dem jeweils aktuellen Stand der Technik abgesichert sein.
- Der AN verpflichtet sich, den Verlust oder die Kompromittierung eines Endgerätes unverzüglich an die Verantwortlichen des AG zu melden und dieses umgehend zu deaktivieren bzw. zu sperren.
- Der Einsatz von Hacking-Tools ist untersagt, sofern dies nicht ausdrücklich zugelassen ist.
- Der AN ist dafür verantwortlich, dass keine Netzkopplung der Datennetze des AG und den mit diesem verbundenen Unternehmen mit anderen Datennetzen stattfindet.

2.9 Meldung von Sicherheitsvorfällen

Der AN verpflichtet sich, im Rahmen seines Auftrags den AG unverzüglich über die in 2.2.1 und 2.2.2 genannten Ansprechpartner – grundsätzlich binnen 24 Stunden nach Bekanntwerden – alle Sicherheitsvorfälle in Informationssystemen des AN die Auswirkungen auf Informationssysteme des AG haben oder die Auswirkungen auf seine unmittelbare oder mittelbare Leistungserbringung haben, zu melden. Die Meldung muss eine konkrete und detaillierte Sachverhaltsbeschreibung umfassen und muss Stellungnahmen zu folgenden Punkten beinhalten:

- Allgemeine Beschreibung des Vorfalls
- Betroffene Daten des AG
- Betroffene Systeme des AG
- Betroffene Kommunikationsverbindungen mit dem AG
- Klassifizierung des Schweregrades des Vorfalls beim AN

- Datum und Uhrzeit des Bekanntwerdens des Vorfalls
- Verwendeter Angriffsvektor und genutzte Schwachstellen
- Verursacher (z.B. fahrlässiger Mitarbeiter, Cybercrime/APT Gruppe, technische Störung)
- Ergriffene und geplante Maßnahmen zur Vorfallbehandlung
- Voraussichtlicher Abschluss der Vorfallbehandlung
- Meldepflichtigkeit des Vorfalls (z.B. an BSI, Datenschutzaufsicht)

Der AN unterstützt den AG bei der weiteren Sachverhaltsaufklärung und -behandlung. Sobald neue Informationen bekannt werden, sind diese unaufgefordert dem AG mitzuteilen.

2.10 Zugriffe

Ein direkter oder verdeckter Zugang zu den Informationssystemen (operative Systeme, Netze, Programme, Datenbestände) des AG und der mit diesem verbundenen Unternehmen ist dem AN nur dann gestattet, wenn er vom AG eine ausdrückliche, dokumentierte Zugriffsberechtigung erhalten hat; die Zugriffsberechtigung ist auf die eingesetzten und ausdrücklich zugelassenen Mitarbeiter des AN 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.

2.11 Betriebssicherheit

Der AG 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 des AG angeschlossenen Informationssysteme des AN in irgendeiner Weise die Betriebssicherheit bzw. das Betriebsverhalten des Netzes oder daran angeschlossener anderer Informationssysteme oder Software beeinträchtigt werden. Vorgenanntes gilt vorbehaltlich abweichender Regelungen zum Umgang mit personenbezogenen Daten im Auftragsverhältnis.

3 Bewertung des Reifegrads der Informationssicherheit beim AN

3.1 Informationen der Sicherheitsorganisation

Der AN hat dem AG auf Anforderung Informationen seiner Sicherheitsorganisation offenzulegen, auf deren Basis der AG 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 des Anwendungsbereiches (Scope) und der Erklärung der Anwendbarkeit (Statement of Applicability (SoA)) bzw. äquivalente Nachweise oder aktuelle Auditergebnisse im Anwendungsbereich der Leistung sein.

3.2 Sicherheitsmonitoring

Der AN stimmt zu, dass der AG oder ein nach HPA Sicherheitskriterien ausgewählter und beauftragter Dritter beim AN während der Laufzeit des Vertrages regelmäßige Sicherheitsbewertungen mit Schwachstellenerkennung in Bezug auf dessen Cybersicherheit durchführen und den AN bei Feststellungen zur Behebung der Abweichung kontaktieren darf. Der AN ergreift geeignete Maßnahmen zur Behandlung erkannter Schwachstellen.

3.3 Audit

Der AN stimmt zu, dass der AG oder ein anderer beauftragter Dritter im Auftrag des AG den AN während der Laufzeit des Vertrages in Bezug auf dessen Informationssicherheit auditieren darf. Die Prüfungen werden auf der Grundlage der von dem Auftragnehmer zur Verfügung gestellten Dokumentation durchgeführt. Der genaue Umfang, die Dauer und die Organisation werden z.B. anlassbezogen und einvernehmlich vereinbart. Zusätzlich muss der Auftragnehmer die Abweichungen von den vereinbarten Sicherheitsanforderungen dem AG melden.

3.4 Vertragsbeendigung

Der AN gewährleistet, dass sämtliche im Zusammenhang mit dem Auftragsverhältnis stehenden Daten an allen primären und sekundären Standorten des AN und seiner Nachunternehmer bei Beendigung des Vertrags unverzüglich an den AG zurückzugeben oder diese nach Vereinbarung sicher zu löschen und zu vernichten, so dass diese nicht wiederhergestellt werden können. Ausnahmen bestehen nur bei Daten, zu deren Aufbewahrung der AN gesetzlich verpflichtet ist oder dies vertraglich geregelt wurde. Der AN weist dies auf Verlangen des AG nach.

[i] **Anlage 1 Klassifikationshilfe für Vertraulichkeitsklassen**

Für die korrekte Einstufung von Informationen in die jeweiligen Vertraulichkeitsklassen ist das Wissen um den potenziellen Schaden bei unerwünschter Offenlegung oder Weitergabe an Dritte wichtig.

Vertraulich-keitsklasse dt./engl.	**Auswirkung (Gesamt-Risiko)**	**Schaden für das Unternehmen**
Streng vertraulich / Strictly confidential	Wesentlich bis bestandsgefährdend (hoch bis sehr hoch)	• Betroffen ist das gesamte Unternehmen • Gravierende rechtliche Konsequenzen bis hin zu Haftstrafen • Erheblicher Verlust von Ansehen und Vertrauen in der Öffentlichkeit und bei mehreren Kunden • Sehr negative Auswirkungen für die Geschäftszwecke und Ziele des Hauses • Personenbezogene Daten besonderer Kategorien nach Art. 9 DSGVO (z.B. Gesundheitsdaten) Schaden gegen Leib und Leben • Kritischer bis elementarer finanzieller Schaden
Vertraulich / Confidential	Relevant (mittel)	• Betroffen ist ein Geschäftsprozess • Rechtliche Konsequenzen bis hin zu Ordnungswidrigkeiten und Geldstrafen • Personenbezogene Daten gem. DSGVO • Verärgerung bei einzelnen Kunden und Imageverlust in der Öffentlichkeit • Schwerwiegender finanzieller Schaden
Intern / Internal	Akzeptabel (niedrig)	• Keine weit reichenden Konsequenzen für die Sparten • Geringe rechtliche Konsequenzen (Mahnungen) • Leichte Irritation in den Medien
Öffentlich / Public	Keine	Kein Schaden, da Information für Öffentlichkeit bestimmt