Verpflichtungserklärung betreffend Informationssicherheit, Datenschutz und Schutzrechte gegenüber den Unternehmen der TIWAG-Gruppe

1. Zweck, Anwendungsbereich und Rangfolge

Diese Verpflichtungserklärung regelt Mindestanforderungen an Vertraulichkeit, Datenschutz, Informations- und Cybersicherheit, Lieferkettensicherheit, Resilienz sowie den Umgang mit Schutzrechten im Zusammenhang mit Vergabeverfahren und Aufträgen von Unternehmen der TIWAG-Gruppe (nachfolgend „Auftraggeber“). Sie gilt für Bewerbende und Bietende ab Bereitstellung der Vergabeunterlagen sowie für Auftragnehmer ab Vertragsabschluss.

Der Auftragnehmer hat die Pflichten dieser Erklärung allen von ihm eingesetzten Personen und sicherheitsrelevanten Unterauftragnehmern vor deren Zugang zu Informationen, Standorten oder IT-/OT-Systemen des Auftraggebers mindestens in gleichwertiger und nachweisbarer Form zu überbinden.

Bei Widersprüchen gilt folgende Rangfolge: zwingendes Recht; individuell vereinbarter Hauptvertrag; Auftragsverarbeitungsvereinbarung; projektspezifischer Sicherheitsanhang; diese Verpflichtungserklärung. Strengere, widerspruchsfreie Anforderungen bleiben unberührt.

2. Rechtliche und normative Anforderungen

Der Auftragnehmer hält sämtliche auf ihn, die vereinbarte Leistung sowie die eingesetzten Produkte und Dienste anwendbaren gesetzlichen, regulatorischen, behördlichen und vertraglich vereinbarten Anforderungen an Informationssicherheit, Cybersicherheit, physische Sicherheit und Resilienz ein.

Hierzu zählen, soweit sachlich, persönlich und räumlich anwendbar, insbesondere:

- Netz- und Informationssystemsicherheitsgesetz 2026 (NISG 2026) einschließlich darauf beruhender Verordnungen;
- Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie);
- Durchführungsverordnung (EU) 2024/2690 für die von ihrem Anwendungsbereich erfassten Einrichtungen und Dienste;
- Verordnung (EU) 2024/2847 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (Cyber Resilience Act);
- Resilienz kritischer Einrichtungen-Gesetz (RKEG) einschließlich darauf beruhender Verordnungen;
- Delegierte Verordnung (EU) 2024/1366 zur Festlegung eines Netzkodex für Cybersicherheitsaspekte grenzüberschreitender Stromflüsse;
- ISO/IEC 27001 und ISO/IEC 27002 sowie bei energiewirtschaftlichen IT-/OT-Leistungen ISO/IEC 27019; ergänzend können ISO 22301 und IEC 62443 maßgeblich sein.

Die bloße Nennung einer Rechtsvorschrift oder Norm begründet keine Anwendung außerhalb ihres jeweiligen Anwendungsbereichs. Der Auftragnehmer prüft die Anwendbarkeit auf seine Leistung eigenverantwortlich und informiert den Auftraggeber unverzüglich über wesentliche daraus resultierende Pflichten oder Änderungen.

3. Begriffsbestimmungen

Vertrauliche Informationen: alle nicht öffentlich bekannten kaufmännischen, rechtlichen, technischen, organisatorischen oder sicherheitsbezogenen Informationen, unabhängig von Form und Kennzeichnung, deren Schutzbedürftigkeit sich aus Kennzeichnung, Inhalt oder Offenlegungsumständen ergibt.

Sicherheitsvorfall: ein Ereignis, das Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten, Systemen, Produkten oder Diensten beeinträchtigt oder beeinträchtigen kann.

Schwachstelle: eine Schwäche, Anfälligkeit oder Fehlfunktion eines IKT-Produkts oder IKT-Dienstes, die durch eine Bedrohung ausgenutzt werden kann.

Sicherheitsrelevanter Unterauftragnehmer: eine zur Leistungserbringung beigezogene Person oder Organisation, die Zugriff auf Informationen, Systeme, Räumlichkeiten oder Kontrollsysteme erhält oder wesentliche IT-, OT-, Cloud-, Hosting-, Telekommunikations-, Entwicklungs-, Wartungs- oder Sicherheitsleistungen erbringt.

Kenntnisnahme: der Zeitpunkt, zu dem hinreichende Tatsachen vorliegen, die mit angemessener Wahrscheinlichkeit auf einen Sicherheitsvorfall oder eine relevante Schwachstelle schließen lassen.

Produkt mit digitalen Elementen: ein Produkt, dessen bestimmungsgemäße oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische oder physische Datenverbindung zu einem Gerät oder Netz einschließt, soweit der Cyber Resilience Act anwendbar ist.

4. Pflichten im Vergabeverfahren

Bewerbende und Bietende verpflichten sich,

- die Teilnahme- und Ausschreibungsunterlagen sowie alle im Zusammenhang mit dem Vergabeverfahren bekanntwerdenden vertraulichen Informationen ausschließlich zur Erstellung und Einreichung des Teilnahmeantrags oder Angebots zu verwenden;
- Zugriff nur Personen zu gewähren, die ihn für das Vergabeverfahren benötigen und zuvor angemessen zur Geheimhaltung verpflichtet wurden;
- keine zusätzlichen oder vertraulichen Informationen außerhalb der vom Auftraggeber vorgesehenen Kommunikationswege zu beschaffen oder zu nutzen;
- Pressemitteilungen, Referenznennungen und sonstige Veröffentlichungen zum Vergabeverfahren nur nach vorheriger ausdrücklicher Freigabe des Auftraggebers vorzunehmen;
- Unterlagen nach Abschluss oder Abbruch des Verfahrens auf Aufforderung zurückzugeben oder sicher zu löschen, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen;
- auf Verlangen die zur Bewertung der Cybersecurity-Eignung erforderlichen Informationen und Nachweise bereitzustellen, insbesondere zur Sicherheitsorganisation, zu Zertifikaten oder Prüfberichten, zum Risiko-, Vorfall-, Schwachstellen- und Patchmanagement, zu sicheren Entwicklungsverfahren, sicherheitsrelevanten Unterauftragnehmern sowie zur Aufrechterhaltung und Wiederherstellung der angebotenen Leistung.

Unrichtige, unvollständige oder irreführende Angaben können nach Maßgabe der vergabe- und vertragsrechtlichen Bestimmungen zum Ausschluss oder zu vertraglichen Maßnahmen führen. Die vergaberechtlichen Grundsätze der Gleichbehandlung, Transparenz, Verhältnismäßigkeit und des lauteren Wettbewerbs sind einzuhalten.

5. Vertraulichkeit und Geschäftsgeheimnisse

Vertrauliche Informationen dürfen nur für den vereinbarten Zweck und nur im erforderlichen Umfang verarbeitet, vervielfältigt und zugänglich gemacht werden. Zugangsdaten, kryptografische Schlüssel, Sicherheitskonfigurationen, Netz- und Systemarchitekturen, Schwachstelleninformationen, personenbezogene Daten sowie Geschäfts- und Betriebsgeheimnisse gelten stets als vertraulich.

Ausgenommen sind Informationen, die der Empfänger nachweislich bereits rechtmäßig kannte, ohne Pflichtverletzung allgemein bekannt sind oder werden, von einem berechtigten Dritten rechtmäßig erlangt wurden oder unabhängig ohne Nutzung vertraulicher Informationen entwickelt wurden.

Ist eine Offenlegung gesetzlich oder aufgrund einer vollstreckbaren behördlichen oder gerichtlichen Anordnung erforderlich, ist der Auftraggeber, soweit rechtlich zulässig, vorab, sonst unverzüglich danach zu informieren. Die Offenlegung ist auf das rechtlich erforderliche Mindestmaß zu beschränken.

Die Geheimhaltungspflicht gilt während des Vertragsverhältnisses und fünf Jahre danach. Für Geschäftsgeheimnisse, personenbezogene Daten, Zugangsdaten und sicherheitskritische Informationen gilt sie so lange, wie deren vertraulicher oder schutzbedürftiger Charakter fortbesteht.

6. Datenschutz und Datengeheimnis

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich rechtmäßig, zweckgebunden, transparent und auf das erforderliche Maß beschränkt. Er gewährleistet Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Verarbeitungssysteme nach Art. 32 DSGVO und verpflichtet eingesetzte Personen auf das Datengeheimnis gemäß § 6 DSG, soweit keine gleichwertige gesetzliche Verpflichtung besteht.

Personenbezogene Daten dürfen nur auf dokumentierte Weisung des hierzu berechtigten Verantwortlichen verarbeitet oder übermittelt werden, sofern keine gesetzliche Verarbeitungspflicht besteht. Betroffene Personen sind nach den anwendbaren Datenschutzbestimmungen zu informieren.

Soweit der Auftragnehmer personenbezogene Daten im Auftrag verarbeitet, ist vor Verarbeitungsbeginn eine gesonderte Vereinbarung nach Art. 28 DSGVO abzuschließen. Diese Erklärung ersetzt eine solche Vereinbarung nicht. Drittlandübermittlungen und der Einsatz weiterer Auftragsverarbeiter sind nur im Rahmen der anwendbaren Vereinbarungen und gesetzlichen Voraussetzungen zulässig.

7. Personaleinsatz und Zuverlässigkeit

Der Auftragnehmer setzt ausschließlich fachlich geeignete, für die jeweilige Aufgabe unterwiesene und hinreichend zuverlässige Personen ein. Art und Umfang eigener Hintergrund- oder Strafregisterprüfungen müssen auf geeigneter Rechtsgrundlage beruhen sowie risikobasiert, verhältnismäßig und datensparsam sein. Eine pauschale Verarbeitung strafrechtlicher Daten wird nicht verlangt.

Soweit die Voraussetzungen des § 16 RKEG vorliegen und der Auftraggeber auf Grundlage seiner Risikoanalyse eine behördliche Zuverlässigkeitsüberprüfung begründet verlangt, stellt der Auftragnehmer die erforderliche Mitwirkung der betroffenen Personen sicher. Entscheidung, Ersuchen und Übermittlung an den Bundesminister für Inneres erfolgen durch den Auftraggeber als kritische Einrichtung über den vorgesehenen sicheren Kommunikationskanal.

Der Auftragnehmer informiert betroffene Personen rechtzeitig über Zweck, Rechtsgrundlage, Datenkategorien, Empfänger, Speicherdauer und Betroffenenrechte. Unterlagen für die behördliche Prüfung sind nur im erforderlichen Umfang und nicht länger als erforderlich aufzubewahren.

8. Schutzbedarf und Kritikalität

Die einzuhaltenden Sicherheitsanforderungen richten sich nach dem Schutzbedarf der Informationen, der Kritikalität der betroffenen Leistungen, Produkte, Systeme und Standorte sowie den möglichen Auswirkungen einer Beeinträchtigung auf den Auftraggeber.

Der Auftraggeber kann die Leistung insbesondere nach Daten- und Systemzugriff, Betriebsrelevanz, Abhängigkeit von Unterauftragnehmern, möglicher Auswirkung von Ausfall oder Manipulation sowie dem Einsatz von Produkten mit digitalen Elementen einstufen. Der Auftragnehmer stellt hierfür erforderliche Informationen vollständig, richtig und aktuell bereit und meldet wesentliche Änderungen der Leistung, Systemarchitektur, Lieferkette oder Risikolage unverzüglich.

9. Informations- und Cybersicherheit

Der Auftragnehmer setzt unter Berücksichtigung des Stands der Technik, anerkannter Normen und bewährter Verfahren sowie von Risiko, Größe, Kritikalität und Umsetzungskosten geeignete technische, operative und organisatorische Maßnahmen um. Bei IKT-Dienstleistungen sind die einschlägigen Kontrollen der ISO/IEC 27001 in Verbindung mit ISO/IEC 27002 oder gleichwertige Maßnahmen anzuwenden. Bei Leistungen der Energieversorgung, Prozessleit-, Automatisierungs-, Fernwirk-, Schutz-, Mess-, Steuerungs- oder OT-Technik sind zusätzlich ISO/IEC 27019 oder gleichwertige Maßnahmen zu berücksichtigen. Eine Zertifizierung ist nur geschuldet, wenn sie ausdrücklich vereinbart wurde.

Die Maßnahmen umfassen, soweit für die Leistung relevant, insbesondere:

- dokumentierte Risikoanalysen, Sicherheitskonzepte, Informationssicherheitsrichtlinien und klare Verantwortlichkeiten;
- Asset-, Identitäts- und Berechtigungsmanagement nach Need-to-know und Least-Privilege;
- personenbezogene Konten und Mehrfaktor-Authentisierung für Remote- und privilegierte Zugriffe, soweit technisch möglich;
- sichere Konfiguration, Systemhärtung sowie geregeltes Änderungs-, Patch- und Schwachstellenmanagement;
- Verschlüsselung vertraulicher Informationen bei Übertragung und risikoadäquat bei Speicherung sowie sichere Schlüsselverwaltung;
- Protokollierung, Zeitsynchronisierung und Überwachung sicherheitsrelevanter Aktivitäten sowie Schutz und angemessene Aufbewahrung der Protokolle;
- Malware-Schutz beziehungsweise EDR, Netzsegmentierung, insbesondere zwischen IT und OT, sowie kontrollierte Fernwartung;
- sichere Datensicherungen, getestete Wiederherstellung, Business-Continuity-, Krisen- und Wiederanlaufmaßnahmen;
- sichere Entwicklungs-, Test-, Freigabe- und Änderungsverfahren;
- sichere Löschung, Datenträgervernichtung und dokumentierter Exit bei Vertragsende.

Konkrete Mindestmaßnahmen, Nachweisformen und Schutzklassen werden bei Bedarf in einem projektspezifischen Sicherheitsanhang festgelegt.

10. Nutzung von IT-/OT- und Kommunikationsinfrastruktur

Zweckbindung

Der Zugriff auf Systeme und Netze des Auftraggebers ist nur im für den Auftrag erforderlichen Umfang, innerhalb freigegebener Zeitfenster und über genehmigte Zugangswege zulässig.

Konten und Zugangsdaten

Es sind personenbezogene Konten zu verwenden. Gemeinsame Konten bedürfen einer dokumentierten Ausnahme. Zugangsdaten dürfen nicht weitergegeben, ungeschützt gespeichert oder für andere Zwecke verwendet werden. Nicht mehr benötigte Zugänge sind unverzüglich zu sperren.

Hard- und Software

Installation, Anschluss oder Inbetriebnahme eigener Hard- oder Software in der Umgebung des Auftraggebers bedürfen der vorherigen Freigabe. Eingesetzte Systeme müssen aktuell, gehärtet, verschlüsselt und frei von bekannten kritischen Schwachstellen sowie Schadsoftware sein.

Remote-Zugriff

Remote-Zugriffe erfolgen ausschließlich über die vom Auftraggeber freigegebene Lösung, mit personenbezogenen Kennungen und grundsätzlich mit Mehrfaktor-Authentisierung. Berechtigungen sind auf die konkrete Tätigkeit und, soweit vorgesehen, zeitlich zu beschränken. Der Auftragnehmer akzeptiert sicherheitsbezogene Protokollierung und Session-Monitoring nach Maßgabe der bereitgestellten Datenschutzinformation und informiert die eingesetzten Personen vorab.

Vor-Ort-Arbeiten

Eigene Geräte dürfen vor Ort nur nach Freigabe angeschlossen werden. Wechselmedien sind auf das notwendige Maß zu beschränken und vor Nutzung sicherheitstechnisch zu prüfen.

Unberechtigter Zugang

Das Umgehen von Sicherheitsmaßnahmen, eigenmächtige Penetrationstests, Portscans oder Zugriffe außerhalb der Berechtigung sind untersagt. Ausnahmen bedürfen eines schriftlich definierten Testauftrags.

11. Schwachstellen und Sicherheitsvorfälle

Der Auftragnehmer meldet über den vom Auftraggeber festgelegten Meldeweg unverzüglich, spätestens innerhalb von zwölf Stunden nach Kenntnisnahme, jeden tatsächlichen oder hinreichend vermuteten Sicherheitsvorfall und jede relevante Schwachstelle, die Daten, Systeme, Produkte, Dienste, Zugangsdaten oder die Leistungserbringung für den Auftraggeber beeinträchtigt oder beeinträchtigen kann. Dies gilt auch für Ereignisse bei sicherheitsrelevanten Unterauftragnehmern und in der Lieferkette. Bereits ein begründeter Verdacht ist zu melden; die Meldung darf nicht bis zum Abschluss der Ursachenanalyse aufgeschoben werden.

Die Erstmeldung enthält, soweit verfügbar: Zeitpunkt der Kenntnisnahme, Art des Ereignisses, betroffene Leistungen, Systeme, Standorte und Informationen, mögliche Auswirkungen, bekannte oder vermutete Ursache, Ausnutzungshinweise, verfügbare Kompromittierungsindikatoren, bekannte Exploits, bereits gesetzte Maßnahmen und erreichbare Incident-Kontakte.

Fehlende Informationen sind unverzüglich nachzureichen. Spätestens innerhalb von 72 Stunden nach Kenntnisnahme ist eine qualifizierte Folgemeldung mit einer ersten Bewertung des Schweregrads, der Auswirkungen, der betroffenen Systeme sowie der getroffenen und geplanten Maßnahmen vorzulegen. Auf Verlangen sind Zwischenberichte und nach Abschluss ein Ursachen- und Abschlussbericht einschließlich Abhilfemaßnahmen zu übermitteln.

Der Auftragnehmer unterstützt den Auftraggeber bei gesetzlichen, regulatorischen, vertraglichen und behördlichen Meldepflichten, sichert relevante Protokolle und Beweismittel manipulationsgeschützt und unterlässt deren Löschung oder Veränderung, soweit keine gesetzlichen Pflichten entgegenstehen. Veröffentlichungen oder Meldungen im Namen des Auftraggebers bedürfen dessen Freigabe; eigene gesetzliche Meldepflichten bleiben unberührt.

12. Lieferkette und Unterauftragnehmer

Der Auftragnehmer ermittelt, bewertet, behandelt und überwacht die mit seiner Leistung verbundenen Risiken der Lieferkette über die gesamte Vertragslaufzeit. Dabei sind insbesondere Kritikalität, bekannte Schwachstellen, Cybersicherheitspraxis, sichere Entwicklungs-, Herstellungs-, Wartungs- und Bereitstellungsprozesse, Abhängigkeiten von einzelnen Bezugsquellen sowie die Wiederherstellbarkeit bei Ausfall eines Zulieferers zu berücksichtigen.

Sicherheitsrelevante Unterauftragnehmer dürfen nur entsprechend dem Hauptvertrag und den einschlägigen Datenschutzvereinbarungen eingesetzt werden. Der Auftragnehmer überbindet die für die Leistung relevanten Pflichten mindestens gleichwertig, überwacht deren Einhaltung und bleibt für die Vertragserfüllung verantwortlich.

Beabsichtigte wesentliche Änderungen der Lieferkette, der Leistungserbringungsorte oder sicherheitsrelevanter Unterauftragnehmer sind dem Auftraggeber vorab mitzuteilen, soweit dies vertraglich vorgesehen oder für die Risikobewertung erheblich ist. Entstehen wesentliche zusätzliche Risiken, kann der Auftraggeber angemessene Sicherheitsmaßnahmen verlangen oder der Änderung aus sachlich gerechtfertigten Sicherheitsgründen widersprechen.

13. Sichere Produkt- und Softwarelieferung

Soweit Hard-, Soft- oder Firmware geliefert, entwickelt oder gewartet wird, gewährleistet der Auftragnehmer risikoadäquate sichere Entwicklungs-, Build-, Test-, Freigabe-, Änderungs- und Updateprozesse. Er schützt Quellcode, Build-Systeme, Artefakte, Signatur- und Updateinfrastrukturen angemessen und dokumentiert sicherheitsrelevante Änderungen nachvollziehbar.

- Sicherheitsupdates und Patches sind authentisch, integritätsgeschützt und über definierte Wege bereitzustellen;
- kritische oder hohe Sicherheitsmängel sind vor Produktivsetzung zu beheben oder im Einvernehmen mit dem Auftraggeber durch dokumentierte Ersatzmaßnahmen zu behandeln;
- kritische Schwachstellen und kompromittierte Signatur-, Build- oder Updateinfrastrukturen sind unverzüglich zu melden;
- auf Anforderung sind angemessene Komponenten- und Abhängigkeitsinformationen, vorzugsweise in maschinenlesbarer Form, sowie Nachweise über die Schwachstellenbehandlung bereitzustellen.

Anforderungen des Cyber Resilience Act

Soweit der Auftragnehmer Produkte mit digitalen Elementen bereitstellt und die Verordnung (EU) 2024/2847 anwendbar ist, erfüllt er die auf seine Rolle als Hersteller, Bevollmächtigter, Importeur oder Händler anwendbaren Pflichten. Auf Verlangen stellt er insbesondere EU-Konformitätserklärung, Angaben zur CE-Kennzeichnung, Sicherheits- und Nutzungshinweise, den vorgesehenen Supportzeitraum, Informationen zu Sicherheitsupdates, Schwachstellen-Meldewege sowie Angaben zu wesentlichen Komponenten und Abhängigkeiten bereit.

Der Auftragnehmer informiert den Auftraggeber rechtzeitig über End-of-Support, Einstellung eines Produkts oder einer Produktlinie, wesentliche Einschränkungen der Update- oder Wartungsfähigkeit, aktiv ausgenutzte Schwachstellen und Änderungen des Hersteller- oder Supportmodells, soweit diese Sicherheit oder Verfügbarkeit beeinflussen können.

14. Business Continuity, Wiederherstellung und Krisenmanagement

Soweit die Leistung für die Aufrechterhaltung des Betriebs relevant ist, trifft der Auftragnehmer dokumentierte und regelmäßig überprüfte Maßnahmen zur Aufrechterhaltung und Wiederherstellung seiner Leistung. Zu berücksichtigen sind insbesondere Ausfälle von Personal, Standorten, Systemen, Kommunikationsverbindungen, kritischen Herstellern oder Unterauftragnehmern, Cyberangriffe, Datenverlust sowie die Verfügbarkeit erforderlicher Ersatzteile, Lizenzen, Schlüssel und Dokumentationen.

Die Wirksamkeit der Wiederherstellungs- und Notfallmaßnahmen ist nach wesentlichen Änderungen und regelmäßig zu testen. Die für die vereinbarte Leistung relevanten Ergebnisse sind dem Auftraggeber auf Verlangen nachzuweisen.

15. Network Code on Cybersecurity

Soweit die Leistung in den sachlichen Anwendungsbereich der Delegierten Verordnung (EU) 2024/1366 fällt oder für Prozesse und Systeme relevant ist, die der Auftraggeber aufgrund dieser Verordnung schützen muss, unterstützt der Auftragnehmer den Auftraggeber angemessen. Dies umfasst, soweit vertraglich konkretisiert, Informationen für Cyberrisikobewertungen, Umsetzung sektorspezifischer Mindestanforderungen, Monitoring, Berichterstattung, Krisenmanagement, Sicherheitsprüfungen und Übungen, Nachweise zur Sicherheit von Produkten und Diensten sowie Behandlung von Lieferkettenrisiken.

16. Rückgabe, Löschung und Exit

Nach Zweckfortfall oder Vertragsende sind Informationen, Unterlagen, Datenträger, Verarbeitungsergebnisse, Konten, Zugangsberechtigungen, Konfigurationen, Dokumentationen, Schlüssel und sonstige für Betrieb oder Fortführung erforderliche Elemente nach Weisung des Auftraggebers zurückzugeben, zu entziehen, zu löschen oder sicher zu vernichten.

Gesetzlich aufzubewahrende Daten sind auf den erforderlichen Mindestumfang zu beschränken, gegen unzulässige Nutzung zu sperren, weiterhin angemessen zu schützen und nach Ablauf der Aufbewahrungsfrist unverzüglich zu löschen. Die Löschung hat Arbeitskopien und kontrollierbare Sicherungskopien zu erfassen. Technisch nicht sofort löschbare Backup-Daten dürfen bis zur turnusmäßigen Überschreibung isoliert bleiben und nicht produktiv verarbeitet werden.

Der Auftragnehmer bestätigt Rückgabe, Löschung oder Vernichtung auf Verlangen in geeigneter Form und berücksichtigt dabei sicherheitsrelevante Unterauftragnehmer. Nach Vertragsende bekanntwerdende Schwachstellen oder Sicherheitsvorfälle mit möglichen Auswirkungen auf gelieferte Produkte oder erbrachte Leistungen sind weiterhin unverzüglich zu melden.

17. Nachweise, Kontrollen und Audits

Der Auftragnehmer weist die Einhaltung dieser Pflichten auf angemessene Anforderung durch geeignete Unterlagen nach, insbesondere durch Richtlinien, Zertifikate, unabhängige Prüfberichte, Selbstauskünfte, Sicherheitskonzepte, Risikoanalysen, Maßnahmenpläne sowie Nachweise über Schwachstellen-, Notfall- oder Wiederherstellungstests.

Bei erhöhtem Risiko, begründetem Verdacht, wesentlichen Änderungen oder Sicherheitsvorfällen kann der Auftraggeber risikoadäquate Kontrollen oder Audits selbst oder durch zur Vertraulichkeit verpflichtete Dritte durchführen. Kontrollen sind grundsätzlich anzukündigen, auf den Vertragsgegenstand zu beschränken und unter angemessener Berücksichtigung von Geschäftsgeheimnissen, Datenschutz und Betriebsablauf durchzuführen. Anlassbezogene Prüfungen dürfen mit kürzerer Ankündigung erfolgen, soweit dies zur Risikobegrenzung erforderlich ist.

Festgestellte Abweichungen sind innerhalb einer risikogerechten Frist zu beheben und die Behebung ist nachzuweisen. Kritische Risiken sind unverzüglich zu behandeln. Der Auftragnehmer informiert unverzüglich über Aussetzung, Einschränkung oder Entzug vereinbarter Zertifikate sowie wesentliche Abweichungen in einschlägigen Prüfberichten. Gesetzliche und behördliche Prüfungsrechte bleiben unberührt.

18. Schutz- und Nutzungsrechte

An Vergabe- und Vertragsunterlagen können Urheberrechte, Datenbankrechte, Geschäftsgeheimnisse und sonstige Schutzrechte bestehen. Die Unterlagen dürfen ausschließlich zur Teilnahme am jeweiligen Vergabeverfahren oder zur vertragsgemäßen Leistungserbringung genutzt und nur den hierfür erforderlichen Personen zugänglich gemacht werden.

Nutzungsrechte an Arbeitsergebnissen richten sich nach dem jeweiligen Vertrag. Gesetzlich zwingende Rechte, zulässige Sicherungskopien und erforderliche Nutzungen bleiben unberührt.

19. Haftung und Rechtsfolgen

Der Auftragnehmer haftet nach den gesetzlichen Bestimmungen für schuldhafte Verstöße gegen diese Erklärung. Zulässige Haftungsbeschränkungen des Hauptvertrags bleiben anwendbar, soweit dort nicht ausdrücklich etwas anderes bestimmt ist.

Der Auftragnehmer hält den Auftraggeber von berechtigten Ansprüchen Dritter frei, soweit diese unmittelbar auf einem vom Auftragnehmer oder seinen Erfüllungsgehilfen zu vertretender Verstoß beruhen. Der Auftraggeber informiert den Auftragnehmer unverzüglich und ermöglicht eine angemessene Beteiligung an der Rechtsverteidigung. Eigene Verursachungsbeiträge des Auftraggebers sind zu berücksichtigen.

Wesentliche Verstöße können Maßnahmen zur Risikobegrenzung, Sperre von Zugängen, Austausch eingesetzter Personen und, bei Vorliegen der vertraglichen oder gesetzlichen Voraussetzungen, außerordentliche Vertragsbeendigung nach sich ziehen.

20. Schlussbestimmungen

Änderungen und Ergänzungen bedürfen der Schriftform, soweit nicht gesetzlich eine strengere Form vorgeschrieben ist. Operative Ansprechpartner, Meldewege und technische Anlagen können in dokumentierter elektronischer Form aktualisiert werden. Individuelle Vereinbarungen bleiben unberührt.

Ändern sich während der Vertragslaufzeit gesetzliche oder regulatorische Anforderungen, die auf die vereinbarte Leistung anwendbar sind, informieren sich die Vertragsparteien über wesentliche Auswirkungen. Notwendige Anpassungen der Sicherheitsmaßnahmen sind risikobasiert und unter Berücksichtigung gesetzlicher Umsetzungsfristen abzustimmen.

Sollte eine Bestimmung unwirksam oder undurchführbar sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. An ihre Stelle tritt keine automatische geltungserhaltende Reduktion, sondern die gesetzliche Regelung; die Parteien werden eine rechtlich zulässige, dem Zweck möglichst nahekommende Vereinbarung treffen.

Es gilt österreichisches Recht unter Ausschluss seiner Verweisungsnormen. Soweit gesetzlich zulässig, wird die ausschließliche Zuständigkeit des sachlich zuständigen Gerichts in Innsbruck vereinbart.