VERPFLICHTUNGSERKLÄRUNG

des Auftragnehmers zu Informationssicherheit, Cyberresilienz, physischer Resilienz und Lieferkettensicherheit

Präambel

Der Auftragnehmer erbringt für den Auftraggeber Leistungen. enercity AG, enercity Netz GmbH sowie weitere Unternehmen der enercity-Gruppe unterliegen – abhängig von ihrer jeweiligen Tätigkeit und gesetzlichen Einordnung – besonderen Anforderungen insbesondere an Informationssicherheit, Cyberresilienz, Datenschutz, physische Resilienz und Lieferkettensicherheit. Die sichere und rechtskonforme Leistungserbringung durch Auftragnehmer ist für die Erfüllung dieser Anforderungen von wesentlicher Bedeutung.. Im Hinblick darauf verpflichtet sich der Auftragnehmer nachfolgend zur Einhaltung der einschlägigen Vorgaben.

Diese Verpflichtungserklärung wird Bestandteil des jeweiligen Hauptvertrags, soweit sie dort einbezogen wird.

Die jeweilige Verpflichtung trifft den Auftragnehmer nur insoweit, als sie auf die konkrete, vertraglich geschuldete Leistungserbringung Anwendung findet.

§ 1 Geltungsbereich und Anwendbarkeit

(1) Diese Verpflichtungserklärung gilt für alle Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, soweit dabei gesetzliche Vorgaben in den Bereichen Informationssicherheit, Datenschutz, Lieferkettenverantwortung oder kritischer Infrastrukturen berührt werden.

(2) Die nachfolgenden Verpflichtungen gelten jeweils nur, soweit die jeweiligen gesetzlichen Vorgaben auf den Auftragnehmer und die von ihm erbrachten Leistungen Anwendung finden. Der Auftragnehmer hat dem Auftraggeber auf Verlangen in nachvollziehbarer und dokumentierter Form mitzuteilen, welche der nachfolgenden Anforderungen auf ihn und seine Leistungen Anwendung finden. Die eigenständige rechtliche Bewertung des Auftraggebers bleibt unberührt.

(3) Der Auftragnehmer weist die Einhaltung der Anforderungen auf Wunsch des Auftraggebers durch Vorlage gültiger Zertifikate, Auditberichte oder gleichwertiger Nachweise nach.

§ 2 IT-Sicherheit

(1) Der Auftragnehmer implementiert, dokumentiert, unterhält und überprüft für die Dauer der Leistungserbringung angemessene und wirksame technische und organisatorische Sicherheitsmaßnahmen. Die Maßnahmen müssen dem Stand der Technik, dem mit der Leistung verbundenen Risiko, den einschlägigen gesetzlichen und behördlichen Anforderungen sowie den im Hauptvertrag vereinbarten Sicherheitsanforderungen entsprechen.

(2) Der Auftragnehmer stellt insbesondere sicher, dass Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der von der Leistung betroffenen Systeme,

Komponenten und Daten angemessen geschützt werden. Soweit einschlägig, berücksichtigt er insbesondere die Anforderungen des BSIG, des EnWG, der DSGVO, der IT-Sicherheitskataloge der Bundesnetzagentur sowie anerkannter Standards der Informationssicherheit.

(3) Soweit der Auftragnehmer Lieferungen oder Leistungen in Bezug auf von dem Auftraggeber genutzte oder betriebene kritische Infrastrukturen erbringt, verpflichtet sich der Auftragnehmer zur Einhaltung aller anwendbarer gesetzlicher, behördlicher oder sonstiger regulatorischer Anforderungen, insbesondere der NIS-2 Richtlinie (EU) 2022/2555 und der einschlägigen nationalen Umsetzungsgesetze. Dies umfasst insbesondere die Unterstützung des Auftraggebers bei der Umsetzung gesetzlicher Nachweis-, Prüf- und Meldepflichten gegenüber zuständigen Behörden sowie die Einhaltung einschlägiger Sicherheitsstandards nach dem Stand der Technik und branchenspezifischen Sicherheitsstandards.

(4) Soweit die Leistungen Produkte mit digitalen Elementen im Sinne der Verordnung (EU) 2024/2847 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen („Cyberresilienz-Verordnung“) umfassen, erfüllt der Auftragnehmer die für ihn jeweils sachlich und zeitlich anwendbaren Anforderungen dieser Verordnung.

(5) Soweit Art, Umfang und Kritikalität der Leistung dies erfordern, betreibt der Auftragnehmer ein dokumentiertes und wirksam implementiertes Informationssicherheitsmanagementsystem, das sich an ISO/IEC 27001 oder einem gleichwertigen anerkannten Standard orientiert. Bei Cloud-Diensten sind, soweit einschlägig, zusätzlich ISO/IEC 27017 und bei der Verarbeitung personenbezogener Daten ISO/IEC 27018 oder jeweils gleichwertige Standards zu berücksichtigen. Der Auftragnehmer unterhält angemessene Notfallvorsorge- und Wiederanlaufprozesse. Soweit die Leistung für die Aufrechterhaltung kritischer Geschäftsprozesse oder kritischer Dienstleistungen wesentlich ist, vereinbaren die Parteien konkrete Wiederanlaufzeiten, Wiederherstellungspunkte und Testanforderungen. Der Auftragnehmer betreibt ein Business Continuity Management (BCM) nach den Anforderungen des KRITIS-Dachgesetzes.

(6) Der Auftragnehmer meldet dem Auftraggeber Sicherheitsvorfälle unverzüglich, spätestens innerhalb von 6 Stunden nach Kenntniserlangung, und stellt innerhalb von 24 Stunden einen Erstbericht, innerhalb von 72 Stunden einen vorläufigen Untersuchungsbericht sowie innerhalb von 30 Kalendertagen einen vollständigen forensischen Abschlussbericht einschließlich Ursachenanalyse, Auswirkungen, Nachweisen und Abstellmaßnahmen zur Verfügung. Der Auftragnehmer unterstützt den Auftraggeber hierbei uneingeschränkt bei der Erfüllung gesetzlicher Melde-, Nachweis- und Auskunftspflichten gegenüber Behörden, insbesondere dem BSI und der Bundesnetzagentur.

(7) Soweit die Leistungen Anlagen, Systeme oder Prozesse betreffen, die energiewirtschaftlichen Sicherheitsanforderungen unterliegen, erfüllt der Auftragnehmer die für seine Leistungen einschlägigen Anforderungen des EnWG, der auf dessen Grundlage erlassenen Regelungen und der jeweils anwendbaren IT-Sicherheitskataloge der Bundesnetzagentur. Technische Anschlussbedingungen, VDE-Anwendungsregeln und sonstige technische Regelwerke sind einzuhalten, soweit sie auf den konkreten Leistungsgegenstand Anwendung finden oder im Hauptvertrag vereinbart sind. Soweit Komponenten, Hersteller oder Unterauftragnehmer erhöhten geopolitischen, regulatorischen oder sicherheitsbezogenen Risiken unterliegen, führt der Auftragnehmer eine dokumentierte, risikobasierte Vertrauenswürdigkeitsprüfung nach den mit dem Auftraggeber abgestimmten Kriterien durch.

§ 3 Regulatorische Konformität

(1) Der Auftragnehmer konzipiert und erbringt seine Leistungen so, dass sie beim vertraglich vorausgesetzten Einsatz durch den Auftraggeber die Einhaltung der auf den Leistungsgegenstand anwendbaren gesetzlichen und regulatorischen Anforderungen ermöglichen. Dies gilt insbesondere für Anforderungen aus Datenschutzrecht, Datenrecht, KI-Regulierung, Produktsicherheitsrecht, Cybersicherheitsrecht und Energierecht, soweit diese nach Leistungsgegenstand und Rollenverteilung einschlägig sind. Der Auftragnehmer informiert den Auftraggeber rechtzeitig über regulatorisch relevante Eigenschaften, Einschränkungen und erforderliche Mitwirkungshandlungen.

(2) Soweit der Weitervertrieb oder die Bereitstellung der Leistungen an Kunden des Auftraggebers im Hauptvertrag vorgesehen oder für den Auftragnehmer erkennbar ist, stellt der Auftragnehmer dem Auftraggeber rechtzeitig alle Informationen, Dokumentationen, Nachweise, Aktualisierungen und Unterstützungsleistungen zur Verfügung, die der Auftraggeber zur Erfüllung seiner gesetzlichen Pflichten gegenüber seinen Kunden benötigt. Bei digitalen Produkten umfasst dies, soweit einschlägig, insbesondere die Unterstützung bei Informations- und Aktualisierungspflichten nach §§ 327 ff. BGB.

§ 4 Physische Resilienz und KRITIS-Dachgesetz

(1) Soweit der Auftragnehmer selbst Betreiber kritischer Anlagen im Sinne des KRITIS-Dachgesetzes ist, erfüllt er die für ihn geltenden Registrierungs-, Risikoanalyse-, Resilienz-, Nachweis- und Meldepflichten. Auf Verlangen weist er dem Auftraggeber seinen Registrierungsstatus sowie die Erfüllung der für die Leistungen relevanten Anforderungen in geeigneter Form nach.

(2) Soweit die Leistungen die physische Resilienz kritischer Anlagen des Auftraggebers berühren, unterstützt der Auftragnehmer insbesondere Maßnahmen zur Prävention, zum physischen Schutz, zur Reaktion, zur Schadensbegrenzung, zur Wiederherstellung und zur Aufrechterhaltung kritischer Dienstleistungen.

§ 5 Lieferungen und Lieferkettensicherheit

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung seiner gesetzlichen Pflichten und stellt sicher, dass Produkte und Leistungen den daraus folgenden Anforderungen an die Sicherheit der Lieferkette genügen. Er stellt durch geeignete vertragliche Vereinbarungen und Kontrollen sicher, dass von ihm eingesetzte Hersteller und Unterlieferanten die für die Vertragsprodukte relevanten Sicherheitsanforderungen erfüllen. Für deren Handeln und Unterlassen haftet der Auftragnehmer nach Maßgabe des Hauptvertrags und der gesetzlichen Vorschriften.

(2) Der Auftragnehmer stellt sicher, dass Vertragsprodukte nach anerkannten Prinzipien sicherer Produktentwicklung, insbesondere „Security by Design“, „Security by Default“ und dem Prinzip der geringsten Berechtigung, entwickelt, hergestellt, konfiguriert und ausgeliefert werden. Hard- und Firmware müssen gegen unbefugte Veränderungen angemessen geschützt sein. Versteckte, nicht dokumentierte oder vom Auftraggeber nicht freigegebene Zugänge sind unzulässig.

(3) Der Auftragnehmer unterhält ein dokumentiertes Schwachstellenmanagement und ein Verfahren zur koordinierten Offenlegung von Schwachstellen. Sicherheitsupdates und sicherheitsrelevante Fehlerbehebungen sind für den im Hauptvertrag festgelegten Unterstützungszeitraum bereitzustellen. Der Auftragnehmer teilt dem Auftraggeber spätestens bei Vertragsschluss das Enddatum des Sicherheits- und Produktsupports mit.

Auf Verlangen übergibt er eine Software-Stückliste (SBOM) und richtet ein Verfahren zur koordinierten Schwachstellenoffenlegung (Coordinated Vulnerability Disclosure) ein.

(4) Für Sicherheitsvorfälle, Schwachstellen und Kompromittierungen von Vertragsprodukten oder deren Lieferkette gelten die Melde- und Mitwirkungspflichten nach § 2 entsprechend.

(5) Soweit Vertragsprodukte als kritische Komponenten nach den jeweils geltenden gesetzlichen Bestimmungen einzustufen sind, stellt der Auftragnehmer die gesetzlich oder behördlich erforderlichen Erklärungen, Nachweise und Informationen rechtzeitig bereit und wirkt an erforderlichen Vertrauenswürdigkeitsprüfungen mit.

(6) Der Hersteller ist verpflichtet, dem Auftraggeber oder von diesem beauftragten, zur Verschwiegenheit verpflichteten, fachkundigen Dritten Einblick in sicherheitskritische Bestandteile der Software zu gewähren, soweit dies nachweislich zur Prüfung der sicherheitsrelevanten Anforderungen erforderlich ist. Der Source-Code-Zugriff erfolgt ausschließlich in dem zur Prüfung erforderlichen Umfang („Need-to-know-Prinzip“), unter Wahrung von Geschäfts- und Betriebsgeheimnissen und in einer kontrollierten Umgebung (z. B. vor Ort, Read-only, ohne Weitergabe des Codes).

(7) Auftragnehmer und Hersteller geben die vorstehenden Pflichten an etwaige Unterlieferanten weiter.

§ 6 Aktualisierung und Anpassung an Rechtsänderungen

(1) Der Auftragnehmer überprüft die für seine Leistungen geltenden Sicherheitsmaßnahmen regelmäßig und passt sie an Änderungen des Stands der Technik sowie an zwingende gesetzliche oder behördliche Anforderungen an. Er informiert den Auftraggeber unverzüglich über Änderungen, die Auswirkungen auf Sicherheit, Leistung, Kosten, Termine oder die regulatorische Nutzbarkeit der Leistungen haben können.

(2) Soweit Anpassungen über die bei Vertragsschluss geschuldete Leistung hinausgehen, stimmen die Parteien deren Umsetzung, Zeitplan und etwaige Mehrkosten nach dem im Hauptvertrag vorgesehenen Änderungsverfahren ab. Zwingend erforderliche Maßnahmen zur Beseitigung einer vom Auftragnehmer zu vertretenden Vertrags- oder Rechtswidrigkeit erfolgen ohne Mehrkosten für den Auftraggeber.

§ 7 Personeneinsatz und Unterauftragnehmer

(1) Bei Tätigkeiten an Standorten oder Anlagen des Auftraggebers beachten Auftragnehmer und Hersteller dessen Zutritts-, Sicherheits- und Geheimhaltungsvorgaben. Der Auftragnehmer setzt nur fachlich geeignete, angemessen geschulte und, soweit nach Art der Tätigkeit erforderlich und rechtlich zulässig, überprüfte Personen ein. Sicherheits- und Geheimhaltungsvorgaben des Auftraggebers sind vor Tätigkeitsaufnahme zu vermitteln und zu dokumentieren.

(2) Der Auftragnehmer verpflichtet seine Unterauftragnehmer zu denjenigen Sicherheits-, Nachweis-, Mitwirkungs- und Meldepflichten, die für deren jeweilige Leistung sachlich einschlägig sind und den Verpflichtungen des Auftragnehmers gegenüber dem Auftraggeber mindestens gleichwertigen Schutz gewährleisten. Der Auftragnehmer bleibt für die ordnungsgemäße Leistungserbringung seiner Unterauftragnehmer verantwortlich. Er stellt sicher, dass erforderliche Nachweise und Prüfungen auch hinsichtlich der von Unterauftragnehmern erbrachten Leistungen ermöglicht werden. Bei erheblichen Sicherheitsbedenken kann der Auftraggeber verlangen, dass der Auftragnehmer geeignete Abhilfemaßnahmen ergreift; soweit diese nicht ausreichen,

kann der Auftraggeber aus wichtigem Grund den weiteren Einsatz des betreffenden Unterauftragnehmers untersagen.

§ 8 Zusammenarbeit und Auditrechte

(1) Der Auftraggeber ist berechtigt, die Einhaltung dieser Verpflichtungserklärung risikobasiert und in angemessenem Umfang selbst oder durch unabhängige, zur Verschwiegenheit verpflichtete Dritte zu überprüfen. Regelmäßige Prüfungen sind mit angemessener Frist anzukündigen und während der üblichen Geschäftszeiten durchzuführen. Anlassbezogene Prüfungen dürfen bei konkreten Anhaltspunkten für erhebliche Pflichtverletzungen oder Sicherheitsrisiken auch kurzfristiger erfolgen.

(2) Der Auftragnehmer kann zunächst geeignete aktuelle Zertifikate, Auditberichte oder sonstige gleichwertige Nachweise vorlegen. Soweit diese zur Prüfung nicht ausreichen, gewährt er Zugang zu den erforderlichen Informationen, Unterlagen, Räumlichkeiten und Systemen. Prüfungen sind so durchzuführen, dass Betriebsabläufe und berechtigte Geheimhaltungsinteressen des Auftragnehmers möglichst wenig beeinträchtigt werden.

(3) Jede Partei trägt grundsätzlich ihre eigenen Prüfungskosten. Bei festgestellten erheblichen Pflichtverletzungen trägt der Auftragnehmer die angemessenen Kosten einer erforderlichen Nachprüfung. Festgestellte Mängel sind innerhalb einer vom Auftraggeber unter Berücksichtigung ihrer Kritikalität gesetzten Frist zu beseitigen.

(4) Im Fall von Prüfungen, Auskunftsverlangen oder sonstigen Maßnahmen zuständiger Behörden, insbesondere des Bundesamts für Sicherheit in der Informationstechnik oder des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe, unterstützt der Auftragnehmer den Auftraggeber unverzüglich und in angemessenem Umfang, soweit die Maßnahme die Leistungen oder den Verantwortungsbereich des Auftragnehmers betrifft.

§ 9 Geltung

(1) Diese Verpflichtungserklärung gilt für die Dauer des Hauptvertrags. Verpflichtungen, die nach ihrem Sinn und Zweck über die Vertragsbeendigung hinaus fortgelten müssen, insbesondere Geheimhaltungs-, Nachweis-, Mitwirkungs-, Lösch-, Rückgabe-, Sicherheitsupdate- und Vorfallmeldepflichten, gelten für den jeweils vereinbarten oder gesetzlich erforderlichen Zeitraum fort.

(2) Sollten einzelne Bestimmungen dieser Verpflichtungserklärung ganz oder teilweise unwirksam oder undurchführbar sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung treten die gesetzlichen Regelungen.

§ 10 Maßnahmen bei Pflichtverletzungen

(1) Erkennt der Auftragnehmer eine Verletzung dieser Verpflichtungserklärung oder ein erhebliches Sicherheitsrisiko, informiert er den Auftraggeber unverzüglich und legt einen Maßnahmen- und Zeitplan zur Abhilfe vor.

(2) Der Auftraggeber kann unter Berücksichtigung der Schwere und Dringlichkeit insbesondere angemessene Abhilfemaßnahmen, zusätzliche Nachweise, eine Nachprüfung, die vorübergehende Aussetzung betroffener Leistungen oder den Austausch gefährdeter Komponenten verlangen. Gesetzliche und vertragliche Rechte des Auftraggebers, insbesondere Schadensersatz-, Minderungs-, Rücktritts- und Kündigungsrechte, bleiben unberührt.