VERPFLICHTUNGSERKLÄRUNG

über die Einhaltung gesetzlicher Vorgaben durch den Auftragnehmer

Präambel
Der Auftragnehmer erbringt für den Auftraggeber Leistungen. enercity AG, enercity Netz GmbH und die mit ihnen i. S. v. § 15 AktG verbundenen Unternehmen sind ,,Betreiber kritischer Infrastrukturen" und unterliegen besonderen gesetzlichen Verpflichtungen. Im Hinblick auf die zunehmende Bedeutung der Einhaltung gesetzlicher Vorschriften in den Bereichen Informationssicherheit, Datenschutz und kritischer Infrastrukturen verpflichtet sich der Auftragnehmer nachfolgend zur Einhaltung der einschlägigen Vorgaben, soweit diese auf die erbrachten Leistungen Anwendung finden.
Diese Verpflichtungserklärung wird wesentlicher Bestandteil eines jeden Auftrags.

§ 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 erklärt sich bereit, dem Auftraggeber auf Verlangen Auskunft darüber zu geben, welche der nachfolgenden Verpflichtungen auf ihn zutreffen.

§ 2 IT-Sicherheit
(1) Der Auftragnehmer wird für die Dauer seiner Leistungserbringung für den jeweiligen Vertragszweck geeignete und angemessene technische und organisatorischen Maßnahmen implementieren, vorhalten und fortlaufend verbessern. Diese Maßnahmen müssen mindestens den anwendbaren gesetzlichen, behördlichen oder sonstigen regulatorischen Anforderungen, z. B. gemäß der NIS-2 Richtlinie (EU) 2022/2555 und den nationalen Umsetzungsgesetzen, den für kritische Infrastrukturen anwendbaren Gesetzen, der DSGVO sowie anerkannten Standards der Informationssicherheit entsprechen, insbesondere dem BSI IT-Grundschutz oder diesem gleichwertige Anforderungen. Die Maßnahmen sind so auszugestalten, dass Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der Systeme und Daten jederzeit gewährleistet sind.
(2) Der Auftragnehmer betreibt für die Bereitstellung der Lieferungen und Leistungen für die Dauer der Leistungserbringung ein geeignetes, dokumentiertes und wirksam implementiertes Sicherheitskonzept und ein Informationssicherheits-Managementsystem (ISMS) jeweils gemäß ISO 27001 einschließlich eines Notfall-Managements. Im Fall der Bereitstellung von Cloud-Diensten muss das Sicherheitskonzept außerdem den Anforderungen gemäß ISO 27017 genügen, im Fall der Verarbeitung personenbezogener Daten ferner den Anforderungen gemäß ISO 27018. Der Auftragnehmer weist die Einhaltung der Anforderungen auf Wunsch des Auftraggebers durch Vorlage gültiger Zertifikate, Auditberichte gemäß SOC 2 Typ II oder gleichwertiger Nachweise nach.
(3) Der Auftragnehmer verpflichtet sich, Sicherheitsvorfälle, welche die Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von Systemen, Komponenten oder Daten des Auftraggebers betreffen oder betreffen können, unverzüglich zu erkennen, zu bewerten und zu behandeln. Er informiert den Auftraggeber über jeden solchen Sicherheitsvorfall unverzüglich, spätestens jedoch innerhalb von 6 Stunden nach Kenntniserlangung, sofern dieser die Leistungserbringung beeinträchtigt oder beeinträchtigen kann, Auswirkungen auf Systeme oder Daten des Auftraggebers hat oder haben kann oder potenziell meldepflichtig nach anwendbaren gesetzlichen, behördlichen oder sonstigen regulatorischen Vorschriften ist. Zusätzlich verpflichtet sich der Auftragnehmer, die Ursachen der Sicherheitsvorfälle zu analysieren, Gegenmaßnahmen zu treffen und den Auftraggeber bei etwaigen forensischen Analysen zu unterstützen.
(4) Der Auftragnehmer unterstützt den Auftraggeber ferner aktiv und unverzüglich bei der Erfüllung gesetzlicher, behördlicher oder sonstiger regulatorischer Meldepflichten des Auftraggebers, insbesondere durch Bereitstellung aller hierfür erforderlichen Informationen in geeigneter Form und unverzüglich, spätestens innerhalb der hierfür maßgeblichen gesetzlichen Fristen sowie durch Mitwirkung an Abstimmungen mit zuständigen Behörden. Eigene gesetzliche Meldepflichten des Auftragnehmers bleiben unberührt; der Auftragnehmer erfüllt diese fristgerecht und informiert den

Auftraggeber hierüber parallel, soweit rechtlich zulässig. Der Auftragnehmer stellt sicher, dass entsprechende Verpflichtungen auch gegenüber etwaigen Subunternehmern vereinbart werden und diese eingehalten werden. Auf Verlangen weist der Auftragnehmer geeignete organisatorische und technische Maßnahmen zur Umsetzung dieser Pflichten nach.
(5) 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.

§ 3 Regulatorische Anforderungen
(1) Der Auftragnehmer wird seine Lieferungen und Leistungen so konzipieren und erbringen, dass dies in Einklang mit den jeweils für ihn geltenden und den für den Auftraggeber beim vertragsgemäßen Einsatz der Lieferungen und Leistungen einschlägigen gesetzlichen, behördlichen und sonstigen regulatorischen Anforderungen steht. Dazu zählen in der Regel insbesondere die Anforderungen der DSGVO, des Data Act, der KI-Verordnung, gesetzliche Anforderungen in Bezug auf IT-Sicherheit und für den Energiesektor einschlägige Anforderungen.
(2) Soweit der Auftraggeber Lieferungen und Leistungen des Auftragnehmers bestimmungsgemäß an seine Kunden weitervertreibt, muss der Auftragnehmer den Auftraggeber ferner in die Lage versetzen, die für den Auftraggeber in Bezug auf die Lieferung oder Leistung bestehenden gesetzlichen, behördlichen oder sonstigen regulatorischen Anforderungen gegenüber seinen Kunden zu erfüllen. Falls der Auftraggeber von dem Auftragnehmer bezogene digitale Produkte bestimmungsgemäß an seine Kunden weitervertreibt, zählen dazu insbesondere die Bestimmungen der §§ 327 ff. BGB einschließlich dort geregelter gesetzlicher Aktualisierungspflichten.

§ 4 KRITIS-Dachgesetz und kritische Infrastrukturen
(1) Soweit der Auftragnehmer als Betreiber kritischer Infrastrukturen im Sinne KRITIS-Dachgesetzes qualifiziert ist, verpflichtet er sich, die Anforderungen des KRITIS-Dachgesetzes in ihrer jeweils geltenden Fassung einzuhalten.
(2) Der Auftragnehmer stellt sicher, dass die für kritische Infrastrukturen geltenden besonderen Sicherheitsanforderungen erfüllt werden und dass geeignete Maßnahmen zur Gewährleistung der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme getroffen werden.

§ 5 Aktualisierung und Anpassung an Rechtsänderungen
Der Auftragnehmer verpflichtet sich, die Sicherheitsmaßnahmen regelmäßig zu überprüfen und an den aktuellen Stand der Technik sowie an neue oder geänderte rechtliche Anforderungen anzupassen. Sollten sich die rechtlichen Anforderungen, insbesondere durch Änderungen der NIS2-Richtlinie oder deren nationaler Umsetzung, ändern, verpflichtet sich der Auftragnehmer, seine Maßnahmen entsprechend anzupassen und dies dem Auftraggeber unverzüglich anzuzeigen.

§ 6 Weiterverpflichtung von Unterauftragnehmern
Der Auftragnehmer verpflichtet sich, alle Unterauftragnehmer vertraglich zu mindestens den gleichen Einhaltungs-, Sicherheits- und Meldepflichten zu verpflichten, wie sie in dieser Verpflichtungserklärung festgelegt sind. Der Auftragnehmer haftet für die Einhaltung dieser Verpflichtungserklärung durch seine Unterauftragnehmer wie für eigenes Verschulden.

§ 7 Zusammenarbeit und Auditrechte
(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Überprüfung der Einhaltung der in dieser Verpflichtungserklärung genannten Pflichten. Der Auftraggeber ist berechtigt, nach vorheriger Ankündigung und in angemessenem Umfang Auditmaßnahmen bei dem Auftragnehmer durchzuführen oder durch Dritte durchführen zu lassen, um die Einhaltung der gesetzlichen Vorgaben zu überprüfen.
(2) Die Auditmaßnahmen beschränken sich auf die für die Auftragsdurchführung relevanten Bereiche und werden zu üblichen Geschäftszeiten durchgeführt. Der Auftragnehmer gewährt dem Auftraggeber

oder den beauftragten Prüfern Zugang zu den erforderlichen Informationen, Unterlagen und Systemen, soweit dies zur Überprüfung der Einhaltung der Verpflichtungen erforderlich ist und keine berechtigten Geheimhaltungsinteressen des Auftragnehmers entgegenstehen.
(3) Der Auftragnehmer und der Auftraggeber verpflichten sich, alle im Rahmen der Auditmaßnahmen erlangten Informationen vertraulich zu behandeln und nur für den Zweck der Überprüfung der Einhaltung dieser Verpflichtungserklärung zu verwenden.

§ 8 Folgen der Pflichtverletzung
(1) Die Verletzung der in dieser Verpflichtungserklärung genannten Pflichten berechtigt den Auftraggeber zur außerordentlichen Kündigung des mit dem Auftragnehmer geschlossenen Hauptvertrages, sofern die Verletzung nicht unerheblich ist und der Auftragnehmer eine ihm gesetzte angemessene Frist zur Behebung der Verletzung fruchtlos verstreichen lässt.
(2) Schadensersatzansprüche des Auftraggebers wegen Verletzung dieser Verpflichtungserklärung bleiben unberührt. Der Auftragnehmer haftet dem Auftraggeber für alle Schäden, die dem Auftraggeber aus der Verletzung der in dieser Verpflichtungserklärung genannten Pflichten entstehen, soweit dem Auftragnehmer ein Verschulden zur Last fällt. Eine Verletzung der Pflichten aus dieser Verpflichtungserklärung begründet keine zivilrechtliche Haftung über die gesetzlichen Vorschriften hinaus.

§ 9 Geltungsdauer
Diese Verpflichtungserklärung gilt für die gesamte Dauer des Vertragsverhältnisses im Rahmen des Hauptvertrages zwischen den Parteien.