Anhang – Anforderungen zur Informationssicherheit und zum Datenschutz bei Consulting-Dienstleistungen

1 Allgemeine Anforderungen der Informationssicherheit

Allgemeine Anforderungen sind Anforderungen, die generell für die Erbringung aller Leistungen durch den LIEFERANTEN gelten.

1.1 **Seriöse Quellen**: Der LIEFERANT stellt sicher, dass Hard- und Softwareprodukte aus bekannten und seriösen Quellen bezogen werden und dass es einen zuverlässigen technischen Support und eine nachvollziehbare Lieferkette gibt.

1.2 **Verwaltung von Betriebsmitteln**: Der LIEFERANT stellt sicher, dass (i) Betriebsmittel/Assets (Hardware und Software), die zur Erstellung, Verarbeitung, Speicherung oder Übertragung von E.ON Informationen verwendet werden, während ihres gesamten Lebenszyklus vor Korruption, Verlust, Diebstahl und unbefugter Offenlegung geschützt sind. Der LIEFERANT stellt sicher, dass diese Betriebsmittel (Assets) in Inventarlisten erfasst sind, die (ii) gegen unbefugte Änderungen geschützt sind, (iii) aktuell gehalten wird, (iv) regelmäßig gesichert werden und (v) die erforderlichen Angaben über die Betriebsmittel/Assets (Hardware und Software) enthalten und – falls zutreffend – Compliance-Anforderungen in Bezug auf die Betriebsmittel enthalten. Der LIEFERANT stellt sicher, dass (vi) alle Betriebsmittel (Assets) einem Verantwortlichem zugeordnet werden, der für den Betrieb der Betriebsmittel/Assets verantwortlich ist.

1.3 **Systemzugang/-zugriff**: Der LIEFERANT beschränkt den Zugang zu bzw. Zugriff auf Betriebsmittel/Assets, mit denen E.ON Informationen erstellt, verarbeitet, gespeichert oder übertragen werden, auf autorisiertes Personal für zweckgebundene betriebliche Zwecke. Dazu gehört zumindest, dass (i) nur autorisiertes Personal Zugang zu bzw. Zugriff auf relevante Informationen erhält, (ii) die Zugriffsrechte auf die genehmigte Systemfunktionalität beschränkt sind, (iii) eine angemessene Funktionstrennung besteht, (iv) die Zugriffsrechte nicht geteilt werden (Benutzer-IDs und Passwörter dürfen nicht geteilt werden). Der LIEFERANT stellt sicher, dass der administrative Zugriff auf Systeme, die E.ON Informationen speichern oder verarbeiten, (v) auf eine minimale Anzahl von Administratoren beschränkt ist (vi.) Der Lieferant stellt sicher, dass E.ON Informationen „in transit“ sowie „at rest“ verschlüsselt sind.

1.4 **Systemverwaltung**: Der LIEFERANT betreibt Systeme, die E.ON Informationen erstellen, speichern, verarbeiten oder übertragen, um (i) die aktuelle und prognostizierte Auslastung bewältigen zu können und (ii) sie konsistent und fehlerfrei zu konfigurieren. Der LIEFERANT verwaltet die Sicherheit der Systeme, indem er (iii) Backups wichtiger Informationen und Software durchführt.

1.5 **Netzwerk und Kommunikation**: Der LIEFERANT stellt sicher, dass physische, drahtlose und – falls zutreffend – Sprachnetze so ausgelegt sind, dass sie (i) zuverlässig und belastbar sind, (ii) unberechtigten Zugriff verhindern, (iii) verschlüsselte Verbindungen verwenden, und (iv) verdächtigen Datenverkehr erkennen. (v) Der LIEFERANT stellt sicher, dass Netzwerkgeräte (einschließlich Router, Firewalls und Wireless Access Points) so konfiguriert werden, dass sie nach Bedarf funktionieren und nicht autorisierte und fehlerhafte Updates verhindern. Der LIEFERANT gewährleistet den Schutz elektronischer Kommunikations-systeme, indem er (vi) Sicherheitseinstellungen festlegt und die Systeme entsprechend konfiguriert.

1.6 **Technisches Sicherheitsmanagement**: Der LIEFERANT installiert Malware-Schutzlösungen auf Systemen, auf denen E.ON Informationen Malware ausgesetzt sein können, einschließlich (i) Malware-Schutzsoftware, die vor allen Formen von Malware schützen (z. B. Viren, Würmern, Trojanischen Pferden, Spyware, Rootkits, Botnet-Software, Keylogger, Ransomware) sollte. (ii) Malware-Schutzsoftware sollte automatisch verteilt werden. (iii) Der LIEFERANT stellt sicher und überprüft regelmäßig, dass Malware-Schutzsoftware nicht deaktiviert oder in der Funktion eingeschränkt wurde, die Konfiguration der Malware-Schutzsoftware korrekt ist, Updates korrekt angewendet werden, regelmäßige Scans durchgeführt werden, und eine angemessene Benachrichtigung über identifizierte Malware-Ereignisse erfolgt.

1.7 **Aktuelle Patch Level**: Der LIEFERANT stellt sicher, dass technische Schwachstellen behoben werden, indem (i) Patches identifiziert und von autorisierten Quellen bezogen werden, sobald sie verfügbar sind, (ii) entschieden wird, wann Patches bereitgestellt werden, (iii) Patches rechtzeitig bereitgestellt werden. (iv) Der LIEFERANT ist befugt, Patches in der IT-Umgebung anzuwenden, einschließlich Virtualisierungshypervisoren, virtuellen Maschinen, Betriebssystemen und Anwendungen, solange dies keine negativen Auswirkungen auf die Vertraulichkeit, Integrität oder Verfügbarkeit von E.ON Informationen hat.

1.8 **Härtung**: Alle Informations- und Netzwerksysteme müssen gehärtet werden. Dies beinhaltet (i) das Deaktivieren unnötiger Anwendungen, Dienste, Tools, Protokolle und Schnittstellen, (ii) das Löschen oder zumindest Ändern der vom Hersteller bereitgestellten Standardbenutzernamen und Passwörter, (iii) das Aktivieren von sicherheitserhöhenden Optionen und (iv) das Verhindern der Übertragung von technischen Informationen an externe Stellen.

1.9 **Sichere Entsorgung und Wiederverwendung**: Der LIEFERANT stellt sicher, dass ausrangierte Hardware (i) entweder vor der Wiederverwendung, dem Verkauf oder der Rückgabe so gesäubert wird, dass alle E.ON Informationen sicher gelöscht werden (ii) oder sicher vernichtet werden. (iii) Die Säuberung oder Vernichtung muss auf sichere Weise mit dem Stand der Technik entsprechenden Technologien und Verfahren, wie z. B. der in NIST 800-88 „Guideline for Media Sanitization“ definierten Werkzeuge und Verfahren, durchgeführt werden. (iv) Die Konzepte für die sichere Entsorgung und Löschung sowie die Nachweise für die sichere Entsorgung und Löschung von E.ON Informationen werden E.ON auf Anfrage zur Verfügung gestellt.

1.10 **Vertraulichkeitsvereinbarung (NDA):** Der LIEFERANT stellt sicher, dass alle involvierten Mitarbeiter, die E.ON Informationen verarbeiten, eine Vertraulichkeitsvereinbarung unterzeichnet und verstanden haben.

1.11 **Awareness im Bereich Informationssicherheit**: Der LIEFERANT stellt sicher, dass relevante Benachrichtigungen zur Aufklärung im Bereich Informationssicherheit angemessen an die Mitarbeiter kommuniziert werden. Mitarbeiter, die E.ON Informationen verarbeiten, sind verpflichtet, E.ONs Information Security Awareness Online Training erfolgreich zu absolvieren.

1.12 **Rückgabe von Unternehmenswerten**: Der LIEFERANT stellt sicher, dass Unternehmenswerte der E.ON vor Beendigung der Zusammenarbeit unbeschadet zurückgegeben werden.

1.13 **Kollaboration:** Beide Parteien vereinbaren, dass im Bereich der Informationssicherheit Ansprechpartner existieren und sie gemeinsam kooperieren.

2 Anforderungen des Datenschutzes

2.1 Der Auftragnehmer verpflichtet sich, die gesetzlichen Bestimmungen über den Datenschutz (z. B. Datenschutz-Grundverordnung (DS-GVO)) einzuhalten.

2.2 Der Auftragnehmer verarbeitet oder nutzt die personenbezogenen Daten der E.ON ausschließlich im Rahmen der vertraglichen Vereinbarungen, insbesondere gibt er die Daten nicht an Dritte weiter. Die Parteien gehen davon aus, dass der Auftragnehmer seine Dienstleistungen für E.ON in eigener Verantwortlichkeit gemäß Art. 4 Nr. 7 DS-GVO durchführt. Der Auftragnehmer wird die personenbezogenen Daten, die er von E.ON erhält, durch geeignete technische und organisatorische Maßnahmen (wie unter Ziffer 1 beschrieben) vor dem Zugriff unberechtigter Dritter schützen. Der Auftragnehmer unterrichtet die E.ON unverzüglich bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf Datenschutzverletzungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten der E.ON.

2.3 Sollte sich aufgrund einer Änderung der ursprünglichen Beauftragung des Auftragnehmers eine von Ziffer 2.2 abweichende datenschutzrechtliche Beurteilung ergeben, werden die Parteien im Rahmen dieser Beauftragung und bevor eine Verarbeitung der personenbezogenen Daten durch den Auftragnehmer erfolgt eine weitere entsprechende datenschutzrechtliche Vereinbarung (Auftragsverarbeitungsvereinbarung bzw. Vereinbarung über die gemeinsame Verantwortlichkeit) schließen.

2.4 Werden Ansprüche von Betroffenen, deren Daten von E.ON und vom Auftragnehmer verarbeitet werden, gegenüber der E.ON wegen einer nach der DS-GVO oder anderen Vorschriften über den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung geltend gemacht und ist streitig, ob die Datenschutzverletzung von E.ON oder dem Auftragnehmer verursacht worden ist, so liegt die Beweislast für das Nicht-Vorliegen der Verantwortlichkeit des Auftragnehmers bei dem Auftragnehmer.