INFORMATIONSSICHERHEIT

1 Definitionen

Daten sind alle Finanz-/Geschäftsinformationen, Entwürfe, Maße, Spezifikationen, Zeichnungen, Muster, Computerdateien oder Software, Know-how oder andere Informationen, einschließlich technischer Daten, die sich auf Methoden, Herstellungsverfahren, Ausrüstungen, Messgeräte und Werkzeuge beziehen, die bei der Entwicklung und Herstellung von Waren oder der Erbringung von Dienstleistungen verwendet werden. Die Daten können in einem schriftlichen oder gedruckten Dokument, in einem Computer oder in einer elektronisch gespeicherten Datei, in Software oder in einer anderen greifbaren Ausdrucksform festgehalten werden.

Informationssicherheitsvorfall ist (1) jeder tatsächliche oder potenzielle Vorfall, der ein Informationssystem betrifft, das sich im Besitz oder unter der Kontrolle des Lieferanten befindet, und welches möglicherweise sensible Informationen des Auftraggebers betrifft, oder (2) jeder tatsächliche oder potenzielle unbefugte Zugriff auf, die Nutzung oder Offenlegung von sensiblen Informationen des Auftraggebers. Vorfall ist ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten beeinträchtigt,

Information ist jede Mitteilung oder Darstellung von Wissen wie Fakten, Daten oder Meinungen auf einem beliebigen Medium oder einer beliebigen Form, einschließlich Text, Zahlen, Grafiken, Kartografie, Erzählungen oder audiovisuellem Material.

Informationssystem: Informationsressourcen, die Informationen sammeln, verarbeiten, pflegen, nutzen, weitergeben, verbreiten oder entsorgen.

Beschaffungsbeauftragter ist die Person, die vom Auftraggeber ermächtigt ist, diesen Vertrag zu verwalten und/oder auszuführen, und die allein befugt ist, im Namen des Auftraggebers vertragliche Verpflichtungen einzugehen, vertragliche Anweisungen zu erteilen und vertragliche Anforderungen dieses Vertrags zu ändern.

Sensible Informationen sind alle Informationen, die im Zusammenhang mit diesem Vertrag gesammelt, verarbeitet, gepflegt, verwendet, weitergegeben oder verbreitet werden und die geschützt werden müssen, um ihre Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten, einschließlich, aber nicht beschränkt auf nach dem Urheberrechtsgesetz oder dem Gesetz zum Schutz von Geschäftsgeheimnissen geschützte oder sonstige vertrauliche Informationen des Auftraggebers und rechtlich geschützte Informationen von Dritten sowie personenbezogene Daten.

2 Angemessene Sicherheitsmaßnahmen

2.1 Der Lieferant/Dienstleister wendet angemessene und geeignete administrative, technische, physische, organisatorische und betriebliche Sicherheitsvorkehrungen und -maßnahmen an, um sensible Informationen vor zufälliger und schuldhafter Zerstörung, Veränderung und unbefugter oder unzulässiger Offenlegung oder unberechtigtem Zugriff zu schützen, unabhängig davon, ob sich diese sensiblen Informationen in den internen Systemen des Lieferanten oder in einer Cloud-Umgebung befinden.

2.2 Wenn die Erfüllung des Vertrags durch den Lieferanten die Übertragung, Speicherung oder Verarbeitung sensibler Informationen in einem Informationssystem beinhaltet, muss der Lieferant mindestens die folgenden Maßnahmen einsetzen:

a) Grundlegende Sicherheitsmaßnahmen

1. Beschränkung des Zugriffs auf Informationssysteme für ausschließlich autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, oder Geräte (einschließlich anderer Informationssysteme).
2. Reduzierung der Zugriffe für autorisierte Benutzer auf die zur Aufgabenerfüllung notwendigen Funktionen.
3. Überprüfung und Begrenzung von Verbindungen von und zu externen Informationssystemen und deren Nutzung.
4. Kontrolle von Informationen, die in öffentlich zugänglichen Informationssystemen verarbeitet werden.
5. Identifizierung der Benutzer von Informationssystemen, und den Prozessen, die durch den Benutzer oder von Systemen/Systemkonten ausgeführt werden.
6. Authentifizierung von Benutzern, Prozessen oder Geräten als Voraussetzung für die Gewährung des Zugangs zu den Informationssystemen des Lieferanten.
7. Speichermedien, die sensible Informationen enthalten, sind vor der Entsorgung oder der Freigabe zur Wiederverwendung ausreichend sicher zu bereinigen oder zu vernichten.
8. Beschränkung des physischen Zugangs zu den Informationssystemen des Lieferanten auf autorisierte Personen.
9. Begleitung von Besuchern und Überwachung der Besucheraktivitäten; Führung von Prüfprotokollen über den physischen Zugang; Kontrolle und Verwaltung der physischen Zugangsgeräte.
10. Überwachung, Kontrolle und Schutz der Kommunikationsverbindungen an Zugangspunkten zum Netzwerk.
11. Implementierung von Teilnetzen für öffentlich zugängliche Systeme, die physisch oder logisch von internen Netzen getrennt sind.
12. Feststellung, Meldung und rechtzeitige Behebung von Fehlern in Informationen und Informationssystemen.
13. Einsatz von Schutzprogrammen vor Schadsoftware an geeigneten Stellen in den Informationssystemen des Lieferanten.
14. Aktualisierung von Schutzprogrammen für Schadsoftware, sobald neue Versionen verfügbar sind.
15. Durchführung regelmäßiger Schwachstellen-Scans von Informationssystemen und Echtzeit-Scans von Dateien aus externen Quellen, wenn Dateien heruntergeladen, geöffnet oder ausgeführt werden.

b) Zusätzliche Sicherheitsmaßnahmen
    1. Erstellung und Anwendung von Sicherheitseinstellungen von Produkten, die in den Informationssystemen des Lieferanten eingesetzt werden.
    2. Einrichtung und Aufrechterhaltung von Verfahren und Systemen zum angemessenen Schutz sensibler Informationen, einschließlich der angewandten Vernichtungsmethoden, des Schutzes von Audit- und Systemprotokolldaten und der Möglichkeit zur verschlüsselten Übertragung sensibler Informationen.
    3. Sicherstellung, dass die bei den durchgeführten Schwachstellen-Scans festgestellte Risiken unverzüglich behandelt werden.

3 Reaktion auf Informationssicherheitsvorfälle und Benachrichtigung

3.1 Der Lieferant muss über dokumentierte und nachvollziehbare Prozesse verfügen, die sich mit Informationssicherheitsvorfällen befassen. Bei diesen Prozessen sollte es sich um eine Reihe schriftlicher Anweisungen handeln, die unter anderem Folgendes umfassen: Erkennen, Reagieren und Begrenzen der Auswirkungen eines Informationssicherheitsvorfalls inklusive der Sammlung von Beweisen.

3.2 Der Lieferant benachrichtigt den Beschaffungsbeauftragten und den Informationssicherheitsbeauftragten (cybersecurity@litef.de) des Auftraggebers unverzüglich, spätestens jedoch 72 Stunden nach Entdeckung eines Informationssicherheitsvorfalls. Auf Kosten des Lieferanten wird der Lieferant (1) jeden Vorfall im

Bereich der Informationssicherheit unverzüglich untersuchen, (2) alle angemessenen Anstrengungen unternehmen, um sensible Informationen zu sichern und die Auswirkungen des Vorfalls im Bereich der Informationssicherheit zu mindern, (3) dem Auftraggeber laufend zeitnahe und relevante Informationen über den Vorfall im Bereich der Informationssicherheit zur Verfügung stellen und (4) gegebenenfalls mit dem Auftraggeber zusammenarbeiten, um betroffene Dritte zu informieren.

3.3 Diese Klausel entbindet den Lieferanten nicht von anderen anwendbaren Schutzanforderungen, Abhilfemaßnahmen oder Verpflichtungen in Bezug auf den Schutz sensibler Informationen, die in diesem Vertrag, nach anwendbarem Recht oder durch behördliche Anordnung gefordert werden.

4 Der Lieferant antwortet unverzüglich und angemessen auf alle Anfragen des Auftraggebers bezüglich der Einhaltung dieser Regelungen, einschließlich der Dokumentation der implementierten Maßnahmen und Prozesse, welche oben beschrieben sind.