GELSENWASSER

Sicherheitsanforderungen

an Dienstleister und Lieferanten der GELSENWASSER AG

Stand 07/2026

1 Allgemeines

Die nachfolgenden Anforderungen gelten für Auftragnehmer (AN) sowohl im Hinblick auf die IT-Sicherheit als auch im Hinblick auf die OT-Sicherheit des Auftraggebers (AG), inkl. KI, sofern vom AN in Bezug auf die gegenüber dem AG zu erbringenden Leistungen verwendet.

2 IT-Sicherheit

Bei jeglicher elektronischen Kommunikation mit dem AG (insbesondere E-Mail, elektronische Rechnungsstellung, Datenübermittlung) hat der AN folgende dem Stand der Technik entsprechenden Mindestanforderungen zu erfüllen:

a) Verwendung aktueller IT-Systeme mit aktuellem Virenschutz und Malware-Schutz;

b) Nutzung sicherer, geschäftlicher E-Mail-Adressen (keine privaten E-Mail-Konten);

c) Verschlüsselung bei Übermittlung vertraulicher Informationen, insbesondere Informationen über kritische Anlagen oder deren Sicherheit, personenbezogene Daten sowie Geschäftsinterna und vertrauliche Geschäftsinformationen nach Stand der Technik;

d) Verwendung starker Passwörter, Passwortwechsel ereignisbasiert, zweiter Faktor ist möglichst zu aktivieren;

e) Unterlassung der Nutzung unsicherer Übertragungswege wie unverschlüsselte E-Mails für vertrauliche Inhalte, öffentliche File-Sharing-Dienste ohne Ende-zu-Ende-Verschlüsselung sowie SMS oder unverschlüsselte Messenger-Dienste für vertrauliche Informationen.

3 KI-Nutzung

3.1 KI-Einsatz und Zustimmungspflicht

Für die im Zusammenhang mit der Thematik der künstlichen Intelligenz verwendeten Begrifflichkeiten wird auf die EU Verordnung 2024/1689 (KI VO) verwiesen. Der Einsatz künstlicher Intelligenz (KI) bei der Leistungserbringung bedarf der vorherigen textförmlichen Zustimmung des AG. Ohne Zustimmung ist der KI-Einsatz unzulässig.

3.2 KI-Pflichten

Der AN stellt sicher, dass alle gesetzlichen und regulatorischen Anforderungen im Zusammenhang mit KI – insbesondere der KI VO – eingehalten werden. Der AG weist auf die sektorspezifischen Anforderungen für kritische Infrastruktur hin (Art. 6 KI-VO i. V. m. Anhang III).

Der AN muss die vertraglichen Leistungen auch ohne KI vollständig und vertragsgemäß erbringen können. Das Verbot nicht genehmigter KI-Nutzung begründet keine Unmöglichkeit oder Erschwerung der Leistungserbringung. Die Verantwortung für die Richtigkeit und Qualität der Leistungen verbleibt uneingeschränkt beim AN, auch wenn KI-Systeme eingesetzt werden. Der Einsatz von KI entbindet nicht von der Pflicht zur sorgfältigen Leistungserbringung.

3.3 KI-Daten und Restriktionen

Mit KI-Systemen verarbeitet der AN ausschließlich diejenigen Daten des AG, die für den genehmigten Zweck zwingend erforderlich sind.

Die Weitergabe oder Zugänglichmachung von Daten des AG an Dritte ist nur zulässig, wenn sie für den genehmigten KI-Einsatz technisch zwingend erforderlich, vorab offengelegt und vom AG ausdrücklich genehmigt und vertraulichkeitsrechtlich mit dem Dritten abgesichert ist.

Die Verwendung von Daten des AG – auch anonymisiert oder pseudonymisiert – für Training, Optimierung oder Weiterentwicklung von KI-Systemen oder -Modellen ist untersagt, sofern der AG nicht zuvor ausdrücklich in Textform zugestimmt hat.

Der AG kann eine erteilte KI-Genehmigung jederzeit aus wichtigem Grund widerrufen, insbesondere bei geänderter Sicherheits- oder Rechtslage, Verstößen des AN gegen Auflagen des AG, Sicherheitsvorfällen oder erheblichen Fehlfunktionen. Der Widerruf erfolgt in Textform. Die Umstellung auf KI-freie Leistung hat innerhalb von 48 Stunden, bei schweren Vorfällen sofort, zu erfolgen. Der AN setzt die Leistung unverzüglich und in unveränderter Qualität ohne KI fort. Der Widerruf begründet keine Ansprüche des AN auf Mehrvergütung oder Fristverlängerung.

Der Einsatz von KI ist unabhängig von einer Zustimmung grundsätzlich untersagt bei Verarbeitung geheimer/streng vertraulicher Daten des AG, Daten nach Art. 9 DSGVO sowie sicherheitskritischen Vorgängen mit Einfluss auf kritische Infrastruktur. Darüber hinaus bei KI-Systemen mit Datenverarbeitung außerhalb EU/EWR, Training/Modellnutzung mit AG-Daten ohne Zustimmung, nicht nachvollziehbarer Funktionsweise und automatisierten Entscheidungen ohne menschliche Prüfung (Art. 22 DSGVO).

Weitere Ausschlüsse können vom AG aus Sicherheits- oder Gesetzesgründen bestimmt werden.

GELSENWASSER AG
Willy-Brandt-Allee 26, 45891 Gelsenkirchen
E-Mail: materialwirtschaft@gelsenwasser.de
www.gelsenwasser.de

4 Pflichten bei Informationssicherheits- und KI-Vorfällen

4.1 Begriffsbestimmungen

Ein sicherheitsrelevanter Vorfall liegt insbesondere vor, wenn ein Ereignis eintritt, das die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen, Daten, Geschäftsprozessen, IT-Systemen, IT-Anwendungen oder IT-Infrastruktur des AN (soweit eingesetzt auch der KI-Systeme), des AG oder Dritter, deren Daten im Zusammenhang mit dem Vertrag verarbeitet werden, beeinträchtigt ist oder eine solche Beeinträchtigung zu befürchten ist. Dies gilt insbesondere bei:

- Sicherheits-/Datenschutzvorfällen und Verletzungen der Vertraulichkeit,
- unbefugtem Zugriff auf vertrauliche Informationen des AG,
- Verlust/Diebstahl von Unterlagen, Datenträgern oder IT-Geräten mit Informationen des AG,
- Cyberangriffen (z. B. Malware, Ransomware, Phishing) auf für die Vertragserfüllung genutzte IT-Systeme,
- erheblichen Fehlfunktionen eingesetzter KI-Systeme mit Auswirkung auf Qualität/Zuverlässigkeit,
- behördlichen/gerichtlichen Anfragen, Untersuchungen oder Maßnahmen im Zusammenhang mit KI,
- wesentlichen sicherheits- oder funktionsrelevanten Änderungen an KI-Systemen durch den Hersteller.

Vorfälle ausschließlich physischer Natur ohne Bezug zu informationstechnischen Systemen oder Daten werden ausschließlich nach Maßgabe von Ziff. 7 behandelt.

Ein erheblicher Sicherheitsvorfall im Sinne des § 2 Nr. 11 BSIG liegt vor, wenn ein IT-Vorfall zu schwerwiegenden Betriebsstörungen der Dienste geführt hat oder führen kann, erhebliche finanzielle Verluste verursacht hat oder verursachen kann oder andere Personen durch wesentliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann. Dies kann auch Sicherheitsvorfälle mit kombinierter (cyber-physischer) Wirkung umfassen.

4.2 Meldepflichten

Der AN meldet erhebliche Sicherheitsvorfälle, die Auswirkungen auf die IT- oder OT-Systeme des AG haben könnten, wie folgt:

a) unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnis eines erheblichen Sicherheitsvorfalls, der Auswirkungen auf die IT-Systeme des AG haben könnte: frühe Erstmeldung einschließlich Angabe, ob der Verdacht besteht, dass der Vorfall auf rechtswidrige/böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte;

b) unverzüglich, spätestens innerhalb von 72 Stunden nach Kenntnis: Meldung mit erster Bewertung einschließlich Schweregrad und Auswirkungen sowie ggf. Kompromittierungsindikatoren;

c) auf Ersuchen des AG: Zwischenmeldung über relevante Statusaktualisierungen;

d) spätestens einen Monat nach Meldung nach lit. (b): Abschlussmeldung oder, wenn noch nicht möglich, Zwischenmeldung mit

   - ausführlicher Beschreibung (Schweregrad, Auswirkungen),
   - Art der Bedrohung/zugrunde liegende Ursache,
   - getroffene und laufende Abhilfemaßnahmen,
   - ggf. grenzüberschreitende Auswirkungen.

Der AN meldet auch Beinahevorfälle und erhebliche Cyberbedrohungen, die die Vertragserfüllung beeinträchtigen könnten, unverzüglich.

Soweit der sicherheitsrelevante Vorfall kritische Anlagen oder kritische Dienstleistungen des AG im Sinne des BSIG betrifft oder betreffen könnte, hat der AN in seiner Meldung zusätzlich Angaben zu machen zur Art der betroffenen kritischen Anlage, zur betroffenen kritischen Dienstleistung sowie zu den tatsächlichen oder voraussichtlichen Auswirkungen auf diese Dienstleistung. Diese Angaben sind in der Meldung nach lit. (a) als vorläufige Einschätzung und in der Meldung nach lit. (b) in aktualisierter und substantiierter Form zu übermitteln.

Die Meldung erfolgt per E-Mail an Informationssicherheit@gelsenwasser.de, soweit dies nicht möglich ist, in Textform postalisch an die Verwaltung des AG. Sollte sich die Kontaktadresse ändern, wird der AG dem AN diese Änderung textförmlich mitteilen. Der AN hat diese Kontaktadresse spätestens zwei Wochen nach Mitteilung zu verwenden. Die Meldung enthält mindestens Art/Kategorie des Vorfalls, Zeitpunkt/Dauer, betroffene Systeme/Daten/Informationen, Schweregrad/Auswirkungen, ergriffene oder geplante Gegenmaßnahmen sowie eine Ansprechperson inkl. Kontaktdaten. Soweit vorhanden, sind auch Kompromittierungsindikatoren (IOCs) zu übermitteln.

Die Meldepflichten gelten auch für sicherheitsrelevante Vorfälle bei Nachunternehmern/Vorlieferanten des AN, soweit diese die Leistung, Systeme, Daten oder Standorte des AG beeinträchtigen können. Der AN stellt die unverzügliche Weiterleitung verfügbarer Informationen sicher. Die Regelungen in Ziff. 8 bleiben hiervon unberührt.

Die Bearbeitung eines sicherheitsrelevanten Vorfalls gilt erst mit Vorlage eines den jeweils geltenden BSI-Vorgaben entsprechenden Abschlussberichts als abgeschlossen.

Der AN unterstützt den AG bei der Erfüllung weiterer gesetzlicher Melde- und Mitwirkungspflichten.

4.3 Mitwirkungspflichten

Der AN wirkt bei der Beseitigung oder Vermeidung erheblicher Sicherheitsvorfälle mit, soweit diese seine Leistungen betreffen. Soweit zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit erforderlich, wirkt der AN an der Wiederherstellung mit.

Der AN wirkt bei der Ermittlung von Sachverhalten mit, teilt auf Verlangen alle für das Verfahren erheblichen Tatsachen vollständig und wahrheitsgemäß mit und gibt bekannte Beweismittel an.

Soweit der AN Leistungen erbringt, die Standorte/Anlagen/Objekte des AG physisch beeinflussen oder vor Ort erbracht werden, hält der AN angemessene Notfall- und Kontaktwege vor, beachtet Zutritts-/Sicherheitsvorgaben des AG und stellt dem AG auf Anforderung die zur Erfüllung gesetzlicher Resilienz- und Nachweispflichten erforderlichen, bei ihm verfügbaren Informationen zu Abhängigkeiten, Engpässen und Wiederanlaufmöglichkeiten bereit, soweit rechtlich zulässig.

5 Vertragliche Folgen eines Sicherheitsvorfalls

Sofern ein Sicherheitsvorfall beim AN eingetreten ist, der Auswirkungen auf die IT- oder OT-Systeme des AG haben könnte, ist der AG berechtigt, den Zugang zu seinen Systemen so lange zu sperren, bis der Sicherheitsvorfall nachweislich behoben wurde.

Durch die Sperrung des Zugangs gerät der AG nicht in Annahmeverzug. Der AN kann hieraus keine Ansprüche herleiten.

6 Erweitere Pflichten für kritische Lieferanten

Die Regelungen dieser Ziff. 6 finden auf kritische Lieferanten Anwendung.

6.1 Begriffsbestimmung

Kritische Lieferanten sind AN, deren Leistungen unmittelbar oder mittelbar geeignet sind, die Verfügbarkeit, Integrität oder Sicherheit

- kritischer Anlagen,

- kritischer Dienstleistungen oder

-sicherheitsrelevanter IT-, OT- oder KI-Systeme

des AG zu beeinflussen, insbesondere wenn der AN im Zusammenhang mit der Leistungserbringung

- Zugriff auf IT- oder OT-Systeme, Netze, Daten oder Standorte des AG erhält,

- Daten oder Informationen des AG verarbeitet, überträgt oder speichert,

- digitale, vernetzte oder fernwartbare Komponenten, Software oder Services bereitstellt/betreibt oder

- die Verfügbarkeit, Integrität oder Sicherheit betrieblicher Prozesse/ Anlagen/(kritischer) Dienstleistungen des AG beeinflussen kann.

Die Einstufung als kritischer Lieferant erfolgt durch den AG. Der AG teilt dem AN dies auf Anforderung bei Vertragsschluss in Textform mit. Der AN ist verpflichtet, auf Verlangen des AG Angaben zu machen, die eine sachgerechte Einstufung ermöglichen. Der AN hat den AG unverzüglich zu informieren, wenn sich Umstände ändern, die für seine Einstufung relevant sein könnten. Der AG ist berechtigt, die Einstufung nach Maßgabe veränderter Risikoverhältnisse zu aktualisieren. Er teilt dem AN eine geänderte Einstufung auf Verlangen in Textform mit.

6.2 Technische und organisatorische Maßnahmen

6.2.1 Allgemeines

Der AN ist verpflichtet, geeignete, verhältnismäßige, risikobasierte, leistungsbezogene und wirksame technische und organisatorische Maßnahmen zu ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die er für die Erbringung seiner Leistungen nutzt, zu vermeiden und die Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten

Die vom AN umzusetzenden Maßnahmen sind auf Basis einer Verhältnismäßigkeitsbewertung am Stand der Technik auszurichten. Einschlägige europäische und internationale Normen sind angemessen zu berücksichtigen. Die Maßnahmen müssen auf einem gefahrenübergreifenden Ansatz beruhen.

Bei der Bewertung der Verhältnismäßigkeit sind insbesondere Ausmaß der Risikoexposition, Art und Umfang der Leistung, Eintrittswahrscheinlichkeit und Schwere möglicher Sicherheitsvorfälle sowie die wirtschaftliche Zumutbarkeit der Maßnahmen zu berücksichtigen.

Die vom AN eingesetzten IT- und OT-Systeme sowie – sofern der AN für die gegenüber dem AG geschuldete Leistung künstliche Intelligenz verwendet – die in diesem Zusammenhang eingesetzten KI-Systeme müssen dem Stand der Technik entsprechen.

Der AN verpflichtet sich zur Einrichtung, Anwendung, Dokumentation und Aufrechterhaltung eines wirksamen Risikomanagementsystems für Informationssicherheit und Cybersicherheit und – soweit der AN KI einsetzt – auch für den KI-Einsatz und für auf KI beruhende Arbeitsergebnisse. Das Risikomanagementsystem muss insbesondere Risiken in der Informationssicherheit sowie der IT- und OT-Sicherheit und – bei KI-Einsatz – der Robustheit der eingesetzten KI-Systeme identifizieren, bewerten und steuern.

6.2.2 Konkrete Sicherheitsmaßnahmen

Die Maßnahmen müssen zumindest Folgendes umfassen:

a) Konzepte in Bezug auf Risikoanalyse und Sicherheit der Informationstechnik;

b) Bewältigung von Sicherheitsvorfällen;

c) Aufrechterhaltung des Betriebs (insb. Backup Management, Wiederherstellung nach Notfällen, Krisenmanagement);

d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern;

e) Sicherheitsmaßnahmen bei Erwerb, Entwicklung, Betrieb und Wartung informationstechnischer Systeme, Komponenten und Prozesse einschließlich Management und Offenlegung von Schwachstellen;

f) Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagement-Maßnahmen im Bereich der Sicherheit in der Informationstechnik;

g) grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik;

h) Konzepte und Prozesse für den Einsatz kryptographischer Verfahren;

i) Konzepte für die Sicherheit des Personals, Zugriffskontrolle und Verwaltung von IKT-Systemen (Informations- und Kommunikationstechnologie), Produkten und -Prozessen;

j) Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherter Sprach-, Video- und Textkommunikation sowie ggf. gesicherter Notfallkommunikationssysteme.

6.2.3 Sicherheit in der Lieferkette

Der AN ist verpflichtet, den AG unverzüglich über wesentliche Änderungen in der Lieferkette oder beim Hersteller zu informieren, soweit diese für die Informationssicherheit, Resilienz oder Leistungserbringung gegenüber dem AG relevant sein können. Dies gilt insbesondere für bekannt gewordene Sicherheitsrisiken, Schwachstellen oder sicherheitsrelevante Mängel der gelieferten Gegenstände oder Leistungen.

Soweit der AN Software, Firmware, vernetzte Komponenten oder digitale Services liefert oder betreibt, stellt er eine sichere Konfiguration, Wartung sowie die Behandlung von Sicherheitslücken nach dem Stand der Technik sicher und informiert den AG unverzüglich über kritische sicherheitsrelevante Updates oder Warnhinweise, soweit diese die Leistung oder den AG betreffen können. Der AN verpflichtet sich, dem AG eine Software Bill of Materials („SBOM“) der verwendeten Produkte und der in dieser verwendeten Software – einschließlich Applikationssoftware, Middleware, Bibliotheken und in physische Komponenten eingebetteter Software (Firmware) – vor Einbau und/oder Lieferung zur Verfügung zu stellen, soweit vom Hersteller bereitgestellt und rechtlich zulässig. Anderenfalls sind gleichwertige Nachweise über Herkunft, Integrität und Komponentenzusammensetzung zu erbringen.

Sicherheitsrelevante Änderungen der Leistung, insbesondere der Wechsel wesentlicher Hosting- oder Betriebsumgebungen, der Einsatz wesentlicher Nachunternehmer/Vorlieferanten mit Leistungs- oder Zugriffsbezug sowie die Einrichtung oder Änderung von Fernzugriffen, zeigt der AN dem AG vorab in Textform an, soweit dies zur Wahrung der Informationssicherheit oder Resilienz des AG erforderlich ist.

Darüber hinaus gibt der AN auf Verlangen Angaben zum Hersteller der gelieferten Gegenstände sowie zu deren Herkunft heraus.

Der AN informiert den AG außerdem unverzüglich über

a) Änderungen der bei ihm zum Einsatz kommenden Typen kritischer Komponenten,

b) Schwachstellen in eingesetzten IKT-Produkten, soweit für die Vertragserfüllung relevant, sowie

c) geplante wesentliche Änderungen an IT-Sicherheitsmaßnahmen, soweit leistungs-/sicherheitsrelevant.

Mitteilungen nach dieser Ziffer erfolgen unverzüglich, spätestens jedoch innerhalb von zwei Wochen ab Kenntnis der Änderung, soweit nicht eine frühere Information (insb. „vorab“) erforderlich ist. Bei Schwachstellen der Kategorie „kritisch“ (CVSS-Score 9.0 – 10.00) hat eine Meldung unverzüglich, spätestens innerhalb von 3 Stunden nach Kenntnis zu erfolgen. Bei Schwachstellen der Kategorie „hoch“ (CVSS-Score 7.0 – 8.9) – oder jeweils bei der entsprechenden Einordnung anhand einer gleichwertigen anerkannten Einstufungsmethodik – unverzüglich, spätestens innerhalb von 3 Tagen nach Kenntnis.

6.2.4 Schulung und Sensibilisierung

Die Geschäftsleitung des AN ist verpflichtet, die nach dieser Klausel zu ergreifenden Risikomanagement-Maßnahmen umzusetzen und ihre Umsetzung zu überwachen. Die Geschäftsleitung muss regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagement-Praktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen.

Der AN ist verpflichtet, grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik für seine Mitarbeitenden durchzuführen. Nachweise über durchgeführte Schulungen sind auf Verlangen des AG vorzulegen

6.2.5 Kryptographische Verfahren

Der AN ist verpflichtet, Konzepte und Prozesse für den Einsatz von kryptographischen Verfahren zu erstellen und umzusetzen. Bei der Übermittlung vertraulicher oder personenbezogener Daten sind angemessene kryptographische Verfahren nach dem Stand der Technik einzusetzen.

6.3 Besondere Anforderungen für kritische Anlagen

Für die IT-Leistungen, die maßgeblich auf die Funktionsfähigkeit der kritischen Anlagen des AG einwirken können, gelten über das allgemeine Schutzniveau hinausgehende Maßnahmen als verhältnismäßig, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Anlage steht.

6.3.1 Systeme zur Angriffserkennung

Der AN ist verpflichtet, für die IT-Leistungen, die für die Funktionsfähigkeit kritischer Anlagen maßgeblich sind, Systeme zur Angriffserkennung einzusetzen. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen. Dabei soll der Stand der Technik eingehalten werden.

Die vorstehenden Anforderungen gelten für kritische Lieferanten, die laufende IT- oder OT-Dienste erbringen, Fernzugriff auf Systeme des AG unterhalten oder Monitoring- und Betriebsleistungen für kritische Anlagen des AG ausführen. Für kritische Lieferanten, die ausschließlich digitale oder vernetzte Komponenten liefern und nach erfolgter Lieferung keinen laufenden Zugriff auf IT- oder OT-Systeme des AG haben, beschränkt sich die Pflicht nach dieser Ziffer auf den Betrieb von Systemen zur Angriffserkennung in der eigenen Entwicklungs- und Fertigungsinfrastruktur.

6.3.2 Kritische Komponenten

Der AN ist verpflichtet, vor dem Einsatz kritischer Komponenten im Sinne der jeweils geltenden gesetzlichen Regelungen, insbesondere des BSIG, die Zustimmung des AG einzuholen. Der AG wird dem AN innerhalb einer Frist von vier Wochen mitteilen, ob diese Komponenten verwendet werden dürfen. Etwaige schuldhafte Verzögerungen bei der Beantwortung durch den AG gehen nicht zulasten des AN. Der AN hat die bei ihm zum Einsatz kommenden Typen von kritischen Komponenten zu dokumentieren und dem AG auf Verlangen mitzuteilen. Der AN hat etwaige, sich aus der Eingruppierung der Komponenten nach den gesetzlichen Vorgaben ergebende Folgen, wie bspw. Kosten aufgrund notwendiger Cybersicherheitszertifizierungen selbst zu tragen.

Der AN hat bei der Auswahl von Herstellern kritischer Komponenten sicherheitsrelevante Gesichtspunkte zu berücksichtigen, insbesondere die Vertrauenswürdigkeit des Herstellers und alle sicherheitspolitischen Interessen der Bundesrepublik Deutschland, der Europäischen Union oder des Nordatlantikvertrags. Kritische Komponenten von Herstellern, deren Einsatz durch zuständige Behörden untersagt wurde, dürfen weder eingesetzt noch weiterverwendet werden. Der AG weist auf § 41 BSIG hin.

6.3.3 Vertrauenswürdigkeit und Mitwirkung

Der AN ist verpflichtet, den AG bei der Erfüllung seiner Mitwirkungspflichten gegenüber dem Bundesministerium des Innern nach § 41 Abs. 5 BSIG zu unterstützen und auf Anforderung alle für das Verfahren erheblichen Tatsachen vollständig und wahrheitsgemäß mitzuteilen sowie bekannte Beweismittel anzugeben. Zur Vorbereitung dieser Mitwirkung hat der AN dem AG auf Verlangen, spätestens jedoch innerhalb von vier Wochen nach Aufforderung, Auskunft zu erteilen über:

a) seine unmittelbare und mittelbare Eigentümerstruktur, insbesondere über staatliche oder staatsnahe Beteiligungen oder Einflussrechte von Stellen aus Drittstaaten sowie über eine etwaige Verpflichtung des AN oder des Herstellers zur Zusammenarbeit mit staatlichen Stellen oder Streitkräften eines Drittstaates;

b) etwaige behördliche Maßnahmen oder Ermittlungsverfahren gegen den AN oder den Hersteller der gelieferten Komponenten, die einen Bezug zur Informationssicherheit oder zur öffentlichen Sicherheit haben;

c) sonstige Umstände, die nach den Kriterien des § 41 Abs. 4 BSIG für die Beurteilung der Vertrauenswürdigkeit des AN oder des Herstellers relevant sein könnten.

Der AN ist verpflichtet, den AG unverzüglich textförmlich zu informieren, wenn sich die vorstehend genannten Umstände nach Vertragsschluss wesentlich ändern.

Der AN darf im Rahmen der Leistungserbringung keine kritischen Komponenten im Sinne von § 2 Nr. 23 BSIG einsetzen, deren Einsatz vom BSI nach § 41 BSIG gegenüber dem AG untersagt wurde oder für die eine entsprechende Allgemeinverfügung nach § 41 Abs. 2 BSIG ergangen ist.

6.4 Nachweise und Überprüfungen

Die Einhaltung der Verpflichtungen ist durch den AN angemessen zu dokumentieren und dem AG auf Verlangen nachzuweisen. Näheres regeln die nachfolgenden Bestimmungen.

6.4.1 Nachweispflichten

Der AN weist die Einhaltung und Umsetzung dieser Sicherheitsanforderungen durch Sicherheitsaudits, Prüfungen oder Zertifizierungen nach und übermittelt dem AG auf Verlangen die Ergebnisse einschließlich Angaben über festgestellte Sicherheitsmängel. Der AN hat den AG unverzüglich zu informieren, wenn eine bestehende Zertifizierung entzogen, ausgesetzt oder nicht verlängert wurde. In diesem Fall ist der AG berechtigt, nach erfolgloser Fristsetzung zur Wiederherstellung des zertifizierten Zustands das Vertragsverhältnis aus wichtigem Grund zu kündigen.

Bei Sicherheitsmängeln kann der AG die Vorlage eines geeigneten Mängelbeseitigungsplans, die Beseitigung der Mängel sowie einen geeigneten Nachweis über die erfolgte Mängelbeseitigung verlangen.

Der AN ist ferner verpflichtet, den AG bei der Erfüllung seiner Nachweispflichten gegenüber dem BSI nach § 39 BSIG zu unterstützen und die hierzu erforderlichen Unterlagen, Zertifizierungen und Auskünfte unverzüglich bereitzustellen.

6.5 Kontroll- und Prüfrechte

Der AG ist berechtigt, die Umsetzung und Einhaltung dieser Sicherheitsanforderungen in angemessenem Umfang im Rahmen eines Audits beim AN zu überprüfen. Ein solches Audit kann als reguläres Audit oder als Notfall-Audit unter den jeweils nachfolgend definierten Voraussetzungen erfolgen. Der Informationssicherheitsbeauftragte des AG ist berechtigt, das Audit entweder selbst, durch Vertreter des AG oder durch einen qualifizierten unabhängigen Dritten nach anerkannten Standards zu den marktüblichen Konditionen vorzunehmen (nachfolgend einheitlich „AG“). Der Umfang des Audits ist inhaltlich durch den ISO 27001 Annex A sowie einschlägigen OT-Sicherheitsstandards, insbesondere IEC 62443, soweit der Dienstleister OT-relevante Leistungen erbringt und standortspezifisch durch die Liste der Standorte des Dienstleisters begrenzt, die Daten des AG verarbeiten. Für kritische Lieferanten, die ausschließlich digitale oder vernetzte Komponenten liefern, ohne nach erfolgter Lieferung laufenden Zugriff auf IT- oder OT-Systeme des AG zu haben, beschränkt sich der Auditumfang auf sicherheitsrelevante Aspekte des Entwicklungs-, Fertigungs- und Lieferprozesses sowie das Schwachstellenmanagement für die gelieferten Komponenten. Das Notfall-Audit findet in diesen Fällen nur statt, wenn ein

sicherheitsrelevanter Defekt oder eine Schwachstelle der gelieferten Komponente Auslöser des Sicherheitsvorfalls ist. Der Austausch von Informationen im Rahmen eines Audits hat zwingend über die im Zuge des Audits durch den AG genannten Kontaktdaten zu erfolgen. Prüfergebnisse sind vertraulich zu behandeln. Sofern sich der AG eines Dritten bedient, wird der AG den Dritten zu gleichwertiger Vertraulichkeit verpflichten, der er selbst unterliegt.

6.5.1 Reguläres Audit

Reguläre Audits konzentrieren sich insbesondere auf die Einhaltung der geforderten Anforderungen zur IT- und ggf. OT-Sicherheit (zur OT-Sicherheit, sofern der AN OT-relevante Leistungen erbringt), bspw. Überprüfung der Aktualität und Wirksamkeit eines ggf. einzurichtenden Informationssicherheitsmanagementsystems und dessen Umsetzung durch den AN. Der AG hat das Recht, maximal ein Mal pro Jahr ein reguläres Audit beim AN durchzuführen. Das reguläre Audit kann jederzeit von AG mit einer Vorankündigung von mindestens vier Wochen beim AN, vor dem jeweils gewünschten Termin durchgeführt werden. Für die Ankündigung des regulären Audits ist eine textförmliche Nachricht (z. B. E-Mail) an den AN ausreichend.

Für Verträge, bei denen der AN Zugang zu oder Einfluss auf die IT- oder OT-Systeme oder sicherheitsrelevante Betriebsdaten des AG hat oder haben kann und bei denen Zugang oder Einfluss für einen Zeitraum von nicht mehr als zwölf Monaten bestehen oder bestehen können („einmalige Verträge“), tritt an die Stelle des jährlichen Auditrechts ein einmaliges Prüfungsrecht des AG. Dieses kann ab Beginn der Leistungserbringung bis zu sechs Monate nach deren Abschluss ausgeübt werden. Die Ankündigungsfrist von vier Wochen gilt entsprechend. Beträgt der Einfluss-Zeitraum weniger als acht Wochen, reduziert sich die Ankündigungsfrist auf zwei Wochen. Das Prüfungsrecht nach diesem Absatz erstreckt sich auf die Prozesse, Systeme und Maßnahmen des AN, die für die Erfüllung seiner Verpflichtungen aus diesen Sicherheitsanforderungen im Zusammenhang mit dem konkreten Auftrag relevant sind, unabhängig davon, ob die Leistungserbringung zum Zeitpunkt der Auditdurchführung bereits abgeschlossen ist. Stellt sich nach Vertragsschluss heraus, dass der Einfluss-Zeitraum zwölf Monate überschreitet oder zu überschreiten droht, hat der AN den AG unverzüglich in Textform zu informieren. Ab diesem Zeitpunkt gilt das jährliche Auditrecht. Ein jährliches Auditrecht steht dem AG auch dann zu, wenn der AN auf Grundlage mehrerer einmaliger Verträge oder auf Basis eines Rahmenvertrags mit mehreren Einzelabrufen tätig wird und der Einfluss-Zeitraum berechnet aus den Summen der einzelnen Zeiträume insgesamt zwölf Monate überschreitet. Ein in dem betreffenden Kalenderjahr bereits ausgeübtes einmaliges Audit wird angerechnet. Unterbrechungen zwischen mehreren Verträgen oder zwischen mehreren Einzelabrufen mit demselben AN von weniger als sechs Monaten bleiben bei der Berechnung des Einfluss-Zeitraums außer Betracht.

Das nachfolgend beschriebene Notfall-Audit bleibt in allen Fällen unberührt.

Die Ankündigung des AG zur Durchführung eines regulären Audits enthält zur Information des AN den Prüfungsumfang, die Rollen und die Namen der Prüfer. Maßgeblicher Prüfungsmaßstab ist die ISO-27000-Familie sowie der zum Zeitpunkt des Audits anerkannte Stand der Technik, konkretisiert durch die einschlägigen BSI-Grundschutz-Standards und europäischen Normen (insb. ENISA-Leitlinien).

Reguläre Audits des AG orientieren sich an ISO 27006/7 und ISO 19011. Der AN ist entsprechend verpflichtet, den AG bei der Durchführung eines regulären Audits zu unterstützen, insbesondere durch den Zugang und eine Vor-Ort-Betreuung, die Bereitstellung der vom AG geforderten und für die Überprüfung erforderlichen Informationen und/oder die Bereitstellung von lokalen Kontakten für den AG und/oder designierten Partnern. Vom AG angeforderte Ressourcen werden mit einer Frist von maximal zwei Wochen nach der Anforderung durch den AG vom AN bestätigt und bereitgestellt (bspw. angefragte Dokumentationen zur Auditvorbereitung). Für die Anforderung von Ressourcen ist eine textförmliche Nachricht (z. B. E-Mail) an den AN ausreichend.

Die Kosten der Prüfung zu marktüblichen Konditionen trägt der AN bis zu einem Betrag von 7.500 € pro Prüfung. Darüber hinausgehende Kosten trägt der AG. Sofern es sich ergibt, dass der AN gegen seine Verpflichtungen dieser Sicherheitsanforderungen in erheblichem Umfang verstoßen hat und dieser Verstoß dem Verantwortungsbereich des AN zuzurechnen ist, trägt der AN die Kosten des Audits in vollem Umfang.

Der AG stellt dem AN den vorläufigen Auditbericht innerhalb von zwei Wochen nach Erhalt zur Verfügung. Der AN erhält die Möglichkeit, den vorläufigen Auditbericht innerhalb von zwei Wochen zu kommentieren oder Fehler zu rügen.

Dem AN wird die Möglichkeit eingeräumt, das reguläre Audit durch einen von ihm benannten, für diese Tätigkeiten qualifizierten Dritten (bspw. nachgewiesen durch entsprechende Zertifizierungen) durchführen zu lassen. Der AN hat den AG – wenn er von dieser Möglichkeit Gebrauch macht – innerhalb von zwei Wochen nach Mitteilung über die Durchführung des regulären Audits zu informieren. Das Ergebnis des Audits muss dem AG innerhalb von zwei Wochen nach dem ursprünglich geplanten Termin unaufgefordert vorgelegt werden. Der ausführliche Bericht erfolgt innerhalb von vier Wochen nach dem ursprünglich geplanten Termin. Sollte der AN dieser Pflicht nicht nachkommen, steht dem AG das Recht zur Durchführung des regulären Audits zu, ohne dass der AN dieses für diesen Fall abwenden kann.

Abwendungsbefugnis

Der AN kann das Recht des AG zur Durchführung eines regulären Audits nach dieser Ziffer für das betreffende Kalenderjahr abwenden, indem er dem AG bis spätestens zum 31. März des jeweiligen Kalenderjahres einen Auditbericht vorlegt, der die nachfolgenden Voraussetzungen kumulativ erfüllt (nachfolgend „Substitutionsaudit“):

a) Das Substitutionsaudit wurde von einem unabhängigen, fachkundigen Dritten durchgeführt, der über eine anerkannte Zertifizierung als IT-Sicherheitsauditor verfügt (z. B. zertifizierter ISO/IEC 27001 Lead Auditor, CISA oder gleichwertig) und weder mit dem AN noch mit dem AG in einem Interessenkonflikt steht. Der AG ist berechtigt, den Auditor bei nachweisbarem Interessenkonflikt oder fehlender Qualifikation abzulehnen;

b) das Substitutionsaudit ist zum Zeitpunkt der Vorlage nicht älter als drei Monate;

c) es deckt inhaltlich mindestens denselben Prüfungsumfang ab wie ein reguläres Audit nach dieser Ziffer. Verbleibende Lücken im Prüfungsumfang gehen zu Lasten des AN;

d) der vollständige Bericht einschließlich sämtlicher festgestellter Mängel, Abweichungen und Maßnahmenempfehlungen wird dem AG ungeschwärzt vorgelegt;

e) der AN legt zusammen mit dem Bericht eine aktuelle Erklärung vor, aus der hervorgeht, welche der im Bericht empfohlenen Maßnahmen bereits umgesetzt sind und welche mit verbindlichem Umsetzungszeitplan noch in Bearbeitung sind.

Der AG teilt dem AN seine Entscheidung über die Anerkennung des Substitutionsaudits innerhalb von vier Wochen nach vollständiger Vorlage in Textform mit. Erkennt der AG das Substitutionsaudit als anforderungskonform an, beschränkt sich sein Auditrecht für das betreffende Kalenderjahr auf ein gezieltes Restaudit hinsichtlich derjenigen Bereiche, die das Substitutionsaudit nicht oder nicht vollständig abdeckt oder bei denen der AG aufgrund des Berichts konkrete Anhaltspunkte für fortbestehende Sicherheitsdefizite hat.

Legt der AN das Substitutionsaudit nicht bis zum 31. März des jeweiligen Kalenderjahres vor oder erfüllt der vorgelegte Bericht die Voraussetzungen nach lit. (a–e) nicht, steht dem AG das uneingeschränkte Auditrecht nach dieser Ziffer zu.

Für einmalige Verträge, bei denen der mögliche Einfluss-Zeitraum acht Wochen oder länger beträgt, gilt die vorstehende Abwendungsbefugnis mit folgenden Maßgaben:

An die Stelle der Vorlagefrist bis zum 31. März tritt eine Frist von vier Wochen ab Beginn der Leistungserbringung. Legt der AN das Substitutionsaudit innerhalb dieser Frist vor, entfällt das einmalige Prüfungsrecht des AG mit der Maßgabe, dass dem AG ein Restauditrecht entsprechend den Regelungen der vorstehenden Regelung verbleibt. Im Übrigen gelten die Voraussetzungen nach lit. (a–e) und die Kostentragungsregelungen unverändert. Beträgt der mögliche Einfluss-Zeitraum weniger als acht Wochen, findet die Abwendungsbefugnis keine Anwendung.

Das Abwehrrecht nach diesem Absatz findet keine Anwendung auf das nachfolgend beschriebene Notfall-Audit.

Die Kosten des Substitutionsaudits trägt der AN. Die Kosten eines Restaudits trägt der AG, es sei denn, das Restaudit ergibt, dass der AN gegen seine Verpflichtungen dieser Sicherheitsanforderungen verstoßen hat oder das Substitutionsaudit die betreffenden Bereiche nachweislich nicht oder nicht vollständig abgedeckt hat. In diesem Fall trägt der AN die Kosten des Restaudits bis zu einem Betrag von 7.500,00 €.

6.5.2 Notfall-Audit

Notfall-Audits finden anlässlich eines erheblichen Sicherheitsvorfalls im Sinne von § 2 Nr. 11 BSIG – worunter auch Vorfälle mit kombinierter (cyber-physischer) Wirkung fallen können – beim AN statt. Der AG ist bei einem erheblichen Sicherheitsvorfall berechtigt, Notfall-Audits unverzüglich, zu den üblichen Geschäftszeiten, jedoch ohne Vorankündigung beim AN durchzuführen.

Der Umfang des vom Auftraggeber durchzuführenden Notfall-Audits richtet sich nach den Erfordernissen zur Aufklärung des Vorfalls beim AN und kann vom Auftraggeber im Verlauf des Notfall-Audits abhängig vom Schweregrad und Tragweite des Vorfalls dynamisch verändert und auf Bereiche ausgedehnt werden, die in einem nachvollziehbaren sachlichen Zusammenhang mit dem erheblichen Sicherheitsvorfall stehen. Der AG oder der beauftragte Dritte führt Notfall-Audits mit der Zielsetzung durch, die folgenden Fragestellungen zu klären:

1) Was ist passiert, inkl. wann und wie lange?

2) Wie konnte dieses Ereignis eintreten?

3) Was ist der Umfang und wer sind die Betroffenen?

4) Welche temporären Schutzmaßnahmen wurden getroffen?

5) Wie wird ein solches Ereignis für die Zukunft ausgeschlossen?

Der AN ist verpflichtet, an der Aufklärung der vorstehenden Fragestellungen mitzuwirken. Insbesondere wird der AN hierfür Anfragen vom Auftraggeber innerhalb einer Frist von maximal 24 Stunden beantworten und angeforderte Ressourcen und Hilfestellungen gewähren (bspw. Zutritt und Support vor Ort, die Bereitstellung von angeforderten Informationen oder das zur Verfügung stellen von Ansprechpartnern gegenüber AG oder benannten Partnern).

Die Kosten des Notfall-Audits trägt der AN, sofern das Audit ergibt, dass der Sicherheitsvorfall dem Verantwortungs- oder Risikobereich des AN zuzurechnen ist. In allen übrigen Fällen trägt der AG die Kosten.

7 Physische Resilienz und KRITISDachG

Soweit der AN Leistungen an Standorten oder Anlagen des AG erbringt oder diese physisch beeinflussen kann, hat er angemessene Maßnahmen zur physischen Sicherheit zu beachten und umzusetzen. Hierzu zählen insbesondere die Einhaltung von Zutrittskontroll- und Identitätsprüfungsanforderungen, Begleit- und Bereichsbeschränkungsvorgaben, der gesicherte Umgang mit Arbeitsmitteln, Datenträgern und Zugangsmitteln sowie die Einhaltung etwaiger Fotografier- und Dokumentationsverbote.

Der AN informiert den AG unverzüglich in Textform über Umstände, die im Rahmen der Leistungserbringung eintreten oder bekannt werden und für die Erfüllung der Melde- und Resilienzpflichten des AG als Betreiber kritischer Anlagen nach dem KRITISDachG relevant sein könnten. Er stellt dem AG die hierfür erforderlichen Informationen auf Anforderung unverzüglich bereit.

Soweit ein Vorfall sowohl physische als auch informationstechnische Bezüge aufweist (cyber-physischer Vorfall), gelten vorrangig die Meldepflichten nach Ziff. 4.2 die Anforderungen dieser Ziffer bleiben daneben anwendbar.

Detaillierte Anforderungen zur physischen Resilienz werden gesondert geregelt.

8 Weitergabepflicht in der Lieferkette

8.1 Grundsatz

Der AN ist verpflichtet, eigenen Auftragnehmern („Subunternehmer“) die Sicherheitsanforderungen des AG aufzuerlegen, soweit dies die Leistungserbringung gegenüber dem AG betrifft. Die Regelungen aus Ziff. 6 sind auf solche Subunternehmer entsprechend zu übertragen, soweit es sich bei diesen um nachgelagerte kritische Lieferanten handelt. Unter nachgelagerten kritischen Lieferanten sind solche Subunternehmer zu verstehen, die als kritische Lieferanten im Sinne von Ziff. 1.6.1 anzusehen wären, würden sie ihre Leistung unmittelbar gegenüber dem AG erbringen. Meldepflichten nach Ziffer 4.2 sind mit der Maßgabe weiterzugeben, dass Meldungen an den AN zu richten sind, der sie unverzüglich an den AG weiterzuleiten hat. Der AN bleibt gegenüber dem AG für die Einhaltung dieser Sicherheitsanforderungen uneingeschränkt verantwortlich, unabhängig davon, inwieweit er Leistungen durch nachgelagerte kritische Lieferanten erbringen lässt.

8.2 Überprüfung in der Lieferkette

Der AN stellt sicher, dass die Einhaltung der nach Ziff. 8 weitergereichten Pflichten durch nachgelagerte kritische Lieferanten im Rahmen des Audits in der Lieferkette nach Ziff. 6.5 überprüfbar ist. Er ist verpflichtet, dem AG auf Verlangen gleichwertige Nachweise über die Einhaltung der weitergereichten Pflichten durch nachgelagerte kritische Lieferanten beizubringen. Kann der AN solche Nachweise nicht erbringen, gilt dies als Pflichtverletzung des AN gegenüber dem AG.

8.3 Kaskadierende Weitergabe

Der AN ist verpflichtet, in den Verträgen mit den Subunternehmern zu vereinbaren, dass diese ihrerseits gleichwertige Weitergabepflichten gegenüber ihren eigenen Subunternehmern und Vorlieferanten übernehmen. Die Weitergabepflicht kaskadiert über alle Ebenen der Lieferkette.

8.4 Dokumentation

Der AN dokumentiert fortlaufend, welche seiner Subunternehmer und Vorlieferanten als nachgelagerte kritische Lieferanten eingestuft sind, und legt diese Dokumentation dem AG auf Verlangen innerhalb von 4 Wochen vor.

9 Einschränkung zu übermittelnder Daten

Informationen Dritter dürfen nur offengelegt werden, soweit rechtlich zulässig. Im Übrigen sind sie nach dem Need-to-know-Prinzip zu anonymisieren oder zu schwärzen.