Informationssicherheitsanforderungen an Lieferanten und Dienstleister der Unternehmensgruppe Stadtwerke Bielefeld

(bestehend aus: Stadtwerke Bielefeld GmbH, moBiel GmbH, BBF Bielefelder Bäder und Freizeit GmbH, BITel Gesellschaft für Telekommunikation mbH, Bielefelder Netz GmbH, Interargem GmbH, MVA Bielefeld –Herford GmbH und der Enertec Hameln GmbH)

1 Generelle Verantwortlichkeit

Der Auftragnehmer trägt die Verantwortung dafür, dass er sämtliche durch den Auftraggeber in diesem Dokument festgelegten Anforderungen und Vorgaben einhält. Hierzu zählt insbesondere seine Verpflichtung, im Rahmen seiner Leistungserbringung für die Unternehmen der Unternehmensgruppe Stadtwerke Bielefeld die jeweils gültigen rechtlichen Vorgaben sowie die jeweils aktuellen Standards zur Informationssicherheit zu beachten und angemessen zu berücksichtigen.

Ziel dieser Lieferantenverpflichtung ist es sicherzustellen, dass der Auftragnehmer Produkte liefert und Dienstleistungen erbringt, die die Integrität, der Vertraulichkeit, der Verfügbarkeit, der Authentizität und der Belastbarkeit aller im Kontext der Leistungserbringung und des Schutzes des eigenen Unternehmens relevanten, schutzbedürftigen Informationen und Systeme des Auftraggebers (nachfolgend „Schutzziele“ genannt) nicht beeinträchtigen.

2 Gewährleistung eines dem Leistungsgegenstand angemessenen Informationssicherheitsniveaus

Der Auftragnehmer ist verpflichtet, alle im Kontext der Leistungserbringung für den Auftraggeber relevanten Informationen und Systeme nach dem jeweils aktuellen

Stand der Technik gegen unberechtigten Zugriff, Veränderung, Zerstörung und sonstigen Missbrauch zu sichern, um die Leistungserbringung sicherzustellen.

Dabei trifft der Auftragnehmer geeignete und angemessene technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau hinsichtlich der Schutzziele zu gewährleisten.

Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zum Risiko des Nichterreichens der Schutzziele steht.

Der Auftragnehmer verfolgt dabei einen kontinuierlichen Verbesserungsprozess, d.h. er überprüft ständig alle Einflussparameter mit dem Ziel, sein Sicherheitsniveau zu verbessern.

2.1 Stufe 1: Informationssicherheits-Nachweis (Basisanforderungen)

- Je nach Art und Schutzbedarf der Informationen bzw. der Bedeutung der Leistungen des Auftragnehmers für den Geschäftsbetrieb des Auftraggebers kann der Auftraggeber vom Auftragnehmer ein besonderes Maß an Sicherungsmaßnahmen sowie einen geeigneten Nachweis über ein angemessenes Informationssicherheitsniveau im Betrieb des Auftragnehmers verlangen, insbesondere durch Vorlage geeigneter Zertifikate[1].
- Der Auftragnehmer sichert unabhängig von vorgenannten Nachweisen zu, dass
  - in seiner Organisation alle erforderlichen Rollen, Verantwortlichkeiten und Kompetenzen mit Bezug zur Informationssicherheit festgelegt und bekannt sind,
  - bezüglich der **Zugangssteuerung** in seiner Organisation mindestens folgende Maßnahmen etabliert sind:
    - Dokumentierte Freigabeprozesse für Berechtigungen auf Systeme und Informationen
    - Prozesse zur zeitnahen Löschung von Zugriffsrechten bei Austritt oder Abteilungswechsel
    - Angemessene Authentisierungsverfahren mit angemessener Passwortkomplexität und -gültigkeit und höheren Anforderungen an administrative Zugänge
    - Automatische Bildschirmsperre nach Inaktivität
    - Jederzeitige (auch spätere) eindeutige Nachvollziehbarkeit der Identität der Person, die zu einem bestimmten Zeitpunkt einen Zugang genutzt hat.
  - alle im Rahmen der Leistungserbringung eingesetzten Beschäftigten bezüglich der zu beachtenden Aspekte der Informationssicherheit sensibilisiert und unterwiesen wurden und entsprechende Lernzielkontrollen den Erfolg der Maßnahmen bestätigten.
  - alle im Rahmen der Leistungserbringung eingesetzten Mitarbeiter eine **Verpflichtungserklärung** zur Einhaltung der Vorgaben zur Informationssicherheit und zur Wahrung der **Vertraulichkeit** unterzeichnet haben, die soweit

[1] z.B. ISO/IEC 27001, IT-Grundschutz, ISIS12 etc.

gesetzlich zulässig auch über das Ende ihres Beschäftigungsverhältnisses hinaus fortbesteht.

- angemessene und ausreichende Vorkehrungen zur physischen Sicherheit aller für die Leistungserbringung erforderlichen, schutzbedürftigen Informationen und Systeme getroffen wurden (sowohl bei stationärer Verarbeitung als auch beim Transport), insbesondere hinsichtlich
  - elementarer Gefährdungen (Feuer, Wasser, Blitz, Sturm, Katastrophen etc.),
  - höherer Gewalt (Temperatur, Feuchte, Korrosion, sonstige Umwelteinflüsse etc.),
  - technischem Versagen (Ausfall Versorgungseinrichtungen etc.) und
  - vorsätzlichen Handlungen (Einbruch, Sabotage, Diebstahl etc.).

- der **Zutritt** zu Bereichen mit schutzbedürftigen Informationen oder Systemen jeweils nur auf einen autorisierten, besonders vertrauenswürdigen Personenkreis beschränkt ist.

- nicht mehr benötigte schutzbedürftige Informationen und Datenträger in einer Form **gelöscht** bzw. **vernichtet** werden, dass ausgeschlossen ist, dass gelöschte bzw. vernichtete Daten von Dritten unautorisiert wiederhergestellt werden können.

- angemessene DV-technische Sicherheitsmaßnahmen zum Schutz aller für die Leistungserbringung erforderlichen, schutzbedürftigen Informationen und Systeme getroffen wurden, insbesondere durch
  - den Einsatz von geeigneten Firewalls und aktueller Virenschutz-Software
  - den Einsatz ausschließlich von der Organisation geprüfter und freigegebener Hard- und Software
  - aktuelles Patch-Management
  - geeignete System-Härtung
  - angemessene Authentisierungs-Maßnahmen
  - geprüfte Datensicherungs- und Wiederherstellungs-Mechanismen

- ein Inventar- / Wertverzeichnis aller schutzbedürftigen Informationen und Systeme, die für die Leistungserbringung relevant sind, vorliegt und in der Organisation bekannt ist.

- **Schwachstellen Management**
  Der Auftragnehmer hat alle Aspekte seiner Leistungserbringung einer kontinuierlichen Prüfung auf Schwachstellen zu unterziehen und so schnell wie möglich auf neu erkannte Schwachstellen zu reagieren.

  Hierzu sichtet er kontinuierlich Quellen für Sicherheitsempfehlungen und bewertet diese hinsichtlich der gegenüber dem Auftraggeber zu erbringenden Leistungen.

  Der Umfang der Prüfung hat jede potenzielle Schwachstelle zu umfassen, die Einfluss auf die Schutzziele sowohl des Auftraggebers als auch des Auftragnehmers hat oder haben kann.

- **Meldungen**
  Der Auftragnehmer ist verpflichtet, Sicherheitsvorfälle in seiner Organisation, die

Einfluss auf die Schutzziele sowohl des Auftraggebers als auch des Auftragnehmers haben oder haben können, unverzüglich in Textform an den Auftraggeber zu melden.

Der Auftragnehmer hat dem Auftraggeber jegliche Abweichungen von den in diesem Kapitel vereinbarten Sicherheitsanforderungen unverzüglich in Textform zu melden und mit diesem den weiteren Umgang abzustimmen.

- **Audit**
  Der Auftraggeber ist berechtigt, sich jederzeit vor und während der Leistungserbringung in angemessener Weise die Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in der Vereinbarung festgelegten Verpflichtungen seitens des Auftragnehmers nachweisen zu lassen.

  Der Auftragnehmer ermöglicht hierzu dem Auftraggeber auf Verlangen, sich auch vor Ort von der Einhaltung der Verpflichtungen und Zusicherungen zu überzeugen. Der Auftragnehmer hat die Untersuchungen, wie Audits oder Penetrationsanalysen des Auftraggebers unentgeltlich zu unterstützen und Mitwirkungsleistungen, wie Auskünfte oder Einsichtnahme in die gespeicherten Informationen und Daten, zu erbringen, soweit dies für das Audit erforderlich ist.

  Der Auftraggeber ist berechtigt sich nach rechtzeitiger Anmeldung während der üblichen Geschäftszeiten und, soweit möglich und zumutbar, ohne Störung der betrieblichen Abläufe auch in den Betriebsstätten des Auftragnehmers einschließlich der IT-Systeme von der Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen überzeugen.

  Der Auftraggeber ist berechtigt, die Audits durch ein externes, gegenüber Dritten zur Verschwiegenheit verpflichtetes und qualifiziertes Unternehmen durchführen zu lassen. Hierbei darf es sich jedoch nicht um einen Mitwettbewerber im Rahmen der Leistungserbringung handeln. Gesetzliche Kontroll- und Auskunftsrechte des Auftraggebers werden hierdurch weder eingeschränkt noch ausgeschlossen.

  Der Auftraggeber übermittelt dem Auftragnehmer zeitnah den Auditbericht.

  Der Auftragnehmer erhält anschließend Gelegenheit, Stellung zu festgestellten Unregelmäßigkeiten zu nehmen und Vorschläge zum weiteren Umgang zu unterbreiten. Falls der Auftraggeber diesen Vorschlägen nicht zustimmt, ist der Auftragnehmer zur Nachbesserung verpflichtet.

2.2 Stufe 2 Ergänzende Anforderungen bei Leistungen mit IT-Bezug

Über die unter 3.1. definierten Basisanforderungen der Stufe 1 hinaus sind im Falle der Erbringung vertraglicher Leistungen mit IT-Bezug zusätzlich folgende Anforderungen vom Auftragnehmer zu erfüllen:

- **Schwachstellen Management**
  Der Auftragnehmer ist verpflichtet, jede erkannte Schwachstelle unverzüglich in Textform an den Auftraggeber zu melden.

- **Meldungen**
  Der Auftragnehmer hat im Falle eines Sicherheitsvorfalls unentgeltlich Ressourcen zur Minderung und/oder Beseitigung der Auswirkungen des Vorfalls sowie die finalen Analyse-Ergebnisse in Form eines Ursachen- und Korrekturberichts bereitzustellen.

- **Fernzugang**
  Fernzugänge zu Netzwerken des Auftraggebers werden ausschließlich vom Auftraggeber gesteuert und sind nur unter folgenden Bedingungen gestattet:

  - Der Auftragnehmer stellt sicher, dass bei Fernzugängen die Schutzziele im Umgang mit den (materiellen und immateriellen) Vermögenswerten des Auftraggebers jederzeit gewährleistet sind. Dies beinhaltet auch die nachträgliche Verwendung von Informationen, von denen der Auftragnehmer während eines Fernzugriffes Kenntnis erlangt hat. Der Auftragnehmer ist für alle Aktionen und Vorgänge, die unter Verwendung der ihm zur Verfügung gestellten Benutzerkonten mit Fernzugangsfunktion ausgelöst oder durchgeführt werden, verantwortlich.
  - Grundsätzlich hat der Auftragnehmer jedem Nutzer ein eigenes Benutzerkonto zur Verfügung zu stellen. Ausnahmen von dieser Regel sind begründet vorab mit dem Auftraggeber abzustimmen.
  - Wird vom Auftragnehmer ein Nutzerkonto nicht mehr benötigt, ist der Auftraggeber umgehend darüber zu informieren, so dass das entsprechende Konto gesperrt werden kann.
  - Der Auftragnehmer hat Nutzerkonten mit Fernzugangsfunktion mindestens alle sechs Monate zu überprüfen und den Auftraggeber über eventuell notwendige Änderungen zu informieren. Dabei hat er die mit dem Auftraggeber vereinbarten bzw. von diesem vorgegebenen Authentisierungsverfahren zu beachten.

- **Einsatz kryptographischer Absicherungen**
  Der Auftragnehmer stellt sicher, dass eine kryptographische Absicherung der Kommunikation und Ablage überall dort erfolgt, wo es notwendig oder vom Auftraggeber vorgegeben ist. Der Einsatz der kryptographischen Absicherung der Kommunikation ist insbesondere dann notwendig, wenn Informationen mit hohem Schutzbedarf (z.B. Steuerungsdaten der Kritischen Infrastruktur oder vertrauliche Daten) über öffentliche oder als nicht ausreichend sicher anzusehende Netzwerke übertragen werden.

  Der Auftragnehmer ist verpflichtet, von ihm im Rahmen der Leistungserbringung eingesetzte Kryptographielösungen in seinem Schwachstellen-Management (s.o.) zu berücksichtigen und hinsichtlich ihres Sicherheitsniveaus zu bewerten. Bei seinen Einschätzungen hat er sich an der BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen zu orientieren.

- **Release- und Patch-Management**
  Der Auftragnehmer stellt sicher, dass alle oben genannten Komponenten vor der Abnahme gepatcht und aktualisiert werden. Der Patch-Level sollte dabei nicht älter als 12 Monate ab dem Tag der Systemabnahmeerklärung sein. Abweichungen von dieser Vorgabe sind nur mit Zustimmung des Auftraggebers möglich. Der Auftragnehmer muss alle öffentlich verfügbaren und durch den Auftraggeber freigegebenen Patches als Teil der Lieferung installieren.

Über sicherheitsrelevante Updates und Patches hat der Auftragnehmer den Auftraggeber umgehend zu informieren und diese umgehend bereitzustellen. Im Übrigen ist der Auftragnehmer verpflichtet, mindestens einmal pro Jahr Updates und Patches bereitzustellen.

Der Auftragnehmer stellt dem Auftraggeber für jede im Patchzyklus adressierte Schwachstelle einen Bericht in Textform zur Verfügung, der Auskunft über die jeweils möglichen Gefährdungen der Schutzziele gibt.

Falls der Drittanbieter eines Betriebssystems oder einer anderen Komponente (Software, Datenbanken, Anwendungen etc.), die entweder im Leistungsumfang inkludiert ist oder vom Auftragnehmer für seine Leistungserbringung vorausgesetzt wurde, das Ende des Lifecycles verkündet, ist vom Auftragnehmer sicherzustellen, dass die Anforderungen des Auftraggebers weiterhin erfüllt werden (z.B. weitere Funktionsfähigkeit der Systeme, keine Einschränkungen der Leistungserbringung des Auftraggebers etc.).

In Fällen, in denen der Auftragnehmer nur Anwendungen und / oder andere Funktionalitäten liefert und der Auftraggeber oder sonstige Drittanbieter in seinem Namen für das Update-Management auf den darunterliegenden Schichten wie Betriebssystem verantwortlich ist, gewährleistet der Auftragnehmer eine kontinuierliche Funktionsfähigkeit seiner gelieferten Leistung auch bei Patches der ggf. darunterliegenden Systemplattform.

Das Release- Patch-Management umfasst:

- Betriebssystem
- Alle Softwarepakete und Services, die Teil des Betriebssystems sind
- Alle Tools und Applikationen, die der Hersteller zu Betriebs- und Wartungszwecken installiert hat
- Zielapplikation (Servicelogik)
- Alle Middleware-Application-Layer, Datenbanken, Access-, Monitoring- oder Applikationsserver, die für den Service genutzt werden
- Frühzeitige Information über neuartige Produkte, Funktionen und Technologien
- Auf Anfrage konkrete Informationen über die Produktentwicklung der sicherheitsrelevanten Systemanteile seiner Produkte geben.

- **Systemhärtung**
  Der Auftragnehmer verpflichtet sich, die von ihm gelieferten Systeme (bereits vor der Systemabnahme) zu härten, um die Auswirkungen potenzieller Sicherheitsrisiken zu minimieren.

  Es ist dem Auftragnehmer gestattet, zwecks Umsetzung der erforderlichen Systemhärtung folgende Komponenten zu installieren / zu konfigurieren:

- Jede Komponente, die für die Anwendung oder nach der Logik des Dienstes benötigt wird
- Jede aus der Integration mit anderen Services resultierende andere Anwendung oder Komponente
- Jede aus Betriebs- und Wartungsanforderungen resultierende Komponente

Jede andere Komponente darf nur nach vorheriger ausdrücklicher Genehmigung (Einwilligung) seitens des Auftraggebers installiert oder konfiguriert werden.

Jeder nicht benötigte Netzwerkzugang (TCP/IP- oder UDP-Port) muss deaktiviert sein. Die Nutzung jedes Zugangs muss in der Dokumentation des Auftragnehmers erläutert werden.

Der Auftragnehmer stellt sicher, dass die vom Auftraggeber vorgegebenen allgemeinen Konfigurationsstandards und Sicherheitsvorschriften eingehalten werden.

Der Auftragnehmer stellt sicher, dass jedes Standardpasswort in allen Fällen geändert werden kann.

Der Auftragnehmer stellt im Rahmen seiner Möglichkeiten sicher, dass seine Lösungen frei von „Backdoors“ sind, die dazu geeignet sind, die verwendeten Sicherheitsmechanismen zu umgehen.

Der Auftragnehmer weist hinsichtlich seiner Produkte mit geeigneten Maßnahmen und Protokollen nach, dass alle in diesem Kapitel genannten Anforderungen eingehalten werden, damit die Schutzziele und die Funktionsfähigkeit der Kritischen Infrastruktur gewährleistet sind.

- **Anforderungen an die Softwareentwicklungsprozesse**
  Die Softwareentwicklungsprozesse des Auftragnehmers müssen so ausgelegt sein, dass der Sicherheit der entwickelten Software angemessene Beachtung in allen wichtigen Entwicklungsphasen geschenkt wird und die Prozesse sich an den allgemein anerkannten Industriestandards orientieren.

  Der Auftragnehmer sichert zu, dass er diesbezüglich mindestens folgende Anforderungen erfüllt:
  - Es liegen Standards der sicheren Softwarearchitektur vor.
  - Die Entwickler halten sich an die vorhandenen Standards zur sicheren Programmierung, um Schwachstellen vorzubeugen. Die von Ihnen einzuhaltenden Standards sind dokumentiert und sind den Entwicklern bekannt. Gleiches gilt für Änderungen, die sich an den betreffenden Standards ergeben bzw. ergeben sollten.
  - Secure-Code-Reviews sind Teil der Qualitätssicherung des Auftragnehmers und Bestandteil der Leistungserbringung durch den Auftragnehmer.
  - Im Falle der Nutzung von Open-Source-Komponenten angemessene Konfiguration, Dokumentation und Wartung dieser Komponenten.
  - Die hausinternen Tests des Auftragnehmers vor Auslieferung an den Auftraggeber umfassen explizit auch die Prüfung aller implementierten Sicherheitsmechanismen und -funktionen (Verschlüsselung, Zugriffskontrollen,

Authentisierung und andere). Der Auftragnehmer stellt zu jeder Lieferung und zu jedem Update dem Auftraggeber die notwendige Menge von funktionalen Testfällen und -skripten zur Verfügung, die zum sicheren Funktionsnachweis benötigt werden.

- Es werden regelmäßig Sicherheitsüberprüfungen entsprechend den vorgesehenen Betriebsumgebungen durchgeführt, z.B. unabhängige Penetrationstests für die Systeme, die aus den externen bzw. nicht abgesicherten Netzen erreichbar sein sollen.

Die Ergebnisse der durchgeführten Secure-Code-Reviews sowie Informationen über die Durchführung von Penetrationstests werden dem Auftraggeber jeweils umgehend mitgeteilt.

- **No-Spy-Klausel**
  Der Auftragnehmer erbringt seine Leistungen frei von möglicherweise Schaden stiftender Software (Viren, Würmer, Trojaner etc.), z.B. in mitgelieferten Treibern oder der Firmware. Dies hat der Auftragnehmer in geeigneter Form kontinuierlich zu überprüfen. Auf Anforderung hat er dem Auftraggeber schriftlich zu bestätigen und nachzuweisen, dass er bei diesen Prüfungen keine Hinweise auf Schaden stiftende Software gefunden hat.

  Der Auftragnehmer sichert zu, dass die im Rahmen der Leistungserbringung gegebenenfalls eingesetzte Hard- und Software frei von Funktionen ist, die die Schutzziele gefährden, beispielsweise durch Funktionen
  - zum unerwünschten Absetzen/Ausleiten von Daten,
  - zur unerwünschten Veränderung/Manipulation von Daten oder der Ablauflogik oder
  - zum unerwünschten Einleiten von Daten oder unerwünschte Funktionserweiterungen.

  „Unerwünscht“ in diesem Sinne ist eine Funktion, die weder vom Auftraggeber gefordert noch vom Auftragnehmer unter konkreter Beschreibung der Funktion und ihrer Auswirkungen angeboten, noch im Einzelfall vom Auftraggeber ausdrücklich autorisiert („opt-in“) wurde.

2.3 Stufe 3 Ergänzende Anforderungen bei Cloud-Leistungen

Über die in Stufen 1 und 2 definierten Anforderungen hinaus sind in der Stufe 3 zusätzlich folgende Anforderungen vom Auftragnehmer zu erfüllen:

- Die Anforderungen des C5-Katalogs des BSI werden erfüllt
- **Sicherheit in Auslagerungsprozessen**
  Beabsichtigt der Auftragnehmer Teile der Betriebsleistung oder anderer Dienstleistungen für den Auftraggeber an weitere Dienstleister auszulagern, stellt er sicher, dass die in diesem Dokument beschriebenen Sicherheitsanforderungen in den Vereinbarungen mit Dienstleistern berücksichtigt sind. Die von den Dienstleistern zu erfüllenden Sicherheitsanforderungen sind so zu definieren, dass die Sicherheitsstandards für die Daten des Auftraggebers und Leistungen für den Auftraggeber in je-dem Fall eingehalten werden können und dass der

Auftragnehmer in der Lage ist, eigene Verpflichtungen zur Sicherheit gegenüber dem Auftraggeber vollumfassend zu erfüllen. Eine transparente Darstellung der durchgehenden Lieferkette einschließlich Subunternehmer ist gegenüber dem Auftraggeber vor Auftragserteilung nachzuweisen. Alle vom Auftragnehmer beabsichtigten Auslagerungen von Betriebs- oder Dienstleistungen an Subunternehmer sind nur mit vorheriger Zustimmung des Auftraggebers zulässig.

Für die Einhaltung und Überwachung dieser Standards, auch bei durch den Auftragnehmer gegebenenfalls eingesetzten Subunternehmern, ist der Auftragnehmer verantwortlich. Der Auftragnehmer stellt sicher, dass der Auftraggeber zum Zwecke der Prüfung entsprechende Kontrollbesuche bzw. Audits bei den durch den Auftragnehmer eingesetzten Subunternehmern durchführen kann, indem er insbesondere dafür Sorge trägt, dass dem Auftraggeber Zutritt zu den Räumlichkeiten des Subunternehmers gewährt und Auskunft gegeben wird.

2.4 Stufe 4 Ergänzende Anforderungen bei Einsatz von KÜNSTLICHER INTELLIGENZ (KI)

Über die in Stufen 1 und 2 definierten Anforderungen hinaus sind in der Stufe 4 zusätzlich folgende Anforderungen vom Auftragnehmer zu erfüllen:

- Der Auftragnehmer sichert zu, notwendige Maßnahmen hinsichtlich AI literacy getroffen zu haben. Hierzu gehören insbesondere Maßnahmen,
  - die fachliche Kompetenz zu den eingesetzten KI-Modellen sicherstellen,
  - den sicheren Betrieb der KI gewährleisten
  - die sichere und datenschutzkonforme Überwachung der KI-Nutzung sicherstellen.
- Der Auftragnehmer sichert zu, dass ein KI-spezifisches Risikomanagement existiert, das über den gesamten Lebenszyklus des KI-Systems systematisch KI-relevante Risiken analysiert.
- Entsprechend dem Gefährdungspotential der Anwendung werden die Metriken, welche verwendet werden, um die Qualität der KI-Modelle zu bewerten, regelmäßig überprüft. Neben der Genauigkeit auf den erwarteten Eingabedaten werden auch andere Aspekte berücksichtigt, wie z. B. Over-/Underfitting, Bias-Effekte sowie die Robustheit gegenüber zufälligen oder gezielten Änderungen.
- Der Auftragnehmer sichert zu, dass Daten und Modelle gegen Manipulationen geschützt und Änderungen protokolliert werden sowie jedes Datum seiner Quelle zuzuordnen ist.
- Die Verwendung von Daten oder Modellen aus externen Quellen wird dem Auftraggeber in Textform (z.B. Angebot oder Releasenotes) angezeigt.
- Der Auftragnehmer sichert zu, dass Anfragen an und Zugriffe auf das KI-System geeignet protokolliert und die Protokolldaten regelmäßig auf Anomalien untersucht werden.
- Der Auftragnehmer sichert zu, dass er das KI-System regelmäßig anhand entsprechender Metriken auf eine korrekte Funktionsweise überprüft.

3 Schlussbestimmungen

Ist eine der genannten Regelungen unwirksam oder unvollständig, so bleiben die weiteren Regelungen hiervon im Übrigen wirksam. Anstelle der unwirksamen Regelung tritt die gesetzliche Regelung.

Sämtliche mit diesem Dokument in Zusammenhang stehenden finanziellen Aufwände des Auftragnehmers sind mit den Regelungen im Hauptvertrag abgegolten.

Änderungen dieses Dokuments, des Verarbeitungsgegenstandes oder Verfahrensänderungen bedürfen der Schriftform und erfordern die Zustimmung des Auftraggebers.