



Teil B Leistungsbeschreibung

Inhalt

I. Ausgangslage	2
1. Der Landkreis Peine	2
2. Der „IST“- Zustand	2
3. Anforderungen und Ziele	2
II. Allgemeine Leistungsanforderungen	3
1. Organisation	3
2. Kommunikationsmanagement	4
3. Personalqualifikation und Einsatz	4
4. Grundsätzliche Unterstützungspflicht des AN	5
5. Technische Unterstützung und Softwareeinsatz	7
5.1. Plattform und Systemumgebung	7
5.2. Datenmodell, Modularität und Integration	8
5.3. Funktionalität	9
5.4. Betrieb, Wartung, Support und Verträge	11
5.5. Datenschutz, Datenhoheit und Exit-Fähigkeit	11
III. Besondere Leistungsanforderungen	11
1. Leistungsumfang GAP-Analyse	11
2. Leistungsbereich Aufbau und Implementierung von ISMS, BCMS, DSMS	12
3. Leistungsbereich Datenschutz (sofern einzelne Leistungen nicht bereits im Rahmen von III. Ziffer 2 erbracht werden)	15
4. Leistungsbereich Informationssicherheit (sofern einzelne Leistungen nicht bereits im Rahmen von III. Ziffer 2 erbracht werden)	16
5. Leistungsbereich BCM (sofern einzelne Leistungen nicht bereits im Rahmen von III. Ziffer 2 erbracht werden)	17
6. Leistungsbereich Schulung, Awareness und Wissenstransfer	18
6.1. Awarenessmaßnahmen und Wissenstransfer	18
6.2. Schulungen	18
7. Leistungsbereich anlassbezogene Unterstützung bei sicherheitsrelevanten Ereignissen (optional)	18



I. Ausgangslage

1. Der Landkreis Peine

Der Landkreis Peine ist ein niedersächsischer Landkreis zwischen den Oberzentren Braunschweig und Hannover. Mit ca. 1200 Mitarbeitenden zählt der Landkreis Peine zu einem der größten Arbeitgeber in der Region.

Der Landkreis Peine ist organisatorisch nach einem Dezernatsmodell aufgebaut. Es gibt drei Dezernate. Das Dezernat 1 (Zentrale Verwaltung, Ordnung, Recht), das Dezernat 2 (Umwelt, Bauen, Verbraucherschutz) und das Dezernat 3 (Soziales, Jugend, Gesundheit). Hinzu kommen Stabsstellen: Das Referat 1 (Landrat, Kreistag und Öffentlichkeitsarbeit), das Referat 2 (Migration und Teilhabe), das Referat 3 (Gleichstellung) und das Referat 4 (Referat Fördermittelmanagement, Koordination Informationssicherheit, BCM und Datenschutz), der externe Datenschutzbeauftragte, der externe Informationssicherheitsbeauftragte, das Rechnungsprüfungsamt sowie der Personalrat.

Siehe dazu:

<https://www.landkreis-peine.de/Verwaltung/Verwaltungsaufbau/>

2. Der „IST“- Zustand

Der Landkreis Peine befindet sich im Zuge des Megatrends Digitalisierung in einer komplexen Gesamttransformation. Dies sowohl technisch als auch organisatorisch. Für die Themen Datenschutz, Informationssicherheit, Business Continuity Management (BCM) und Compliance befindet sich die Koordination im Referat Fördermittelmanagement, Koordination Informationssicherheit, BCM und Datenschutz (REF4). Dies ist für den Auftragnehmer grundsätzlich die Schnittstelle beim Auftraggeber. Dies gilt für alle benannten Themen und Leistungen. **Der Auftraggeber stellt die Rolle Koordinator für den Datenschutz, die Informationssicherheit, Compliance und BCM (Schnittstelle).** Grundstrukturen wie z.B. Rollenkonzepte und Verantwortungsbereiche wurden für einige Bereiche (Informationssicherheit und Datenschutz sowie indirekt Compliance) bereits geschaffen. Für den Bereich BCM steht dies noch aus. Die Umsetzungsstände in den benannten Themenbereichen sind unterschiedlicher Ausprägung. Daher setzt der Auftraggeber eine GAP-Analyse voraus, sodass dann die Ziele im weiteren Verlauf näher definiert und kommuniziert werden können.

3. Anforderungen und Ziele



Es besteht Unterstützungs-, Begleitungs- und Steuerungsbedarf hinsichtlich der Schaffung durchgängiger Managementsysteme, gerade in den drei Themenbereichen (Datenschutz, Informationssicherheit und Business Continuity Management). Hier auch im Bereich der Prozesse und Maßnahmen. Alle Maßnahmen sollen grundsätzlich der Umsetzung rechtlicher, technischer, organisatorischer sowie interner und externer Vorgaben dienen.

Synergien sind in den drei benannten Themenbereichen zu schaffen, sodass ein ganzheitlicher Ansatz zur Erreichung der Gesamtziele vollzogen werden kann. Der Landkreis Peine soll im Bereich des Datenschutzes, der Informationssicherheit sowie im Bereich des Geschäftsfortführungsmanagements (BCM) so aufgestellt sein, dass Managementsysteme etabliert sind, die den generellen Vorgaben und Anforderungen (DS-GVO sowie BSI und weiteren einschlägigen normativen Vorgaben) entsprechen. Die Maßnahmen und Prozesse sollen präventiver und reaktiver Natur sein. Die Resilienz der Kommunalverwaltung, gegenüber aktueller sowie kommender Gefährdungs- und Bedrohungslagen, soll sich dynamisch entwickeln können, um bestenfalls vor der „Lage“ zu sein, respektive bei Vorfällen (Incidents) das Schadensausmaß so gering wie möglich zu halten. Dabei sind die Managementsysteme so auszugestalten und fortzuentwickeln, dass sie sich verbindlich an den Schutzzielen und Resilienzanforderungen orientieren, wie sie für den Betrieb Kritischer Infrastrukturen maßgeblich sind. Dies umfasst insbesondere Anforderungen an Verfügbarkeit, Integrität, Belastbarkeit sowie Wiederanlauf- und Krisenfähigkeit wesentlicher kommunaler Prozesse und informationsverarbeitender Systeme, auch unter außergewöhnlichen und krisenhaften Rahmenbedingungen. Eine formale Einstufung der gesamten Kommunalverwaltung als Kritische Infrastruktur ist hiermit nicht verbunden. Die Aufrechterhaltung der Bürgerservices inkl. der Aufrechterhaltung der Arbeits- und Reaktionsfähigkeit der Kommunalverwaltung sowie die Fortführung der Digitalisierung sollen grundsätzlich im Einklang mit den jeweiligen Maßnahmen der benannten Themenbereiche stehen. Der Landkreis Peine beabsichtigt vorliegend eine zukunftsorientierte Beschaffung.

II. Allgemeine Leistungsanforderungen

1. Organisation

Der Auftragnehmer hält ein eigenes Sicherheitskonzept vor, dass die sichere, unterbrechungsfreie und ordnungsgemäße Erbringung der beauftragten Leistungen gewährleistet. Das Sicherheitskonzept beschreibt die organisatorischen und technischen Maßnahmen zur Aufrechterhaltung der Verfügbarkeit, Integrität, Vertraulichkeit der Systeme und Prozesse, die für die Leistungserbringung erforderlich sind. Es umfasst insbesondere Verfahren zum Schutz vor unbefugten Zugriffen, Mechanismen zur Erkennung und Behandlung von Sicherheitsvorfällen sowie Regelungen für das Notfall-, Wiederanlauf- und Business-Continuity-Management. Der Auftragnehmer stellt sicher, dass alle eingesetzten Systeme, Mitarbeitenden und Unterauftragnehmer diese Anforderungen erfüllen und dass das Sicherheitskonzept regelmäßig überprüft,



aktualisiert und an veränderte Risiken angepasst wird. Weiterhin verpflichtet sich der Auftragnehmer, dem Auftraggeber auf Anforderung geeignete Nachweise, Dokumentationen und Prüfberichte zur Verfügung zu stellen, die die Umsetzung und Wirksamkeit der beschriebenen Sicherheitsmaßnahmen belegen.

2. Kommunikationsmanagement

Der Auftragnehmer muss seine Leistungen über mehrere Kanäle (Telefon, E-Mail, Videokonferenz und Vor-Ort) bereitstellen, um eine flexible und kontinuierliche Betreuung des Auftraggebers sicherzustellen. Er hat während der Geschäftszeiten telefonisch und per E-Mail erreichbar zu sein. Diese sind montags bis donnerstags von 08:00 bis 17:00 Uhr sowie freitags von 08:00 bis 16:00 Uhr (Servicezeiten gemäß Nr. 5.1 des Teil C EVB-IT-Dienstvertrag). Der Auftragnehmer gewährleistet eine Bearbeitung von Anfragen des Auftraggebers spätestens acht Stunden nach Eingang der Anfrage (Reaktionszeit gemäß Nr. 5.2 des Teil C EVB-IT-Dienstvertrag).

3. Personalqualifikation und Einsatz

Der Auftragnehmer übernimmt die Rolle des Informationssicherheitsbeauftragten (ISB) und des Datenschutzbeauftragten (DSB gemäß DS-GVO). Der Auftragnehmer ist verpflichtet, das in seinem Angebot genannte Personal im Auftragsfalle einzusetzen.

Das vom Auftragnehmer eingesetzte Schlüsselpersonal muss über nachweisbare Fachkenntnisse in den Bereichen Informationssicherheit, Datenschutz und Business Continuity Management verfügen und diese in der praktischen Umsetzung sicher anwenden können.

Im Themengebiet Informationssicherheit muss das eingesetzte Personal über fundierte Kenntnisse der einschlägigen Regulierungen (z. B. KRITIS, NIS2, IT-SiG 2.0) sowie relevanter Normen und Prozessmodelle verfügen. Das Personal muss mindestens über drei Jahre praktische Erfahrung, vorzugsweise im kommunalen Umfeld, verfügen. Anerkannte Qualifikationen wie BSI-IT-Grundschutz-Berater/in, ISO 27001 Lead Auditor/in, CISA oder CISSP sind wünschenswert.

Im Themengebiet Datenschutz muss das eingesetzte Personal über umfassende, nachgewiesene Kenntnisse im Datenschutzrecht (DS-GVO, BDSG, NDStG) sowie über mindestens drei Jahre praktische Erfahrung, vorzugsweise im kommunalen Umfeld, verfügen. Zudem sind juristische wie technische Kenntnisse erforderlich, insbesondere im Bereich der technischen und organisatorischen Maßnahmen (TOM) sowie der Informationssicherheit.

Im Themengebiet Business Continuity Management muss das eingesetzte Personal über Kenntnisse normativer Anforderungen (z. B. BSI 200-4, ISO 22301) sowie praktisches Prozessverständnis zu Notfall-, Wiederanlauf- und Krisenmanagementprozessen verfügen. Anerkannte Zertifizierungen wie z.B. BCM-Praktiker/in sind vorteilhaft.



Die Gesamtprojektleitung, fachliche Leitung „Datenschutz“ und fachliche Leitung „Informationssicherheit“ ist Schlüsselpersonal im Sinne der Ziffer 8.3 der EVB-IT-Dienstleistung AGB.

Alle eingesetzten Personen müssen über Deutschkenntnisse auf mindestens Niveau C2 gemäß GER verfügen..

Durch den Auftragnehmer ist ausreichend qualifiziertes Personal vorzuhalten, um die kontinuierliche Leistungserbringung sicherzustellen. Er hat dazu geeignete Vertretungsregelungen vorzusehen.

Auf Verlangen des Auftraggebers sind die vorstehend genannten Anforderungen für das eingesetzte Personal jederzeit nachzuweisen.

4. Grundsätzliche Unterstützungspflicht des AN

Der Auftragnehmer muss den Auftraggeber bei der Erstellung, Überarbeitung und Umsetzung von Dienstvereinbarungen, Strategien und Leistungsbeschreibungen unterstützen, um sicherzustellen, dass datenschutzrechtliche und informationssicherheitsrelevante Anforderungen sowie auf die Institution wirkende normative Vorgaben vollumfänglich berücksichtigt werden.

Er schuldet eine umfassende und durchgängige Beratung des Auftraggebers in allen Belangen des Datenschutzes, der Informationssicherheit sowie der Business Continuity im Rahmen des BCM. Er hat dabei den Auftraggeber bei der Erstellung und Überarbeitung von Richtlinien, Leitlinien und Dienstanweisungen fachlich zu begleiten, inhaltlich zuzuarbeiten und sicherstellen, dass diese den geltenden gesetzlichen und normativen Anforderungen entsprechen. Dazu gehört auch eine Unterstützung des Auftraggebers in den relevanten Gremien (Informationssicherheitsorganisation und der koordinierenden Stelle), einschließlich Teilnahme, Vorbereitung, Informationsfluss und Abstimmung mit Projektverantwortlichen.

Der Auftragnehmer muss regelmäßig und fortlaufend die von ihm vorgeschlagenen und umgesetzten Maßnahmen hinsichtlich ihrer Wirksamkeit und Geeignetheit überprüfen, Verbesserungspotenziale identifizieren und ggf. notwendige Korrekturmaßnahmen einleiten.

Der Auftragnehmer unterstützt und begleitet den Auftraggeber bei Audits und Prüfungen in allen in dieser Ausschreibung benannten, Themengebieten.

Der Auftragnehmer schließt mit dem Auftraggeber nach Zuschlagserteilung einen Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO, soweit er im Rahmen der Leistungserbringung personenbezogene Daten im Auftrag verarbeitet. Der Vertrag zur Auftragsverarbeitung enthält insbesondere eine detaillierte Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DS-GVO, die mindestens die Bereiche Zugriffskontrolle, Zutrittskontrolle, Verschlüsselung, Datenträgerkontrolle, Löschkonzept und Protokollierung abdecken.



Der Auftragnehmer verpflichtet sich sowie alle von ihm eingesetzten Mitarbeiter und Nachunternehmer, über sämtliche im Rahmen der Leistungserbringung bekannt gewordenen oder zugänglich gemachten Informationen, Unterlagen, Erkenntnisse, Kenntnisse und Daten Verschwiegenheit zu wahren.

Die Verschwiegenheitspflicht gilt unabhängig von der Art der Kenntniserlangung sowie von der Darstellungsform und erstreckt sich auf schriftliche, elektronische, mündliche oder sonstige Informationen. Sie umfasst insbesondere, jedoch nicht abschließend, organisatorische, technische, wirtschaftliche, personelle, strategische sowie sicherheits- und datenschutzrelevante Informationen, einschließlich interner Abläufe, Konzepte, Planungen, Bewertungen, Protokolle, Prüfergebnisse, Risiko- und Schwachstellenanalysen, Sicherheitskonzepte, Notfall- und Wiederanlaufpläne, BCM-Dokumentationen sowie Erkenntnisse aus Gesprächen, Workshops, Begehungen, Audits oder Tests.

Die Verschwiegenheitspflicht gilt auch für Informationen, die nicht ausdrücklich als vertraulich gekennzeichnet sind, sofern sich ihre Schutzbedürftigkeit aus dem Inhalt der Information oder den Umständen der Kenntniserlangung ergibt. Eine Weitergabe an Dritte oder eine Nutzung zu anderen als den vertraglich vorgesehenen Zwecken ist ohne vorherige schriftliche Zustimmung des Auftraggebers unzulässig.

Die Verpflichtung zur Verschwiegenheit besteht zeitlich unbegrenzt auch über das Ende der Vertragslaufzeit hinaus. Der Auftragnehmer stellt sicher, dass sämtliche von ihm eingesetzten Mitarbeiter und Nachunternehmer entsprechend verpflichtet werden. Die Verpflichtung zur Verschwiegenheit ist schriftlich für jede eingesetzte Person zu dokumentieren und dem Auftraggeber auf Verlangen jederzeit nachzuweisen.

Nach Beendigung des Vertragsverhältnisses hat der Auftragnehmer sämtliche vom Auftraggeber erhaltenen oder im Rahmen der Leistungserbringung erstellten Informationen und Unterlagen nach Wahl des Auftraggebers entweder vollständig zurückzugeben oder datenschutz- und sicherheitskonform zu löschen bzw. zu vernichten. Die ordnungsgemäße Löschung oder Vernichtung ist dem Auftraggeber auf Verlangen geeignet nachzuweisen.

Sofern der Auftragnehmer Unterauftragnehmer einsetzt oder beabsichtigt, Daten außerhalb des Europäischen Wirtschaftsraums zu verarbeiten, hat er dies dem Auftraggeber unaufgefordert und vorab mitzuteilen. Der Auftragnehmer hat dem Auftraggeber sämtliche Unterlagen und Informationen zur Verfügung zu stellen, die eine datenschutzrechtliche, sicherheitstechnische und rechtliche Beurteilung des Vorhabens ermöglichen. Der Einsatz von Unterauftragnehmern oder eine Drittlandverarbeitung ist erst nach der Genehmigung durch den Auftraggeber zulässig.



5. Technische Unterstützung und Softwareeinsatz

Der Auftragnehmer muss eine geeignete, softwaregestützte modulare Lösung für den Datenschutz, die Informationssicherheit und das BCM einsetzen, die den Betrieb eines Datenschutzmanagementsystems (DSMS) ermöglicht und die Integration von Informationssicherheitsmanagement (ISMS), IT-Grundschutz, zukünftig ggf. Grundschutz++ sowie Business Continuity Management (BCM) unterstützt. Die Softwarelösung muss eine medienbruchfreie digitale Zusammenarbeit mit der Kreisverwaltung gewährleisten und Datenschutz, Informationssicherheit sowie BCM ganzheitlich verzahnen. Die durch den Auftragnehmer zur Verfügung zu stellende Software umfasst die Lizenzen, Installation, ggf. Hosting, Support und Pflege, sowie Schulungen aller Rollen bzw. Nutzern. Sollte der Auftraggeber nach der Grundlaufzeit von zwei Jahren, den Vertrag nur für einen Teil der beauftragten Leistungsbestandteile verlängern (siehe Nr. 15.1 Teil C EVB-IT-Dienstvertrag und wird auch der Leistungsbestandteil der technischen Unterstützung und des Softwareeinsatzes verlängert, so muss die Software unter Berücksichtigung der nachfolgenden inhaltlichen Vorgaben gemäß II., Nr. 5.1 bis 5.4 dieser Leistungsbeschreibung weiterhin nutz- und verlängerbar sein. Näheres regelt der Teil C EVB-IT-Dienstvertrag unter Nr. 15.1.

Die angebotene Software muss gewährleisten, dass eine medienbruchfreie digitale Zusammenarbeit mit dem Auftraggeber möglich ist, insbesondere im Hinblick auf eine gemeinsame Datenpflege, Nachvollziehbarkeit (Historie, z.B. Änderung von Datensätzen), revisionssichere Dokumentation und sichere Kommunikation.

Daher sind folgende Anforderungen an die Software zu stellen:

5.1. Plattform und Systemumgebung

- Die Software muss auf einer einheitlichen, objektorientierten Datenbasis aufbauen, die von allen Modulen genutzt wird (BCM, Datenschutz, Informationssicherheit gesamtheitlich).
- Die Software muss webbasiert, mehrbenutzerfähig und agentenlos (ohne Client-Installation) betrieben werden können. Sie muss mindestens folgende Browser unterstützen: Microsoft Edge und Mozilla Firefox, Chrome. Dies jeweils, in der durch den jeweiligen Browserhersteller supporteten Version.
- Die Software muss sowohl On-Premise in virtualisierten Umgebungen (z. B. VMware, Hyper-V, Citrix, Azure Virtual Desktop) oder im Hosting (SaaS) angeboten werden können.
- Eine Migration zwischen Hosting- und On-Premise oder On-Premise und Hosting, muss jederzeit möglich.
- Die Software muss auf Windows Server (Operating System), in der jeweils durch Microsoft aktuell supporteten Version, betrieben werden können, insofern ein Server benötigt wird.



- Die Software muss auf Microsoft Datenbankserver (MS-SQL), in der jeweils durch Microsoft aktuell supporteten SQL-Version, betrieben werden können, insofern eine Datenbank benötigt wird.
- Sie muss auf Windows-Clients in aktueller, supporteter Version lauffähig sein.
- Der Auftragnehmer ist verpflichtet alle benötigten Komponenten (Software, Middleware, Hardware), die für den Betrieb und die Nutzung der Softwarelösung erforderlich sind, vollständig aufzulisten.
- Die Software muss in virtuellen Desktop-Umgebungen (z. B. Citrix, Microsoft AVD) stabil betrieben werden können.
- Die Software muss SSL/TLS-verschlüsselte Kommunikation zwischen allen Komponenten gewährleisten oder eine anderweitige dem Stand der Technik entsprechende sichere Kommunikation gewährleisten.
- Die Authentifizierung muss über LDAP, SAML oder OpenID Connect oder einer anderen dem Stand der Technik angemessenen Lösung möglich sein. Maßgebend ist die Auftraggeberinfrastruktur.
- Die Software muss Single Sign-On (SSO) fähig sein.

5.2. Datenmodell, Modularität und Integration

- Die Software muss eine Mandantenfähigkeit beinhalten, sodass bei Bedarf oder Notwendigkeit mehrere Organisationseinheiten, Fachbereiche oder anderweitige Bedarfstragende getrennt verwaltet werden können.
- Das Berechtigungssystem muss rollenbasiert und die Zugriffsrechte granular steuerbar sein. Ein rollenbasiertes und granular steuerbares Berechtigungssystem (RBAC – Role Based Access Control) bildet einen zentralen Bestandteil der Anforderungen an die geplante Lösung.
- Das System muss sicherstellen, dass Nutzern ausschließlich jene Zugriffsrechte zugewiesen werden, die für die Erfüllung ihrer jeweiligen Aufgaben notwendig sind. Hierzu ist ein klar strukturiertes Rollenmodell erforderlich, das sowohl einfache Rollen als auch hierarchische Rollenstrukturen unterstützt, in denen Berechtigungen vererbt werden können. Mehrfachzuweisungen von Rollen an einen Benutzer müssen ebenso möglich sein, um komplexe Verantwortlichkeiten flexibel abbilden zu können. Die Zugriffssteuerung hat auf unterschiedlichen Ebenen zu erfolgen, sodass Berechtigungen nicht nur auf Funktions- oder Modulebene, sondern auch auf Objekt- sowie Feldebene definiert werden können. Dadurch wird eine maximale Granularität gewährleistet, bei der einzelne Datensätze, Dokumente oder spezifische Felder individuell geschützt und freigegeben werden können.
- Neben klassischen CRUD-Rechten (Erstellen, Lesen, Aktualisieren, Löschen) müssen auch weiterführende Aktionsrechte, wie etwa Genehmigungen, Exporte oder API-Zugriffe, differenziert zuweisbar sein. Ergänzend hierzu soll das Berechtigungssystem kontextabhängige Regeln unterstützen, sodass Zugriffe dynamisch anhand zusätzli-



cher Attribute gesteuert werden können. Dazu zählen etwa die Rolle und organisatorische Zugehörigkeit eines Nutzers oder der Status der zu bearbeitenden Daten. Ein solcher dynamischer Ansatz ermöglicht eine fein abgestimmte Zugriffskontrolle, die sich an tatsächlichen Arbeitsprozessen orientiert.

- Das System stellt Funktionen zur temporären Delegation von Rechten sowie zur Verwaltung von Vertretungen bereit. Alle Berechtigungsänderungen und sicherheitsrelevanten Aktionen müssen vollständig und revisionssicher protokolliert werden können. Transparenz über Zugriffsrechte ist durch übersichtliche Rechtematrizen, Berichte und Auditfunktionen sicherzustellen.
- Zur langfristigen Governance sind darüber hinaus Mechanismen zur regelmäßigen Überprüfung und Rezertifizierung von Rechten vorzusehen, ebenso wie Workflows für Genehmigungen und automatisierte Entziehungen von Berechtigungen bei Rollenwechseln oder Austritten. Technisch wird eine Integration mit gängigen Identitäts- und Zugriffsmanagementsystemen (z. B. IAM, Active Directory oder vergleichbaren Lösungen) gefordert. Hier ist die Infrastruktur des Auftraggebers maßgebend. Die Berechtigungsprüfung hat über eine moderne Policy-Engine oder entsprechende APIs zu erfolgen und aktuelle dem Stand der Technik entsprechende Standards zu berücksichtigen.
- Die Lösung muss standardisierte Schnittstellen (Im- und Export auf Basis von z.B. API, XML) bieten, um Datenimport/-export mit anderen Systemen (z. B. Ticketing, CMDB, AD, ITIL, Prozessmanagement Tool) zu ermöglichen. Daten müssen automatisiert aus Drittsystemen übernommen werden können und sollten mit definierten Workflows weiterverarbeitet werden können.

5.3. Funktionalität

- Die Software muss Verarbeitungsverzeichnisse, Rechtsgrundlagen, Empfänger, Löschfristen und technische Maßnahmen erfassen und versionieren können.
- Die Software muss Datenschutzfolgenabschätzungen (DSFA) inklusive Risikoanalyse und Maßnahmenbewertung ermöglichen.
- Die Software muss Berichte und Nachweise zur DS-GVO-Konformität generieren können.
- Die Software muss Schutzbedarfe, Risiken und Maßnahmen gemäß ISO 27001/27005 oder BSI Standard 200-3 erfassen können. Die Software muss den IT-Grundschutz nach BSI 200-1, 200-2 und 200-3 abbilden und regelmäßig aktualisierbare Komponenten unterstützen.
- Die Software muss die Abbildung von Rollen, Verantwortlichkeiten und Gremienstrukturen im Rahmen des ISMS unterstützen. Managementbewertungen, Zieldefinitionen, Kennzahlen und Maßnahmenverfolgung müssen systematisch dokumentiert und ausgewertet werden können.
- Die Software sollte die Erstellung, Pflege und Versionierung einer Statement of Applicability (SoA) unterstützen.



- Fortschritte, Abweichungen und Wirksamkeiten von Maßnahmen müssen nachvollziehbar und revisionssicher darstellbar sein.
- Die Software muss ein BCMS vollständig abbilden können, sowie dessen Pflege und Fortführung ermöglichen.
- Sicherheitsvorfälle müssen mittels der Software standardisiert dokumentiert und nachvollziehbar abgewickelt werden können.
- Die Software muss in der Lage sein, sowohl interne als auch externe Audits vollständig zu verwalten und revisionssicher zu dokumentieren.
- Alle sicherheits- und datenschutzrelevanten Aktionen müssen vollständig, manipulationssicher und revisionsfest protokolliert werden können.
- Protokolle müssen zeitlich eindeutig zuordenbar, auswertbar und exportierbar sein.
- Der Zugriff auf Protokolldaten sollte rollenbasiert zu beschränken sein.
- Die Software muss die Unterstützung interner und externer Prüfungen (z. B. Datenschutz, IT-Sicherheit, Revision) ermöglichen.
- Die Software muss Business-Impact-Analysen (BIA) durchführen und kritische Prozesse, Ressourcen und Wiederanlaufzeiten automatisch bewerten können.
- Notfallpläne, Wiederanlaufpläne und Tests müssen mittels Software systematisch erstellt und dokumentiert werden können.
- Die Software sollte Alarmierungs- und Krisenmanagementfunktionen unterstützen, einschließlich Eskalationsketten und Kommunikationsplänen.
- Die Software muss Gefährdungsübersichten, Risikoanalysen und Maßnahmenpläne generieren und verwalten können.
- Referenzberichte und Zertifizierungsnachweise müssen automatisch erzeugt werden können.
- Die Software muss dynamisches Live-Reporting und Visualisierungen (Tabellen, Diagramme, Kennzahlen) ermöglichen. Sie muss CI-konforme Berichte (Logo, Layout, Schrift) erstellen können.
- Alle Änderungen im System müssen revisionssicher dokumentiert werden (Audit-Trail).
- Die Software muss Exportfunktionen (PDF, DOCX, XLSX, HTML) standardmäßig zur Verfügung stellen.
- Die Lösung muss über eine Prozess-Engine verfügen, die Workflows frei konfigurierbar macht (Genehmigungen, Erinnerungen, Eskalationen).
- Wiederkehrende Prozesse (z. B. Auditzyklen, Risikoprüfungen) müssen mittels der Software automatisiert werden können.
- Die Software muss dynamische Fragebögen (z. B. für Selbstbewertungen, Lieferanten, Prüfungen) versenden und auswerten können.
- Die Software sollte die Anforderungen an digitale Barrierefreiheit nach den jeweils geltenden gesetzlichen Vorgaben unterstützen (z. B. BITV), soweit dies technisch möglich ist.



5.4. Betrieb, Wartung, Support und Verträge

- Der Auftragnehmer gewährleistet die langfristige Weiterentwicklung aller Module. Es müssen regelmäßige Updates erfolgen, die eine Kompatibilität auch mit künftigen Normen (z. B. NIS2, Vorhaben aus dem Projekt Digitaler Omnibus) sicherstellt und die Integration weiterer neuer Module (z. B. Nachhaltigkeit, Risikoportale, Lieferkette) ermöglicht. Der Anbieter verpflichtet sich, nicht mehr supportete Softwareversionen unverzüglich zu aktualisieren oder zu ersetzen.
- Es muss die Möglichkeit bestehen, ein Testsystem einzurichten (z. B. zu Schulungs- oder Evaluationszwecken).
- Der Auftragnehmer muss SLA-Dokumente (Service Level Agreement) mit Leistungskennzahlen (z. B. Reaktionszeiten, Verfügbarkeit) bereitstellen.
- Der Auftragnehmer muss Maßnahmen zur Sicherstellung der Verfügbarkeit, Wiederherstellbarkeit und Integrität der Softwarelösung gewährleisten.
- Backup-, Wiederherstellungs- und Wiederanlaufkonzepte müssen vorhanden und dokumentiert sein.
- Bei gehosteten oder virtualisierten Betriebsformen müssen Redundanz- und Notfallkonzepte vorhanden sein.
- Der Auftraggeber ist über wesentliche Störungen oder Sicherheitsvorfälle unverzüglich zu informieren.

5.5. Datenschutz, Datenhoheit und Exit-Fähigkeit

- Sämtliche im Rahmen der Nutzung der Software verarbeiteten Daten verbleiben uneingeschränkt im Eigentum und in der Verfügungsgewalt des Auftraggebers.
- Der Auftragnehmer darf die Daten ausschließlich zur Erfüllung der vertraglich vereinbarten Leistungen verarbeiten. Eine Nutzung zu eigenen Zwecken ist ausgeschlossen.
- Der Auftraggeber muss jederzeit berechtigt sein, sämtliche Daten vollständig, strukturiert, dokumentiert und maschinenlesbar zu exportieren.
- Nach Vertragsende sind alle Daten vollständig, datenschutz- und sicherheitskonform zu löschen oder herauszugeben, nach Wahl des Auftraggebers.
- Die Softwarelösung darf keine versteckten Abhängigkeiten (z. B. proprietäre Exportformate ohne Dokumentation) enthalten, die einen Anbieterwechsel faktisch verhindern.

III. Besondere Leistungsanforderungen

1. Leistungsumfang GAP-Analyse

Durch den Auftragnehmer ist zum Leistungsbeginn eine GAP-Analyse durchzuführen, um den aktuellen Umsetzungsstand der Informationssicherheit, des Datenschutzes sowie des BCM zu ermitteln, bestehende Abweichungen zu identifizieren und konkrete Handlungsempfehlungen



zur Schließung der Lücken abzuleiten. Die Maßnahmen sind auf die Erreichung der Gewährleistungsziele gemäß den einschlägigen BSI-Standards zu planen und umzusetzen. Der Auftragnehmer hat dabei sicherzustellen, dass das vorhandene Prozessmanagement der Kreisverwaltung in das Vorgehen integriert wird, um bestehende Strukturen effizient zu nutzen.

Es sind insbesondere (aber nicht abschließend) folgende Aspekte zu untersuchen:

- Die vorhandenen oder auch fehlenden Strukturen (Datenschutz, Informationssicherheit, BCM) des Auftraggebers sind im Rahmen der GAP-Analyse zu untersuchen. Bei unklaren oder fehlenden Strukturen sind durch den Auftragnehmer geeignete prozessuale und organisationale Lösungen zu entwickeln, abzustimmen und zur Umsetzung vorzuschlagen, um eine klare Aufgaben- und Verantwortungsstruktur zu gewährleisten.
- Fehlende Rollen in der Informationssicherheitsorganisation sind zu identifizieren. Es sind Vorschläge für die Besetzung und/oder Umsetzung zu entwickeln.
- Analyse der Geschäftsprozesse des Auftraggebers hinsichtlich datenschutzrechtlicher, informationssicherheitsrechtlicher sowie geschäftsfortführender (BCM) Bezüge.

2. Leistungsbereich Aufbau und Implementierung von ISMS, BCMS, DSMS

Der Auftragnehmer ist verpflichtet, in Zusammenarbeit mit dem Auftraggeber ein Informationssicherheitsmanagementsystem (ISMS) auf Basis des BSI-Standards 200-1 unter Anwendung der BSI-Standards 200-2 (IT-Grundschutz-Methodik) und 200-3 (Risikomanagement) sowie ein Business Continuity Management System (BCMS) nach BSI-Standard 200-4 sowie ein DSMS auf Grundlage des SDM in aktueller Version aufzubauen und die dafür erforderlichen methodischen und organisatorischen Schritte durchzuführen. Dem Auftragnehmer obliegt dafür die Verantwortung und er ist primär für die Ausführung zuständig. Die genauen Zuständigkeiten werden nach Vertragsschluss zwischen dem Auftraggeber und Auftragnehmer in einer RASCI-Matrix festgelegt.

Der Auftragnehmer legt dazu in Abstimmung mit dem Auftraggeber einen verbindlichen Zeitplan für die Umsetzung von ISMS, BCMS, DSMS und Meilensteine fest, die die Zielerreichung innerhalb der Erstlaufzeit (24 Monate) sicherstellen. Die Priorisierung sollte risikobasiert erfolgen. Der Aufbau des ISMS, BCMS, DSMS muss parallel zum laufenden Dienstbetrieb erfolgen und darf diesen nicht über das zwingend erforderliche Maß beeinträchtigen. Die Abstimmung mit dem Auftraggeber erfolgt über die koordinierende Schnittstelle beim Auftraggeber.

Der Auftragnehmer hat bei der Leistungserbringung einen ganzheitlichen Ansatz zu nutzen, um zeitliche und monetäre Vorteile zu realisieren (Synergieeffekte) und die Akzeptanz in der Organisation („User Adoption“) aktiv zu fördern. Es werden dafür insbesondere folgende Leistungen durch den Auftragnehmer erbracht:



- Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten des Auftraggebers, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach der DS-GVO sowie nach sonstigen Datenschutzvorschriften (z.B. NDSG, BMG, SGB, u.a.).
- Unterstützung und Begleitung des Auftraggebers bei dem Aufbau eines Datenschutz-Managementsystems (DSMS).
- Der Auftragnehmer unterstützt den Auftraggeber beim Aufbau eines neuen software-gestützten Verzeichnisses von Verarbeitungstätigkeiten, indem er die Prozesse mit strukturiert, über die koordinierende Stelle die Fachbereiche des Auftraggebers mit einbindet und gemeinsame Interviews / Workshops durchführt, die Rechtmäßigkeitsgrundlagen unterstützend mit den Fachbereichen überprüft und bewertet sowie bei der Definition der Löschfristen mitwirkt.
- Überwachung der Einhaltung der DS-GVO, anderer Datenschutzvorschriften sowie der Strategien des Verantwortlichen für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen.
- Der Auftragnehmer unterstützt den Auftraggeber in der Zusammenarbeit mit der Datenschutzaufsichtsbehörde und übernimmt auf Anforderung die Rolle als unterstützende Anlaufstelle.
- Die regelmäßige und proaktive, mindestens quartalsweise, Information des Auftraggebers über rechtliche Neuerungen und technologische Entwicklungen im Bereich Datenschutz.
- Die Pflicht darauf hinzuwirken, dass die datenschutzrechtlichen Anforderungen in alle relevanten Geschäftsprozesse des Auftraggebers integriert werden. Er hat dazu Digitalisierungsprojekte mit Datenschutzbezug aktiv zu begleiten und sicherzustellen, dass Datenschutzerfordernisse bereits in der Planungs- und Umsetzungsphase berücksichtigt werden. Er hat dabei die Erkenntnisse aus der Analyse der Geschäftsprozesse im Rahmen der GAP-Analyse (siehe unter **III. Ziffer 1**). zu verwenden. Auf dieser Grundlage sind durch den Auftragnehmer geeignete Maßnahmen zur Datenschutzkonformität in allen Projektphasen zu entwickeln, zu implementieren und zu dokumentieren.
- Der Auftragnehmer unterstützt bei der Erstellung eines TOM-Konzeptes inkl. der Bewertung bestehender technischer und organisatorischer Maßnahmen (TOM), der Identifikation von Lücken sowie der Empfehlung der Maßnahmen zur Schließung und der Erstellung von Maßnahme Listen für die Informationssicherheit.
- Vorschlag eines Verfahrens zur Meldung von Datenschutzverletzungen nach Art. 33 DS-GVO und dessen Implementierung in Abstimmung mit dem Auftraggeber.
- Der Auftragnehmer nimmt aktiv an anlassbezogenen vordefinierten Datenschutz-Meetings teil, wenn dies notwendig ist. Ein wöchentlicher oder in Einzelfällen anlassbezogener Austausch mit der koordinierenden Stelle für Datenschutz wird vorausgesetzt. Dies umfasst Vorbereitung, Protokollierung und Nachverfolgung der Maßnahmen.
- Der Auftragnehmer begleitet und unterstützt bei der Erstellung oder Überarbeitung der grundlegenden BCM-Dokumentation.



- Der Auftragnehmer unterstützt und begleitet beim Aufbau eines Maßnahmen- und Auditmanagements.
- Der Auftragnehmer unterstützt und begleitet Zertifizierungsprozesse (BCM) insofern das Erfordernis beim Auftragnehmer besteht.
- Der Auftragnehmer unterstützt und begleitet den Auftraggeber bei der Aktualisierung der Leitlinie zur Informationssicherheit ggf. Überführung in eine Richtlinie.
- Koordination der sicherheitsrelevanten Projekte.
- Unterstützung und Begleitung des Auftraggebers bei der Erstellung und Pflege, der die Informationssicherheit betreffenden Informationen und Daten, sowie deren Dokumentation, Klassifikation und Lenkung.
- Der Auftragnehmer unterstützt und begleitet den Aufbau und die Pflege des Risikomanagements (Informationssicherheit).
- Der Auftragnehmer unterstützt und begleitet bei der Umsetzung von technischen und organisatorischen Maßnahmen.
- Der Auftragnehmer unterstützt und begleitet Zertifizierungsprozesse (Informationssicherheit), insofern das Erfordernis beim Auftragnehmer besteht.
- Darüber hinaus müssen mindestens zweimal jährlich Vor-Ort-Termine beim Auftraggeber stattfinden. Der Auftragnehmer stellt über die Vor-Ort-Termine zusätzlich sicher, dass die zur Erfüllung der Anforderungen erforderlichen Maßnahmen in den Bereichen Informationssicherheit, Datenschutz und Business Continuity Management beim Auftragnehmer erfolgt. Zudem prüft er über die Vor-Ort-Termine die tatsächliche Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen und unterzieht diese einer Bewertung hinsichtlich ihrer Wirksamkeit im operativen Umfeld. Dabei werden insbesondere physische Sicherheitsmaßnahmen, eingesetzte Systeme, Prozessabläufe, Notfall- und Wiederanlaufmechanismen sowie sonstige für die Leistungserbringung relevante Schutzvorkehrungen überprüft. Die regelmäßige Präsenz ermöglicht die frühzeitige Identifikation neuer oder veränderter Risiken, die aus organisatorischen, technischen oder personellen Änderungen resultieren können und stellt sicher, dass notwendige Anpassungsmaßnahmen rechtzeitig eingeleitet werden.
- Der Auftragnehmer verpflichtet sich zudem zu einem strukturierten und nachvollziehbaren Berichtswesen gegenüber dem Verantwortlichen des Auftraggebers. Dieses umfasst die Dokumentation der durchgeführten Vor-Ort-Prüfungen, die Darstellung festgestellter Abweichungen oder Risiken, konkrete Handlungsempfehlungen sowie den Fortschritt bereits eingeleiteter Maßnahmen. Das Berichtswesen dient der Transparenz, der Nachweisführung gegenüber internen und externen Prüfinstanzen sowie der kontinuierlichen Weiterentwicklung der Informationssicherheits-, Datenschutz- und BCM-Prozesse. Durch die Kombination aus regelmäßiger Vor-Ort-Präsenz und verlässlicher Dokumentation stellt der Auftragnehmer unter Berücksichtigung der Mitwirkung des Auftraggebers ein dauerhaft angemessenes Sicherheitsniveau sowie eine überprüfbare Compliance sicher.



3. Leistungsbereich Datenschutz (sofern einzelne Leistungen nicht bereits im Rahmen von III. Ziffer 2 erbracht werden)

Bei der Erbringung seiner Leistungen hat der Auftragnehmer alle, den Datenschutz direkt und indirekt betreffenden regulatorischen Vorgaben (z.B. DS-GVO, NDSG, BDSG, TDDDG), vollständig zu berücksichtigen und deren Einhaltung sicherzustellen.

Der Auftragnehmer hat dabei methodisch nach dem Standard-Datenschutzmodell (SDM aktuelle Version) zu arbeiten und dessen Grundsätze, insbesondere zu Gewährleistungszielen und Schutzbedarf, in seiner Vorgehensweise anzuwenden.

Die Aufgaben des DSB umfassen dabei insbesondere die nachfolgend beschriebenen Leistungen, sofern diese nicht bereits dem Aufbau des ISMS, BCMS, DSMS (**siehe unter III. Ziffer. 2)**) zuzuordnen sind:

- Der Auftragnehmer hat gemeldete Datenschutzvorfälle strukturiert und fachgerecht zu bewerten. Dies umfasst die Kategorisierung des Vorfalls, die Prüfung der Relevanz im Sinne der DS-GVO sowie die Ersteinschätzung möglicher Auswirkungen auf personenbezogene Daten.
- Der Auftragnehmer führt für jeden relevanten Datenschutzvorfall eine datenschutzrechtliche Risikoanalyse durch. Dabei sind insbesondere Eintrittswahrscheinlichkeit, Schadenshöhe und potenzielle Auswirkungen auf die Rechte und Freiheiten betroffener Personen zu ermitteln und nachvollziehbar zu dokumentieren.
- Der Auftragnehmer hat auf Basis der Bewertung und Risikoanalyse konkrete technische und organisatorische Maßnahmen zur Risikominimierung oder Schadensbegrenzung zu empfehlen. Die Maßnahmen müssen priorisiert, praktikabel und fachlich begründet sein.
- Beratung - auf Anfrage - im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Artikel 35 DS-GVO.
- Tätigkeit als unterstützende Anlaufstelle für die Aufsichtsbehörde für mit der Verarbeitung von personenbezogenen Daten zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Artikel 36 DS-GVO, und gegebenenfalls Beratung zu allen sonstigen Fragen.
- Der Auftragnehmer unterstützt die systematische Einhaltung der gesetzlichen und internen Fristen im Zusammenhang mit Betroffenenanfragen (Art. 12–23 DS-GVO) und stellt sicher, dass der Auftraggeber alle erforderlichen Schritte rechtzeitig umsetzen kann.
- Der Auftragnehmer unterstützt die Geschäftspartner Due Diligence (Aspekte des Datenschutzes).



- Der Auftragnehmer unterstützt aktiv bei der internen Abstimmung zwischen Fachbereichen, um Informationen für Betroffenenanfragen effizient zusammenzutragen und fristgerecht aufzubereiten. Er bedient sich dazu der unter **I. Ziffer 2** . benannten koordinierenden Stelle beim Auftraggeber.
- Der Auftragnehmer prüft datenschutzbezogene Aspekte von Vertragswerken, insbesondere im Hinblick auf datenschutzrelevante Nebenabreden, Sicherheitsspezifikationen, Schutzbedarfsfeststellungen und Datenklassifizierungen.
- Der Auftragnehmer bewertet neue oder geänderte Verarbeitungstätigkeiten des Auftraggebers im Hinblick auf ihre datenschutzrechtliche Zulässigkeit, dokumentiert Risiken, empfiehlt erforderliche Maßnahmen und unterstützt bei der datenschutzkonformen Ausgestaltung.
- Der Auftragnehmer übernimmt die Rolle der aktiven inhaltlichen Bearbeitung aller datenschutzrechtlicher Fragestellungen beim Auftraggeber, sodass eine Abarbeitung dieser ermöglicht wird und eine Hinweisgabe sowie Empfehlung als Ergebnis erfolgen kann. Die Bearbeitung erfolgt mit Unterstützung der koordinierenden Stelle des Auftraggebers (One-to- One im Bedarfsfall One-to-Many) sowie des jeweils anfragenden, betroffenen sowie verantwortlichen Bedarfstragenden.
- Die Unterstützung bei der Meldung von Datenschutzverletzungen nach Art. 33 DSGVO innerhalb von 72 Stunden ist sicherzustellen.

4. Leistungsbereich Informationssicherheit (sofern einzelne Leistungen nicht bereits im Rahmen von III. Ziffer 2 erbracht werden)

Der Auftragnehmer muss bei seiner Arbeit die BSI-Standards 200-1, 200-2, 200-3 sowie 200-4 verbindlich berücksichtigen und deren Anforderungen in seinen Arbeitsprozessen umsetzen. Die BSI - Absicherung in der Ausprägung „Standard“ ist das Ziel.

Der Auftragnehmer muss sicherstellen, dass Best Practices aus den ISO-Normen 27001 bis 27005 in seinen Vorgehensweisen und Dokumentationen integriert sind, insofern diese sinnvoll sind.

Die Aufgaben des ISB umfassen dabei insbesondere die nachfolgend beschriebenen Leistungen, sofern diese nicht bereits dem Aufbau des ISMS, BCMS oder DSMS (**siehe unter III. Ziffer. 2**) zuzuordnen sind:

- Anlassbezogene Beratung des Auftraggebers (z.B. bei der Beschaffung von neuer Software).
- Koordination und Steuerung der Informationssicherheitsprozesse.
- Überprüfung der Realisierbarkeit und Initialisierung von Sicherheitsmaßnahmen.
- Untersuchung und Dokumentation von Sicherheitsvorfällen.
- Unterstützung bei der Geschäftspartner Due Diligence (Aspekte der Informationssicherheit).



- Bewertung der Risiken in der Lieferkette (Aspekte der Informationssicherheit).
- Der Auftragnehmer unterstützt und begleitet den Auftraggeber im Bereich des Schwachstellenmanagements.
- Der Auftragnehmer übernimmt die Rolle der aktiven inhaltlichen Bearbeitung aller, die Informationssicherheit betreffenden, Fragestellungen beim Auftraggeber, sodass eine Abarbeitung dieser ermöglicht wird und eine Hinweisgabe sowie Empfehlung als Ergebnis erfolgen kann. Die Bearbeitung erfolgt mit Unterstützung der koordinierenden Stelle (One-to-One im Bedarfsfall One-to-Many) sowie des jeweils anfragenden, betroffenen sowie verantwortlichen Bedarfstragenden.

5. Leistungsbereich BCM (sofern einzelne Leistungen nicht bereits im Rahmen von III. Ziffer 2 erbracht werden)

Der Auftragnehmer muss bei seiner Arbeit den BSI-Standard 200-4 verbindlich berücksichtigen und deren Anforderungen in seinen Arbeitsprozessen umsetzen.

Der Auftragnehmer muss sicherstellen, dass neben dem Standard auch Best Practices aus seinen eigenen Erfahrungen in seine Vorgehensweisen und Dokumentationen einfließen, insofern diese sinnvoll sind.

Die Aufgaben umfassen dabei insbesondere die nachfolgenden beschriebenen Leistungen, insofern diese nicht bereits dem Aufbau des ISMS, BCMS oder DSMS (**siehe unter III. Ziffer. 2)** zuzuordnen sind:

- Der Auftragnehmer begleitet und unterstützt die aktive Bearbeitung aller, das BCM betreffenden, Fragestellungen beim Auftraggeber, sodass eine Abarbeitung dieser ermöglicht wird und eine Hinweisgabe sowie Empfehlung als Ergebnis erfolgen kann. Die Bearbeitung erfolgt mit Unterstützung der koordinierenden Stelle (One-to-One im Bedarfsfall One-to-Many) sowie des jeweils anfragenden, betroffenen sowie verantwortlichen Bedarfstragenden.
- Der Auftragnehmer begleitet und unterstützt bei BCM bezogenen Audits und Kontrollen.
- Der Auftragnehmer unterstützt und begleitet bei der Aufarbeitung sicherheitsrelevanter Ereignisse (BCM).
- Unterstützung bei der Geschäftspartner Due Diligence (Aspekte des BCM).



6. Leistungsbereich Schulung, Awareness und Wissenstransfer

6.1. Awarenessmaßnahmen und Wissenstransfer

Der Auftragnehmer gewährleistet den Wissenstransfer innerhalb der Organisation des Auftraggebers, indem geeignete Kommunikationsformate (z. B. Newsletter, interne Informationskanäle, Wissensaustauschplattformen, E-Learning-Formate) vorgeschlagen, durchgeführt und fortlaufend hinsichtlich der Effektivität geprüft werden. Der Auftragnehmer hat daher wiederkehrende (grundsätzlich halbjährliche) Awareness-Maßnahmen für die Mitarbeitenden des Auftragnehmers durchzuführen, um das Bewusstsein für Datenschutz, Informationssicherheit, BCM der Mitarbeiter des Auftraggebers nachhaltig zu stärken und aufrechtzuerhalten.

6.2. Schulungen

Zusätzlich ist der Auftragnehmer verpflichtet, nach einem gesonderten Abruf durch den Auftraggeber Schulungen (grundsätzlich online) für die Mitarbeitenden des Auftraggebers durchzuführen, um sicherzustellen, dass alle Mitarbeitenden über die notwendigen erforderlichen Kenntnisse im Datenschutz, der Informationssicherheit sowie im Bereich BCM verfügen. Die Schulungen sollen dabei grundsätzlich eine Dauer von mindestens 90 Minuten haben. Die Schulungen sind nach Zielgruppen (Rollen) zu gestalten. Eine Abstimmung dazu ist mit dem Auftraggeber erforderlich.

7. Leistungsbereich anlassbezogene Unterstützung bei sicherheitsrelevanten Ereignissen (optional)

Der Auftragnehmer bietet dem Auftraggeber optional Leistungen zur anlassbezogenen Unterstützung bei sicherheitsrelevanten Ereignissen an. Die Leistungen können unabhängig von den übrigen Leistungsbestandteilen dieser Ausschreibung sowie unabhängig vom aktuellen Umsetzungs- oder Reifegrad bestehender Strukturen in den Bereichen Informationssicherheit, Datenschutz oder Business Continuity Management in Anspruch genommen werden.

Die Beauftragung erfolgt ausschließlich im konkreten Ereignisfall und nur auf Abruf des Auftraggebers.

Ziel der Leistungen ist es, den Auftraggeber bei akuten sicherheitsrelevanten Ereignissen, erheblichen Störungen sowie Krisen- oder Notfallsituationen mit IT-Bezug fachlich zu unterstützen, um eine strukturierte Lageeinschätzung zu ermöglichen, negative Auswirkungen zu begrenzen und eine belastbare Grundlage für weitere Entscheidungen zu schaffen.

Die Leistungserbringung muss in einer zweistufigen Logik erfolgen:



a. Stufe 1: Erstunterstützung im Ereignisfall (Handlungsfähigkeit)

Mit dem Abruf der Leistungen wird zunächst eine klar abgegrenzte Erstunterstützung ausgelöst. Diese dient der unmittelbaren Lageeinschätzung und Stabilisierung der Situation und ermöglicht eine unverzügliche Aufnahme der Unterstützung, ohne dass vorab weitergehende Abstimmungen erforderlich sind.

Der Leistungsumfang der Erstunterstützung umfasst insbesondere:

- fachliche Unterstützung unmittelbar nach Bekanntwerden eines sicherheitsrelevanten Ereignisses,
- strukturierte Ersteinschätzung der Lage unter Berücksichtigung technischer, organisatorischer und prozessualer Auswirkungen,
- Unterstützung bei der Ableitung und Priorisierung geeigneter Sofortmaßnahmen zur Stabilisierung der Situation und zur Begrenzung weiterer Auswirkungen,
- erste fachliche Einordnung möglicher weiterer Handlungsbedarfe.

Die Vergütung der Erstunterstützung erfolgt zum Pauschalpreis gemäß Nr. 4.2 des Teil C EVB-IT-Dienstvertrag. Die konkrete Ausgestaltung der Leistungen obliegt dem fachlichen Ermessen des Auftragnehmers im Rahmen des vorstehend festgelegten Leistungsumfangs.

b. Stufe 2: Erweiterte Unterstützung im Ereignisfall

Sofern sich im Anschluss an die Erstunterstützung ein weitergehender Unterstützungsbedarf ergibt, kann der Auftraggeber für den konkreten Ereignisfall eine erweiterte Unterstützung im vergaberechtlich zulässigen Umfang beim Auftragnehmer beauftragen.

Der zusätzliche Leistungsumfang wird situationsabhängig konkretisiert und kann insbesondere umfassen:

- vertiefende technische Analysen und IT-forensische Untersuchungen,
- Analyse des Ereignisverlaufs einschließlich Identifikation von Ursachen, Angriffspfaden oder begünstigenden Faktoren,
- Unterstützung bei der fachlichen Einordnung datenschutzrechtlicher, informationssicherheitsbezogener oder betriebsrelevanter Fragestellungen,
- Ableitung weitergehender Maßnahmen und Handlungsempfehlungen zur nachhaltigen Stabilisierung und Verbesserung.

Für die erweiterte Unterstützung („Stufe 2“) holt der Auftraggeber vorab ein konkretes Leistungsangebot beim Auftragnehmer ein. Der Auftragnehmer hat keinen Anspruch darauf, dass der Auftraggeber sein konkretes Leistungsangebot beauftragt. Eine Beauftragung erfolgt überdies nur, sofern sie vergaberechtlich zulässig ist.



ENTWURF