

Service-Level-Agreement

zum Betrieb der digitalen IHK-Prüfungsplattform

Zwischen der

Deutschen Industrie- und Handelskammer
Breite Straße 29
D-10178 Berlin

und der

[Dienstleister]
[Adresse]

1. Präambel & Zweck

Dieses Service-Level-Agreement (SLA) definiert die verbindlichen Service-, Betriebs-, Support- und Wartungsanforderungen für den Betrieb der digitalen IHK-Prüfungsplattform. Es referenziert die Leistungsbeschreibung (05_Digitales-Pruefen_Anlage-01_Leistungsbeschreibung) und bildet zusammen mit dem Auftragsverarbeitungsvertrag (12_Digitales-Pruefen_Anlage-03_AVV inklusive Muster) und den technischen und organisatorischen Maßnahmen (TOMs) die organisatorische und rechtliche Grundlage für den Betrieb ab dem ersten Produktivtag.

Die in der Leistungsbeschreibung vorgegeben **KPIs** stellen verbindliche Vertragspflichten des Dienstleisters dar und definieren Mindestanforderungen, deren Einhaltung für den sicheren, stabilen, nutzerorientierten, datenschutzkonformen und rechtssicheren Betrieb der Prüfungsplattform erforderlich ist.

Nicht Bestandteil des SLA sind:

- Endgeräte der Prüflinge,
- kundenseitige Netzwerke oder lokale IT-Infrastruktur,
- Drittsysteme und externe Dienste außerhalb des direkten Einflussbereichs des Dienstleisters.

Abhängigkeiten zu Drittsystemen, kundenseitiger Infrastruktur oder externen Dienstleistern werden bei der Bewertung der SLA-Einhaltung angemessen berücksichtigt. In Fällen von gemischter Verantwortlichkeit, insbesondere beim Zusammenspiel mehrerer Systeme oder Parteien, wirken Dienstleister und Auftraggeber gemeinsam auf eine Ursachenanalyse sowie die schnellstmögliche Wiederherstellung eines stabilen Betriebs hin.

Die Nutzung der Plattform erfolgt unter der Voraussetzung, dass die definierten technischen Rahmenbedingungen (z. B. unterstützte Browser und Systemumgebungen) eingehalten werden.

Abweichungen von diesem SLA sind nur zulässig, soweit sie ausdrücklich vertraglich vereinbart und durch geeignete Maßnahmen kompensiert werden.

2. Servicepersonal- und zeiten

Der Dienstleister besetzt für den Betrieb die folgenden Rollen mit zugehörigem Aufgabenprofil:

- **Service Manager:**
verantwortet den operativen Betrieb,
führt weitergehende Einschätzungen, Re-Priorisierungen und Eskalationen,
orchestriert die Behebung von Incidents,
führt das Change-Management,
richtet einen Krisenstab auf Seiten des Dienstleisters ein,
koordiniert die Service-Reviews,
ist für kritische Incidents auch außerhalb der Servicezeiten telefonisch erreichbar.
- **1st Level Support / Service Desk:**
ist erste Anlaufstelle für Fragen, Meldungen und Tickets,
führt Ersteinschätzung und Priorisierung,
behebt falls möglich direkt Incidents,
leitet Incidents ggf. an nachfolgende Supportebenen weiter,
ist an Prüfungstagen für kritische Incidents telefonisch erreichbar.
- **2nd Level Support / Application Management (DevOps):**
überwacht das System,
übernimmt wiederkehrende technische Aufgaben, insbesondere Sicherheitsupdates,
Deployments und sonstige Wartungsaufgaben,
unterstützt bei der Behebung von Incidents.
- **3rd Level Support:**
ist die letzte Instanz zur Behebung von Incidents,
berät bei Weiterentwicklung und technischen Innovationen.

Servicezeiten des Dienstleisters sind:

Rolle	Zeit
Service Manager & Service Desk	Mo–Fr, 08:00–17:00 CET/CEST

An Prüfungstagen gilt aufgrund der erhöhten Kritikalität der Verfügbarkeit der Plattform:

Rolle	Zeit
Service Manager & 1st-, 2nd- und 3rd-Level-Support	Mo–Fr, 06:00–18:00 CET/CEST

Um Prüfungstage herum liegen sogenannte Prüfungsfenster, in denen erhöhte Vorsicht im Betrieb und im Umgang mit der Anwendung geboten ist. Prüfungsfenster umfassen:

- den Tag der Prüfungsdurchführung,
- bei initialen Prüfungsläufen, Großprüfungstagen oder erhöhtem Risiko zusätzlich einen vorgelagerten Vorbereitungszeitraum von 3 Werktagen sowie
- den Zeitraum bis zur Bereitstellung der Prüfungsdaten an die umliegenden Systeme.

3. Sicherheit und Datenschutz

Die Anforderungen an Sicherheit und Datenschutz werden im Datenschutzkonzept, im Auftragsverarbeitungsvertrag (AVV) sowie in den technischen und organisatorischen Maßnahmen (TOM) spezifiziert. Die darin enthaltenen Anforderungen sind verbindlich umzusetzen.

Bei Widersprüchen zwischen diesem SLA, dem Auftragsverarbeitungsvertrag (AVV) und den TOM gilt – soweit rechtlich zulässig – jeweils die strengere Anforderung zugunsten des Auftraggebers. Datenschutzrechtliche Anforderungen aus AVV und DSGVO bleiben unberührt und gehen entgegenstehenden Regelungen dieses SLA vor.

Der Auftraggeber bzw. die Bezugsberechtigten bleibt zu jedem Zeitpunkt allein verfügbungsberechtigt über alle im Rahmen der Leistungserbringung verarbeiteten Daten.

Sicherungen (Backups) sind innerhalb der vereinbarten Fristen datenschutzkonform zu bereinigen.

3.1 Sicherheitsupdates

Der Dienstleister gewährleistet die Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und prüfungsrelevanten Daten. Automatisierte Sicherheitsprüfungen (z. B. Schwachstellen-Scans, Abhängigkeitsprüfungen) werden regelmäßig durchgeführt. Werden Sicherheitslücken erkannt, erfolgt eigenständig das rechtzeitige Einspielen aktueller softwaretechnischer Sicherheitsupdates.

Kritische Sicherheitslücken (**CVSS $\geq$ 9.0**) sind innerhalb von **5** Werktagen durch geeignete Maßnahmen zu beheben oder wirksam zu entschärfen. Dies umfasst insbesondere die Einspielung eines Patches, die Deaktivierung der betroffenen Komponente, eine Konfigurationsänderung oder gleichwertige technische Mitigationsmaßnahmen. Sicherheitslücken mit hohem Risiko (**CVSS 7.0–8.9**) sind innerhalb von **15** Werktagen zu entschärfen.

Sofern eine vollständige Behebung innerhalb dieser Fristen technisch nicht möglich ist (z. B. mangels verfügbarer Herstellerlösung), hat der Dienstleister unverzüglich eine Risikobewertung vorzunehmen, geeignete Übergangsmaßnahmen umzusetzen sowie einen verbindlichen Plan zur vollständigen Behebung vorzulegen. Eine Risikoakzeptanz bedarf der ausdrücklichen Zustimmung des Auftraggebers.

Sicherheitslücken mit niedrigerem Risk Score sind möglichst mit dem nächsten regulären Release zu beheben.

4. Verfügbarkeit

Ein Verstoß gegen die Verfügbarkeitsvorgaben in der Leistungsbeschreibung gilt als **schwerwiegender SLA-Verstoß (P1)**.

Sofern einzelne Systembestandteile noch nicht vollständig implementiert und getestet sind, sind diese klar zu kennzeichnen.

4.1 Deployments

Der Dienstleister stellt sicher, dass Deployments und Wartungsmaßnahmen in Abstimmung mit dem Auftraggeber mindestens 5 Werktage im Voraus so geplant und durchgeführt werden, dass der Prüfungsbetrieb nicht beeinträchtigt wird. Während definierter Prüfungsfenster gilt ein „Change Freeze“. In diesem dürfen nur Deployments zum Einspielen funktionaler oder sicherheitskritischer Maßnahmen erfolgen, die zur Stabilisierung oder Absicherung des Prüfungsbetriebs zwingend erforderlich sind. Betroffene Stakeholder sind rechtzeitig zu informieren.

Deployments dürfen ausschließlich in den folgenden vordefinierten Wartungsfenstern und nach vorheriger Abstimmung und Freigabe durch den Auftraggeber durchgeführt werden: **Montag–Donnerstag, 20:00–22:00 Uhr** (CET/CEST). Abweichungen von diesen Wartungsfenstern sind in begründeten Ausnahmefällen möglich.

Deployments sind so durchzuführen, dass die Verfügbarkeit der Plattform möglichst nicht beeinträchtigt wird. Kurzzeitige Beeinträchtigungen von unter **5 Minuten** sind zulässig.

Bei Abweichungen, Störungen oder notwendigen Rollbacks erfolgt unmittelbar eine Information des Dienstleisters an den Auftraggeber.

4.2 Business Continuity & Disaster Recovery (BCP/DRP)

Business Continuity und Disaster Recovery umfassen alle Maßnahmen zur Sicherstellung der Aufrechterhaltung bzw. Wiederherstellung des Prüfungsbetriebs im Falle von Störungen, Ausfällen oder Katastrophenszenarien.

Der Dienstleister führt mindestens einmal im Quartal einen vollständigen Test der Disaster-Recovery-Fähigkeiten durch, die Ergebnisse sind zu dokumentieren.

5. Performance

Die funktionalen und technischen Anforderungen an Performance, Skalierbarkeit und Lastverarbeitung sind in der Leistungsbeschreibung definiert.

Performancebedingte Beeinträchtigungen, die zu einer Einschränkung oder Nichtverfügbarkeit prüfungsrelevanter Funktionen führen, gelten als Incidents im Sinne dieses SLA.

Ein **P1 Incident** liegt vor, wenn Prüflinge sich nicht einloggen können, Aufgaben nicht laden, Antworten nicht eingeben oder nicht speichern können.

6. Monitoring & Kontinuierliche Optimierung

Relevante Kennzahlen zur Stabilität, Performance und Skalierung werden kontinuierlich überwacht.

Abweichungen von definierten Leistungskennzahlen werden analysiert und führen zu geeigneten Optimierungsmaßnahmen.

Ein Ausfall oder eine wesentliche Einschränkung des Monitoring-Systems stellt einen SLA-Verstoß dar.

Sicherheitsrelevante Vorfälle müssen unverzüglich erkannt und als Incident klassifiziert werden, der Auftraggeber ist darüber spätestens innerhalb von **30 Minuten** zu informieren.

Störungen von Schnittstellen, die zu einer Verzögerung, fehlerhaften Verarbeitung oder einem Ausfall der Datenübertragung führen und die Prüfungsdurchführung beeinträchtigen, müssen ebenfalls unverzüglich erkannt und als **P1 Incident** klassifiziert werden.

Identifizierte Verbesserungspotenziale werden dokumentiert, priorisiert und im Rahmen des kontinuierlichen Verbesserungsprozesses umgesetzt.

7. Incident-, Problem- & Change-Management

7.1 Klassifizierung von Incidents und Fehlern

Der Dienstleister stellt sicher, dass alle eingehenden Meldungen und Tickets nach der folgenden Triage-Regel eingestuft werden:

P1 – Kritisch:

Bedingungen: Prüfungsbetrieb unmittelbar beeinträchtigt, Login oder Durchführung nicht möglich, flächendeckende Funktionsstörung.

P2 – Hoch:

Bedingungen: Schwere Funktionseinschränkung ohne vollständigen Prüfungsabbruch, Fehler in der Korrektur- oder Auswertungsprozess, mehrere Standorte betroffen.

P3 – Mittel:

Bedingungen: Einzelne Nutzer oder Prüfungsstationen betroffen; Workaround vorhanden; keine Prüfungsgefährdung.

P4 – Niedrig:

Bedingungen: Kosmetische Fehler, Optimierungen.

Sonderregel:

Tickets, die innerhalb von 48 Stunden vor oder während Prüfungstagen auftreten, werden zunächst vorsorglich mindestens als P2, bei Funktionsverlust oder Login-Problemen als P1 eingestuft und müssen unverzüglich hinsichtlich ihrer tatsächlichen Prüfungsrelevanz bewertet werden.

7.2 Reaktions- und Behebungszeiten

Die maßgeblichen Reaktions- und Behebungszeiten beginnen mit dem frühesten der folgenden Zeitpunkte:

- Eingang der Meldung über einen vereinbarten Kommunikationskanal,
- automatische Erkennung des Vorfalls durch Monitoring-Systeme, oder
- sonstige Kenntniserlangung durch den Dienstleister.

Für eingehende Incidents sind wie folgt definiert:

Priorität	Erstreaktion	Workaround/Restore	Dauerhafte Behebung
P1	≤ 30 Min	≤ 2 Std	≤ 2 Werktage
P2	≤ 2 Std	≤ 8 Std	≤ 10 Werktage
P3	≤ 2 Werktage	n/a	Mit nächstem Release
P4	≤ 2 Werktage	n/a	Mit nächstem Release

Sonderregel:

Auch ein gleichzeitiges Auftreten mehrerer P2-Incidents mit potenzieller Auswirkung auf mehrere IHKs bzw. in den 48 Stunden vor oder während Prüfungstagen löst einen P1-Incident aus.

Erstreaktion:

Der Dienstleister informiert die zentralen Ansprechpartner des Auftraggebers (DIHK) sowie die meldende IHK über den Vorfall, deren Annahme und den aktuellen Status.

Service Requests:

Für Anfragen für Konfigurationsänderungen, Rollen-/Rechteeanpassungen, Datenexporte etc. wird eine Rückmeldung innerhalb von 2 Werktagen erwartet mit einer ersten Kategorisierung nach Standardanfrage (im Umfang der Servicepauschale enthalten), Sonderanfrage oder Change Request (dauerhafte Änderungen an der Plattform). Die Lösungszeit bestimmt sich stark durch die Anfrage selbst. Requests, die sich auf bevorstehende Prüfungen beziehen, werden priorisiert.

7.3 Eskalation / Krisenstab

Zur Koordination prüfungsrelevanter Incidents oder andersartig kritischer P1 Vorfälle richtet der Dienstleister unverzüglich einen digitalen Krisenstab mit dem Auftraggeber ein, beispielsweise über Chat Room in MS Teams.

Der Dienstleister leitet parallel geeignete Maßnahmen zur Stabilisierung des Systems ein, um Auswirkungen auf den Prüfungsbetrieb zu minimieren.

Sollten Prüfungen **länger als 2 Stunden** erheblich gestört sein, erfolgt eine Eskalation an die Geschäftsführung/Direktion.

Vorsorglicher Stab zum Produktionsstart:

In den ersten Tagen und Wochen nach Produktionsstart tauschen sich Dienstleister und Auftraggeber eng und mitunter mehrmals täglich über den Status des Systems, eingehende Meldungen und die Priorisierung entsprechender Maßnahmen aus.

Auch nach dem Deployment von Major Releases sollten Dienstleister und Auftraggeber in engem Austausch stehen.

7.4 Support bestimmter Nutzergruppen

Der Support wird so organisiert, dass unterschiedliche Nutzergruppen in unterschiedlichen Situationen spezifisch unterstützt werden. Support wird hier geleistet seitens Dienstleister und Auftraggeber:

Situation Prüfungsbereitstellung, Nutzergruppe Aufgabenerstellungseinrichtungen (AEEs):

Supportlevel	Alle
Verantwortliche Rolle	Dienstleister
typische Supportfälle	- Unvollständiger Import von Prüfungsaufgaben, Aufgaben werden fehlerhaft dargestellt, Probleme mit Log-In oder Authentifizierung, Erstellung Logiken von Wahlpflichtfächern
Kompetenzen	- Tiefgreifendes Verständnis des Prüfungsprozesses - Spezifisches Wissen zur Schnittstelle zu den AEEs und dem zugrundeliegenden Datenmodell - Spezifisches Wissen zur Benutzeroberfläche für die Aufgabenersteller

Situation Prüfungsdurchführung, Nutzergruppe IHK-Mitarbeiter*innen / technischer Support vor Ort:

Supportlevel	1st Level	2nd		3rd
Verantwortliche Rolle	Prüfungsaufsichten	IHK-Mitarbeiter*innen	Technischer Support vor Ort	Dienstleister
typische Supportfälle	z.B. Log-In funktioniert nicht, Fragen zur Navigation durch die Plattform, Fragen zu Funktionalitäten, Melden von fehlerhaften Aufgaben, Austausch von Endgeräten	z.B. mehrere Aufsichten melden ähnliche Probleme, eine Prüfungsaufsicht meldet sich und braucht Hilfe ein Problem korrekt zu verorten (Software oder lokale Infrastruktur)	z.B. Probleme mit dem lokalen WLAN, der Stromversorgung oder Endgeräten	z.B. Fehlerhafte Darstellung von Aufgaben beheben, kurzfristiger Austausch von Prüfungen, Fehlersuche
Kompetenzen	- Gute System und Prozesskenntnis - Erfassung und Verortung der	- Problemanalyse bzw. Verortung des Themas - Kenntnis der und Durchführung von	- Bereitstellung und Monitoring	- Monitoring des Prüfungssystems - Problemanalyse und -behebung

	Supportthemen (Problem mit Endgerät oder Software) - Arbeiten nach Leitfäden und Checklisten	Notfallprozessen, Eskalationsstufen etc. - Workarounds kennen, testen, und kommunizieren (auch an andere IHKs)	der lokalen Infrastruktur - Behebung von technischen Problemen der lokalen Infrastruktur	- Einschätzung, ob Quick-Fixes möglich sind
Übergangs- zeitpunkt nächstes Support-Level	- Keine Lösung mit Standardleitfäden möglich - Problem ist nicht eindeutig reproduzierbar, - Fachliche Sonderfälle, - Zeitkritische Vorgänge, - Mehrere identische Meldungen (Hinweis auf systematisches Problem)	- Verdacht auf System- oder Softwarefehler - Fachlich alles geprüft, aber Problem bleibt bestehen - Fehler tritt reproduzierbar bei mehreren Nutzern auf - Eingriffe außerhalb der eigenen Zuständigkeit erforderlich		
Übergabe- inhalte nächstes Support-Level	- Was genau funktioniert nicht? (Problembeschreibung, Screenshots), - Seit wann tritt das Problem auf? - Für wen / wie häufig? - Welche Schritte wurden bereits versucht? - System oder Vorgangsnummern (sofern vorhanden)	- Genaue Fehlerbeschreibung - Reproduktionsschritte - Log-Auszüge / Screenshots - Abgrenzung: „Was kann definitiv ausgeschlossen werden?“		

Situation Prüfungskorrektur, Nutzergruppe Prüfer*innen:

Supportlevel	1st Level	2nd
Verantwortliche Rolle	IHK-Mitarbeiter*innen	Dienstleister
typische Supportfälle	- Probleme mit Log-Ins, - Zuordnung zu Prüfungsausschuss falsch, - Fragen zu Funktionalitäten	- Darstellungsfehler von Korrekturen, Funktionsausfall etc.
Kompetenzen	- Gute System und Prozesskenntnis - Arbeiten nach Leitfäden und Checklisten - Problemanalyse bzw. Verortung des Themas	- Problemanalyse und - behebung - Einschätzung, ob Quick- Fixes möglich sind

Übergangszeitpunkt nächstes Support- Level	- Keine Lösung mit Standardleitfäden möglich - Problem ist nicht eindeutig reproduzierbar, - Fachliche Sonderfälle, - Zeitkritische Vorgänge, - Mehrere identische Meldungen (Hinweis auf systematisches Problem)	
Übergabeinhalte nächstes Support- Level	- Was genau funktioniert nicht? (Problembeschreibung, Screenshots), - Seit wann tritt das Problem auf? - Für wen / wie häufig? - Welche Schritte wurden bereits versucht? - System oder Vorgangsnummern (sofern vorhanden)	

Situation Prüfungsplanung und laufender Betrieb, Nutzergruppe IHK-Mitarbeiter*innen:

Supportlevel	Alle
Verantwortliche Rolle	Dienstleister
typische Supportfälle	- Download von Prüfungsakte funktioniert nicht, Probleme beim Upload von Daten (Prüflinge, Prüfer, etc.), Probleme bei der Erstellung von Log-In Codes/Tischkarten
Kompetenzen	- Tiefgreifendes Verständnis des gesamten digitalen IHK-Prüfungssystems und des Prüfungsprozesses - Spezifisches Wissen zur Schnittstelle/Datenhub mit den IHK-Verwaltungssystemen und dem zugrundeliegenden Datenmodell - Spezifisches Wissen zur Benutzeroberfläche für die IHK-Mitarbeiter*innen

7.5 Change-Management

Der Dienstleister unterstützt und berät den Auftraggeber mit seinen Aufgabenerstellungseinrichtungen, insbesondere um neue digitale Aufgaben- und ggf. Prüfungsformate fachlich fundiert zu entwickeln und effizient in die Plattform zu integrieren, bspw. in Form gemeinsamer Workshops.

Neue Formate und andere Änderungswünsche durchlaufen ein ausgewiesenes Change-Management Verfahren des Product Owners, bevor deren Umsetzung verbindlich beauftragt und in die Anwendung mitaufgenommen wird.

7.6 Ticketqualitäts- und Annahmekriterien

Damit Supportfälle effizient bearbeitet werden können, müssen alle vom Auftraggeber eingereichten Tickets die folgenden Mindestangaben enthalten:

- Problembeschreibung:
Klare und vollständige Beschreibung des Symptoms sowie der beobachteten Fehlfunktion.
- Reproduktionsschritte:
Schritt-für-Schritt-Darstellung, wie der Fehler ausgelöst wurde (falls möglich).
- Betroffener Personenkreis:
Anzahl der betroffenen Nutzer*innen bzw. Prüfungsstationen; Angabe, ob prüfungsrelevant.
- Technische Rahmenbedingungen:
Browser und Version, Gerätetyp, Betriebssystem, Standort, Zeitpunkt des Auftretens.
- Nachweise:
Screenshots, Videos, Fehlermeldungen, Logauszüge (falls verfügbar).
- Dringlichkeit / Auswirkung:
Einschätzung der betroffenen Prozesse, ob Workaround existiert, ob Prüfungsbetrieb gefährdet ist.

Regeln zur Annahme von Tickets:

- Tickets, die diese Mindestangaben nicht enthalten, werden grundsätzlich zur Ergänzung zurückgegeben.
- Fehlende Ticketangaben dürfen jedoch die Bearbeitung von P1-, P2- oder prüfungsrelevanten Incidents nicht verzögern. In diesen Fällen beginnt der Dienstleister unverzüglich mit der Bearbeitung und fordert fehlende Informationen parallel beim Auftraggeber nach.
- P1-Fälle müssen zusätzlich unverzüglich über eine telefonische Hotline oder einen vorgesehenen P1-Kanal gemeldet werden. Die Bearbeitung eines P1-Incidents darf jedoch nicht davon abhängig gemacht werden, dass die Meldung über den vorgesehenen Kanal erfolgt ist.

- Nach Erstellung eines Tickets kann die Kommunikation mit Bezug darauf auch über E-Mails fortgeführt werden, insbesondere zum Austausch von Berichten und Dokumentationen als Anlage.

Regel zum Abschluss von Tickets:

- Für alle kritischen Incidents (P1/P2) werden strukturierte Root-Cause-Analysen (RCA) erstellt und im Ticket dokumentiert, die mindestens umfassen: Auslöser und Chronologie, betroffene Systeme, Auswirkungen auf den Betrieb, Dauer und Maßnahmen der kurzfristigen Behebung sowie Empfehlungen zur Vermeidung zukünftiger Vorfälle.

7.7 Ticket-System

Alle Incidents und Requests müssen über ein einheitliches Ticket-System erfasst, priorisiert und nachverfolgt werden.

Das System muss unterstützen (inkl. Suchfilter): o.a. Prioritäten, Mandanten-IDs, Kategorien (Funktion, Modul, Browser, Gerät etc.), Status, Historie, automatische Benachrichtigungen bei Prioritätsänderungen und SLA-Gefährdungen sowie Datenaufbewahrung von mindestens **60** Monaten. Eine Integration mit dem Monitoringsystem ist wünschenswert.

8. Risikomanagement

Der Dienstleister führt ein Risikomanagement zur Identifikation, Bewertung, Steuerung und Überwachung von Risiken mit potenziellen Auswirkungen auf Verfügbarkeit, Datenintegrität oder Prüfungsdurchführung. Risiken sind frühzeitig zu erkennen, zu bewerten, als Incident zu priorisieren, in Form eines Tickets zu dokumentieren und entsprechend ihrer Kritikalität zu behandeln. So können Monitoring-Daten, die eine bestimmte Tendenz zeigen, noch vor Eintritt einer problematischen Situation zu einem Risiko Ticket führen. Maßnahmen zur Risikominimierung werden systematisch erfasst und priorisiert.

9. Schulungen

Der Dienstleister erstellt für die Schulung der gegebenen Rollen Aufgabenersteller, Prüfungskoordinatoren, Prüfungsaufsicht, IHK-Administratoren Benutzerhandbücher oder Unterrichtsmaterialien. Anwenderschulungen werden grundsätzlich durch den Auftraggeber oder vom Auftraggeber beauftragte Drittunternehmer durchgeführt.

Auf Anforderung unterstützt der Dienstleister die Anwenderschulungen des Auftraggebers (voraussichtlich bis zu 8 online Schulungen pro Jahr) direkt.

Für Prüfungsteilnehmer werden Demo-Prüfungen bereitgestellt.

10. Minderleistungen & Service Credits

Die Nichteinhaltung definierter Vorgaben, insbesondere eine Nichterfüllung eines KPI der Leistungsbeschreibung stellt unabhängig vom Eintritt eines konkreten Schadens oder einer

unmittelbaren Gefährdung einen SLA-Verstoß dar. Im Falle eines Verstoßes ist der Auftraggeber – unbeschadet weiterer gesetzlicher und vertraglicher Rechte – insbesondere berechtigt,

- eine Eskalation auszulösen,
- Service Credits geltend zu machen,
- die Vorlage und Umsetzung eines verbindlichen Maßnahmenplans zu verlangen,
- eine Zurückbehaltung oder Minderung vereinbarter Vergütung vorzunehmen sowie
- bei schwerwiegenden oder wiederholten Verstößen eine außerordentliche Kündigung auszusprechen.

Service Credits dienen der Kompensation von Qualitätsmängeln und führen zu Gutschriften zugunsten des Auftraggebers, anhand des folgenden Kataloges. Die Gutschrift für den Auftraggeber ist bei insgesamt 5 % der geschuldeten Vergütung im Bezugszeitraum des laufenden Kalenderjahres gedeckelt.

Verfügbarkeit an Prüfungstagen:

SOLL	Schwerwiegender SLA-Verstoß (P1)	SLA-Verstoß (P2)
≥ 99,95 %	≤ 99,90 %	< 99,95 %

Gutschrift bei schwerwiegendem SLA-Verstoß (P1) = 0,2% der geschuldeten Vergütung im Bezugszeitraum des laufenden Kalenderjahres

Gutschrift bei SLA-Verstoß (P2) = 0,1% der geschuldeten Vergütung im Bezugszeitraum des laufenden Kalenderjahres

Verfügbarkeit außerhalb von Prüfungstagen:

SOLL	SLA-Verstoß (P2)
≥ 99,90 %	< 99,90 %

Gutschrift bei SLA-Verstoß (P2) = 0,1% der geschuldeten Vergütung im Bezugszeitraum des laufenden Kalenderjahres

Performance:

SOLL	Schwerwiegender SLA-Verstoß (P1)	SLA-Verstoß (P2)
KPIs gemäß Leistungsbeschreibung Kap. 3.4.7	Verletzung eines KPIs (Kap. 3.4.7 der Leistungsbeschreibung) an 5 nicht aufeinanderfolgenden Tagen in einem Quartal mit einer Abweichung um den Faktor 1,5 oder höher	Verletzung eines KPIs (Kap. 3.4.7 der Leistungsbeschreibung) an 3 nicht aufeinanderfolgenden Tagen in einem Quartal mit einer Abweichung um den Faktor 1,5 oder höher oder

		an 5 nicht aufeinanderfolgenden Tagen in einem Quartal mit einer Abweichung um einen Faktor geringer als 1,5
--	--	--

Gutschrift bei schwerwiegendem SLA-Verstoß (P1) = 0,2% der geschuldeten Vergütung im Bezugszeitraum des laufenden Kalenderjahres

Gutschrift bei SLA-Verstoß (P2) = 0,1% der geschuldeten Vergütung im Bezugszeitraum des laufenden Kalenderjahres

Datenverlust:

SOLL	Schwerwiegender SLA-Verstoß (P1)
<= 0,001 %	Jeglicher Datenverlust über den SOLL-Wert hinaus (evtl. Schadensersatzansprüche bleiben unberührt)

Gutschrift bei schwerwiegendem SLA-Verstoß (P1) = 0,2% der geschuldeten Vergütung im Bezugszeitraum des laufenden Kalenderjahres

Service Level Agreement:

SOLL	Schwerwiegender SLA-Verstoß (P1)	SLA-Verstoß (P2)
KPIs gemäß Leistungsbeschreibung und Service Level Agreement	5 P1 Incidents in einem Quartal, die nicht in den definierten Reaktions-/Workaround-/Behebungszeiten gelöst wurden (ein Wiederaufkommen eines Incidents zählt für sich)	3 P1 Incidents in einem Quartal, die nicht in den definierten Reaktions-/Workaround-/Behebungszeiten gelöst wurden (ein Wiederaufkommen eines Incidents zählt für sich)

Gutschrift bei schwerwiegendem SLA-Verstoß (P1) = 0,2% der geschuldeten Vergütung im Bezugszeitraum des laufenden Kalenderjahres

Gutschrift bei SLA-Verstoß (P2) = 0,1% der geschuldeten Vergütung im Bezugszeitraum des laufenden Kalenderjahres

11. Service-Reviews

In regelmäßigen Abständen treffen sich Dienstleister und Auftraggeber zu Service-Reviews. In diesen Reviews werden alle aktuellen Aufgaben und Themen des Betriebs besprochen, wie Auffälligkeiten aus dem Monitoring, Performance Schwächen, Risiken mit zugehörigen Maßnahmen, prioritäre Tickets, SLA-Verletzungen und sonstige Erfahrungen aus der Nutzung der Plattform, insbesondere aus Prüfungsdurchführungen und Rollout-Phasen. Die Reviews dienen

der Identifikation von Optimierungspotenzialen und der kontinuierlichen Verbesserung von Betrieb, Prozessen und Leistungen über die Vereinbarung entsprechender Maßnahmen. Zudem wird der Stand an Service Credits gemeinsam ausgewertet.

Alle Governance-Entscheidungen und Maßnahmen zu Roadmap, Architektur, Ressourcen, KPIs oder zum Leistungsumfang des Betriebs werden in einem Governance-Protokoll festgehalten.

12. Geltung, Laufzeit, Exit

Dieses SLA tritt mit Wirksamkeit des Hauptvertrages in Kraft und gilt für dessen gesamte Laufzeit einschließlich vereinbarter Verlängerungszeiträume. Das SLA endet automatisch mit Beendigung des Hauptvertrages, ohne dass es einer gesonderten Kündigung bedarf.

Im Falle von Widersprüchen zwischen diesem SLA und dem Hauptvertrag gehen – soweit rechtlich zulässig – die Regelungen des Hauptvertrages vor.

12.1 Exit Management & Übergaberegelungen

Exit Management umfasst die geordnete Beendigung des Vertragsverhältnisses sowie die vollständige und nachvollziehbare Übergabe aller relevanten Daten und betrieblichen Artefakte vom Dienstleister an den Auftraggeber oder einen vom Auftraggeber benannten Dritten.

Zwischen Kündigung und Vertragsende ist ein kontinuierlicher und unterbrechungsfreier Betrieb sicherzustellen.

Der Dienstleister stellt zu einem möglichen Exit einen vollständigen Export aller relevanten Daten bereit, insbesondere:

- Benutzer- und Rollenstrukturen,
- Protokolle (z. B. Audit-, API- und Betriebslogs) und
- Systemkonfigurationen (Builds, Monitoring, Backup, Automationen).

Die Daten sind in offenen, dokumentierten und maschinenlesbaren Formaten bereitzustellen (z. B. JSON, CSV, XML oder gleichwertige offene Standardformate) und ohne Abhängigkeit von proprietären Systemen nutzbar. Nach Abschluss der Übergabe sind alle Daten gemäß den geltenden datenschutzrechtlichen Vorgaben zu löschen, eine Löschbestätigung ist vorzulegen.

Der Dienstleister unterstützt den Auftraggeber im Exit-Fall aktiv bei der Übergabe, insbesondere durch:

- Bereitstellung des Quellcodes (sofern vertraglich vereinbart),
- Bereitstellung und Erläuterung technischer Dokumentationen,
- Durchführung von Wissenstransfer-Maßnahmen (z. B. Workshops),
- Bereitstellung offener Tickets und Risiken.

Der Exit gilt erst als abgeschlossen, wenn alle vereinbarten Übergabeleistungen vollständig erbracht und dokumentiert sind.

Unterschriften:

Ort, Datum:

Ort, Datum:

Auftraggeber

DIHK

Dienstleister