

## Anlage 1

### SLAs Vergabeverfahren „Gesundheitswelt“

#### Inhalt

<b>1 Ziele der Vereinbarung .....</b>	<b>2</b>
<b>2. Definitionen .....</b>	<b>2</b>
2.1 Verfügbarkeit.....	2
2.2 Nichtverfügbarkeit.....	2
2.3 Störung / Incident .....	3
2.4 Reaktionszeit .....	3
2.5 Behebungszeit.....	3
<b>3 Supportzeiten und Erreichbarkeit.....</b>	<b>3</b>
<b>4 Fehlerkategorien, Reaktionszeiten und Behebungszeiträume .....</b>	<b>4</b>
<b>5. Verfügbarkeit.....</b>	<b>6</b>
<b>6. Service Messung und Service-Level-Reporting.....</b>	<b>6</b>
<b>7. Eskalationsmanagement.....</b>	<b>7</b>
7.1 Allgemeines .....	7
7.2 Eskalationsstufen .....	8
7.3 Automatische Eskalation .....	9
7.4 Kommunikations- und Statuspflichten .....	9
7.5 Major-Incident-Management .....	10
7.6 Root-Cause-Analyse .....	10
7.7 Dokumentationspflicht .....	11
<b>8 Sanktionen bei Nichteinhaltung der SLA.....</b>	<b>11</b>
8.1 Verfügbarkeit.....	11
8.2 Reaktionszeit und Problembehebungszeitraum .....	12
<b>9. Haftungsbegrenzung.....</b>	<b>12</b>
<b>10. Schwachstellenmanagement.....</b>	<b>12</b>
10.1 SLA-Beschreibung .....	12
<b>11. Vorrangige Klauseln.....</b>	<b>14</b>

## 1 Ziele der Vereinbarung

Diese Vereinbarung ergänzt und präzisiert die Regelungen in der Leistungsbeschreibung „Agenturleistungen im Bereich Online (deine-gesundheitswelt.de)“.

Ziel dieser Service-Level-Vereinbarung ist es einen zeitgerechten Support für die Anwendung mit angemessenen Reaktionszeiten sicherzustellen bzw. etwaige Einschränkungen zur Aufrechterhaltung des Systems angemessen zu sanktionieren.

Der laufende Betrieb der Anwendung umfasst insbesondere deren Funktionsfähigkeit sowie alle Bestandteile des mit dem Auftragnehmer vereinbarten Leistungsumfangs. Unter Support sind insbesondere alle Auskünfte sowie alle unterstützenden und durchführenden Handlungen zwischen dem Auftragnehmer einerseits und der Auftraggeberin gemeint.

## 2. Definitionen

### 2.1 Verfügbarkeit

Verfügbarkeit liegt vor, wenn die produktive Plattform einschließlich der definierten Kernfunktionen über HTTPS bestimmungsgemäß nutzbar ist.

**Kernfunktionen sind insbesondere:**

- Benutzerlogin und Authentifizierung
- Nutzerverwaltung
- Formular- und Datenerfassungsfunktionen
- CMS-/Content-Auslieferung
- API-Schnittstellen im produktiven Betrieb Datenbank- und Suchfunktionen
- Zentrale Dienste

### 2.2 Nichtverfügbarkeit

Nichtverfügbarkeit liegt vor, sobald mindestens eine Kernfunktion nicht oder nur eingeschränkt nutzbar ist.

Nicht als Nichtverfügbarkeit gelten ausschließlich:

- geplante Wartungsfenster gemäß Ziffer 4
- höhere Gewalt
- vom Auftraggeber verursachte Störungen
- externe Netz-/Telekommunikationsstörungen außerhalb des Einflussbereichs des Auftragnehmers

## **2.3 Störung / Incident**

Eine Störung ist jede Abweichung vom vereinbarten Sollzustand der Plattform.

## **2.4 Reaktionszeit**

Zeit zwischen Eingang einer Störungsmeldung im Ticketsystem und erster qualifizierter Rückmeldung des Auftragnehmers.

## **2.5 Behebungszeit**

Zeit von Eingang der Störungsmeldung bis zur vollständigen Wiederherstellung der produktiven Funktionsfähigkeit in der Produktionsumgebung.

Eine Störung gilt erst als behoben, wenn die Ursache dauerhaft beseitigt ist und keine Reproduktion des Fehlers innerhalb von 14 Kalendertagen möglich ist. Ein Workaround gilt nicht als endgültige Fehlerbehebung, beendet jedoch den Lauf der Wiederherstellungszeit, sofern die produktive Nutzbarkeit vollständig wiederhergestellt wurde. Die dauerhafte Fehlerbeseitigung erfolgt innerhalb angemessener Frist.

## **3 Supportzeiten und Erreichbarkeit**

Als Supportzeiten gelten soweit nicht nachfolgend (z.B. bei Fehlerkategorie 1) anders geregelt, die Zeiten von 8 – 17 Uhr an Werktagen (Mo – Fr).

Der Auftragnehmer wird während der Supportzeiten

- bei Fragen zum Betrieb zur Verfügung stehen;
- Support-Anfragen innerhalb von 1 Stunde telefonisch oder in einem Ticketsystem der Auftraggeberin auf Deutsch beantworten.

## 4 Fehlerkategorien, Reaktionszeiten und Behebungszeiträume

Der Auftragnehmer wird mit seiner Leistungserbringung einen störungsfreien Betrieb sicherstellen. Nach einer Störungsmeldung sind die Fehler vom Auftragnehmer zu kategorisieren und innerhalb der nachfolgend definierten Zeiten zu beheben. Tritt derselbe Fehler nach der vermeintlichen Fehlerbeseitigung innerhalb des Zeitraums, der als Problembehebungszeitraum gilt, erneut auf, so gilt er als nicht beseitigt. Bei einem Softwarefehler wird der Zeitraum bis zu Lieferung in die Test-Umgebung gerechnet.

### Fehlerkategorie 1

Fehlerkategorie 1 liegt insbesondere vor, wenn:

- Authentifizierung oder Benutzerlogin ausfallen,
- produktive Versichertendienste nicht nutzbar sind,
- sicherheitsrelevante Funktionen beeinträchtigt sind,
- Datenverlust oder Datenkorruption drohen,
- regulatorische Anforderungen gefährdet sind,
- oder wesentliche Geschäftsprozesse nicht mehr durchgeführt werden können.

Reaktionszeit: 1 h bei Eingang der Fehlermeldung beim Auftragnehmer werktags nach 06 Uhr und vor 18 Uhr. (Lauf der Reaktionszeit wird durch Ende der Supportzeiten nicht unterbrochen)

Reaktionszeit: 3 h bei Eingang der Fehlermeldung beim Auftragnehmer werktags nach 18 Uhr und vor 06 Uhr sowie am Wochenende (Sa und So) und bundesweiten Feiertage. (Lauf der Reaktionszeit wird durch Ende der Supportzeiten nicht unterbrochen)

Problembehebungszeitraum: 24 h ab Eingang der Fehlermeldung (egal wann) und der Lauf des Problembehebungszeitraums wird durch Ende der Supportzeiten nicht unterbrochen.

## **Fehlerkategorie 2**

Fehlerkategorie 2 liegt vor, wenn wesentliche Funktionen der Plattform eingeschränkt sind, jedoch ein produktiver Grundbetrieb weiterhin möglich ist.

Reaktionszeit: 8 h während der Supportzeiten

Problembehebungszeitraum: 72 h

## **Fehlerkategorie 3**

Die Einschränkung der Funktionalitäten ist nur geringfügig, d.h. ohne merklichen Einfluss auf ihre Funktionsfähigkeit.

Reaktionszeit: 3 Arbeitstage

Problembehebungszeitraum: 168 h (= 1 Woche) (inkl. der Zeiten außerhalb der Supportzeiten)

## **Fehlerkategorie 4**

Andere Mängel, die nicht die Funktion der deine-gesundheitswelt.de beeinträchtigen, aber unerwünscht sind.

Reaktionszeit: 3 Tage

Problembehebungszeitraum: Der Auftragnehmer informiert den Relevanten Auftraggeber zeitnah über die ergriffenen Maßnahmen

## 5. Verfügbarkeit

Die geschuldete Verfügbarkeit beträgt 99,9 % pro Kalendermonat.

Die Messung erfolgt durch:

- Monitoring des Auftragnehmers und
- optionales unabhängiges Monitoring des Auftraggebers oder Dritter.

Im Streitfall sind Rohdaten beider Messsysteme maßgeblich.

## 6. Service Messung und Service-Level-Reporting

Um die Servicequalität und die Einhaltung der vorstehend genannten Service-Levels überprüfen zu können, wird der Auftragnehmer monatlich (spätestens bis zum 15. des Folgemonats) aussagekräftige und nachprüfbare Reports mit folgenden Kennziffern dem Auftraggeber übermitteln. Der minimale Erfüllungsgrad zur Beurteilung der Servicequalität ist in der folgenden Tabelle festgelegt.

Erbrachte IST-Leistungen	Zu erbringende Soll-Leistungen	Mindestens geschuldeter Erfüllungsgrad
Tatsächliche Verfügbarkeit der Plattform deine-gesundheitswelt.de (und jedes einzelnen darauf betriebenen Zentralen Dienstes, etc.).	Anwendung ist jeweils 24 Stunden pro Kalendertag an allen Tagen im Jahr verfügbar (365 x 24 Betrieb)	99,9% bezogen auf die Sollleistung im Kalendermonat
Tatsächliche Reaktionszeiten (für jede Kategorie einzeln)	Beachtung der Reaktionszeiten (für jede Kategorie einzeln)	100% im Quartal (pro Kategorie)
Tatsächlicher Problembehebungszeitraum (für Fehler der Kategorie 1 und 2)	Beachtung des Problembehebungszeitraums (für Fehler der Kategorie 1 und 2 einzeln)	100% im Quartal (pro Kategorie)

Die Reports müssen mindestens folgende Informationen enthalten:

- Verfügbarkeitswerte,
- sämtliche Störungsmeldungen,
- Kategoriezuordnung,
- Reaktionszeiten,
- Fehlerbehebungszeiten,
- Eskalationen,
- geplante Wartungsfenster,
- Sicherheitsvorfälle.

Der Auftragnehmer liefert die Reports monatlich bis zum 10. Werktag des Folgemonats.

## **7. Eskalationsmanagement**

### **7.1 Allgemeines**

Der Auftragnehmer stellt ein abgestuftes Eskalationsmanagement zur Sicherstellung einer unverzüglichen Bearbeitung kritischer Störungen und Sicherheitsvorfälle bereit.

Das Eskalationsmanagement dient insbesondere:

- der schnellen Wiederherstellung des produktiven Betriebs,
- der Sicherstellung der Kommunikation zwischen den Vertragsparteien,
- der frühzeitigen Einbindung entscheidungsbefugter Stellen,
- sowie der Minimierung betrieblicher und sicherheitsrelevanter Auswirkungen.

Der Auftragnehmer benennt dem Auftraggeber spätestens zum Leistungsbeginn feste Ansprechpartner einschließlich Vertreterregelungen für sämtliche Eskalationsstufen.

Die jeweils aktuellen Kontaktdaten, Rufnummern sowie Erreichbarkeiten sind fortlaufend aktuell zu halten und dem Auftraggeber jederzeit auf Verlangen zur Verfügung zu stellen.

## 7.2 Eskalationsstufen

Das Eskalationsmanagement umfasst mindestens folgende Eskalationsstufen:

### **Level 1 – Operativer Support**

Bearbeitung eingehender Störungen, Supportanfragen und Incidents durch den technischen First-Level- bzw. Betriebs-Support.

Aufgaben insbesondere:

- Ticketannahme,
- Erstanalyse,
- Fehlerklassifizierung,
- Einleitung erster Gegenmaßnahmen,
- Kommunikation mit dem Auftraggeber.

### **Level 2 – Incident Management / Teamleitung**

Einbindung technischer Spezialisten sowie der zuständigen Team- oder Betriebsleitung bei:

- nicht fristgerechter Lösung,
- erheblichen Betriebsbeeinträchtigungen,
- Sicherheitsvorfällen,
- wiederkehrenden Fehlerbildern,
- oder drohender SLA-Verletzung.

Aufgaben insbesondere:

- Koordination der Incident-Bearbeitung,
- Priorisierung technischer Maßnahmen,
- Ressourcensteuerung,
- Abstimmung mit dem Auftraggeber,
- Entscheidung über Workarounds und Sofortmaßnahmen.

### **Level 3 – Management-Eskalation**

Einbindung der technischen Leitung, Geschäftsführung oder anderer entscheidungsbefugter Stellen des Auftragnehmers bei:

- fortdauernden kritischen Störungen,
- erheblichen Sicherheitsvorfällen,
- drohender Gefährdung der Geschäftskontinuität,



- wiederholten SLA-Verletzungen,
- oder erheblichem Reputationsrisiko.

Aufgaben insbesondere:

- Managementkoordination,
- Bereitstellung zusätzlicher Ressourcen,
- Entscheidung über Notfallmaßnahmen,
- Abstimmung strategischer Maßnahmen mit dem Auftraggeber,
- Sicherstellung der externen und internen Kommunikation.

### 7.3 Automatische Eskalation

Die Eskalation erfolgt automatisch entsprechend der nachstehenden Fristen:

Ereignis	Eskalation
Kategorie-1-Störung ohne Wiederherstellung innerhalb von 30 Minuten	Eskalation an Level 2
Kategorie-1-Störung ohne Wiederherstellung innerhalb von 60 Minuten	Eskalation an Level 3
Sicherheitsvorfälle mit hohem oder kritischem Risiko	unverzögliche Eskalation an Level 2 und Level 3
Wiederholtes Auftreten desselben Fehlers innerhalb von 30 Kalendertagen	Eskalation an Level 2

Der Auftraggeber ist jederzeit berechtigt, eine sofortige Eskalation auf eine höhere Eskalationsstufe zu verlangen.

### 7.4 Kommunikations- und Statuspflichten

Bei Fehlerkategorie-1-Störungen sowie Sicherheitsvorfällen informiert der Auftragnehmer den Auftraggeber fortlaufend über:

- aktuellen Bearbeitungsstand,
- Ursache der Störung, soweit bekannt,
- geplante Gegenmaßnahmen,
- erwartete Wiederherstellungszeiten,
- Risiken und Auswirkungen auf den produktiven Betrieb.

Statusupdates erfolgen mindestens:

- alle 30 Minuten bei Fehlerkategorie 1,
- alle 2 Stunden bei Sicherheitsvorfällen hoher Kritikalität,
- sowie auf Anforderung des Auftraggebers.

Die Kommunikation erfolgt über die zwischen den Vertragsparteien abgestimmten Kommunikationskanäle.

## **7.5 Major-Incident-Management**

Liegt eine Fehlerkategorie-1-Störung oder ein schwerwiegender Sicherheitsvorfall vor, richtet der Auftragnehmer unverzüglich ein Major-Incident-Management ein.

Dieses umfasst mindestens:

- Benennung eines Incident Managers,
- zentrale Koordination aller Maßnahmen,
- Einrichtung einer gemeinsamen Lagekonferenz,
- fortlaufende Dokumentation sämtlicher Maßnahmen,
- Koordination eingesetzter Subunternehmer,
- sowie Priorisierung der schnellstmöglichen Wiederherstellung des produktiven Betriebs.

Der Auftragnehmer stellt sicher, dass während des Major-Incident-Managements jederzeit entscheidungsbefugte Ansprechpartner erreichbar sind.

## **7.6 Root-Cause-Analyse**

Bei:

- Fehlerkategorie-1-Störungen,
- Sicherheitsvorfällen,
- oder wiederkehrenden Fehlerbildern
- erstellt der Auftragnehmer spätestens innerhalb von fünf Werktagen nach Wiederherstellung des produktiven Betriebs eine schriftliche Root-Cause-Analyse.

Diese enthält mindestens:

- Beschreibung des Vorfalls,
- Ursache der Störung,
- zeitlichen Ablauf,
- Auswirkungen,
- ergriffene Sofortmaßnahmen,
- dauerhafte Präventionsmaßnahmen,
- sowie Empfehlungen zur Vermeidung vergleichbarer Vorfälle.
- 

Die Root-Cause-Analyse ist dem Auftraggeber unaufgefordert zu übermitteln.

## **7.7 Dokumentationspflicht**

Sämtliche Eskalationen, Kommunikationsmaßnahmen, Entscheidungen und Wiederherstellungsmaßnahmen sind durch den Auftragnehmer nachvollziehbar zu dokumentieren und mindestens 24 Monate aufzubewahren.

Der Auftraggeber ist berechtigt, Einsicht in die Dokumentation zu verlangen.

## **8 Sanktionen bei Nichteinhaltung der SLA**

Sollten die SLAs aufgrund von Fehlern, welche außerhalb des Verantwortungsbereichs des Auftragnehmers (z.B. Rechenzentrumsbetreiber) liegen, nicht eingehalten werden, werden diese Verfügbarkeiten/Zeiten nicht in die Berechnung der Sanktionen aufgenommen.

Vertragsstrafen werden auf etwaige Schadensersatzansprüche angerechnet.

Die Gesamthöhe sämtlicher Vertragsstrafen ist auf 20 % der jährlichen Gesamtvergütung begrenzt.

### **8.1 Verfügbarkeit**

Für jeden Zehntel-Prozentpunkt (0,1%), um den der tatsächliche Erfüllungsgrad für die in Punkt 2 genannte Verfügbarkeit im Quartal unter dem mindestens geschuldeten Erfüllungsgrad liegt, zahlt der Auftragnehmer an die Auftraggeber als Gläubiger eine Vertragsstrafe in Höhe von EUR 1.000, - (in Worten: eintausend Euro) bis zu einem Maximalwert von 8 % des Gesamtpreises je Quartal.

## 8.2 Reaktionszeit und Problembehebungszeitraum

Für jeden Fall, in dem die in Punkt 2 und 3 definierte Reaktionszeit oder der Problembehebungszeitraum überschritten wird, zahlt der Auftragnehmer an die Auftraggeberin als Gläubiger eine Vertragsstrafe in Höhe von EUR 2.000,- (in Worten: zweitausend Euro) bis zu einem Maximalwert von 10.000 Euro im Quartal. Sollte die Reaktionszeit oder der Problembehebungszeitraum um mehr als 50% überschritten werden (z.B. erfolgt also z.B. bei Reaktionszeit von 3 Stunden eine Reaktion erst nach mehr als 4,5 Stunden), so verdoppelt sich die jeweilige Vertragsstrafe.

## 9. Haftungsbegrenzung

Der Auftragnehmer haftet unbeschränkt nur:

- bei Vorsatz,
- grober Fahrlässigkeit,
- Verletzung von Leben, Körper oder Gesundheit,
- nach dem Produkthaftungsgesetz.

Bei einfacher Fahrlässigkeit haftet der Auftragnehmer bei Verletzung wesentlicher Vertragspflichten und beschränkt auf den vertragstypischen vorhersehbaren Schaden. Dies gilt nicht bei

- Datenschutzverstöße
- IT-Sicherheitsverletzungen
- SLA Verstößen

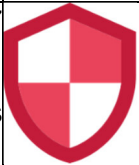
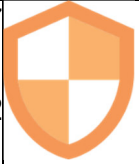
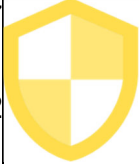

## 10. Schwachstellenmanagement

### 10.1 SLA-Beschreibung

Zusätzlich wird im Rahmen eines kontinuierlichen IT-Sicherheitsprozesses zur Identifizierung, Bewertung, Behebung und Meldung von Sicherheitslücken in der IT-Infrastruktur ein Schwachstellenmanagement durchgeführt. Durch regelmäßige Scans und Patch-Management werden Risiken minimiert, Cyberangriffe verhindert und die Angriffsfläche verkleinert. Es ist essenziell für die IT-Resilienz. Hierzu werden folgende SLAs vereinbart:

Der Auftragnehmer ist berechtigt, gemeldete Schwachstellen technisch zu validieren. Die Validierung hat unverzüglich, spätestens jedoch innerhalb von zwei Stunden nach Eingang der Meldung zu erfolgen. Das Ergebnis der Validierung und die

vorgenommene Einstufung sind zu dokumentieren und dem Auftraggeber auf Verlangen vorzulegen.

Priorität	Beschreibung	SLA	CVE / CVSS
P1 – Hoch	Hoch Massive Störung, Beeinträchtigung des normalen Betriebs, Geschäftskontinuität bedroht	Servicezeit: 24/7 Reaktionszeit: 30 Minuten Fehlerbehebungszeit: sechs Stunden KPI: 99.2%	 Der Temporal Score (CVSS) liegt zwischen 9.0 und 10.0.
P2 – Mittel	Störung des normalen Betriebs, potenziell weitreichende Auswirkungen	Servicezeit: 24/7 Reaktionszeit: eine Stunde Fehlerbehebungszeit: 12 Stunden KPI: 99.2%	 Der Temporal Score (CVSS) liegt zwischen 7.0 und 8.9.
P3 – Niedrig	Geringe Bedrohungslage / Einfache und unmittelbare Behebung mit begrenzten Konsequenzen	Servicezeit: 24/7 Reaktionszeit: zwei Stunden Fehlerbehebungszeit: 12 Stunden KPI: 99.2%	 Der Temporal Score (CVSS) liegt zwischen 4.0 und 6.9.
P4 – Geringfügig/Neutral	Keine aktive Bedrohung, einfache/unmittelbare Behebung mit geringen Auswirkungen	Servicezeit: 24/7 Reaktionszeit: vier Stunden Fehlerbehebungszeit: 24 Stunden KPI: 99.2%	 Der Temporal Score (CVSS) liegt zwischen 0.1 und 3.9.

Zur Risikobewertung wird nicht der CVSS Base Score, sondern der Temporal Score herangezogen, da diese zusätzlichen Kriterien wie Ausnutzbarkeit (Exploitation) und den Stand der Behebung (Remediation Status) berücksichtigt.

► **Servicezeit 24/7:** KPI 99.2 % Verfügbarkeit - Messperiode jährlich

- **Lösungszeit:** KPI 99.2 % der Incidents sind in der vorgegebenen SLA-Zeit gelöst oder an die AOK beziehungsweise an Incident Response weitergeleitet wurden
- **Reaktionszeit:** Zeitdauer, die benötigt wird, um nach dem Eintreffen eines Alarms der Auftraggeberin eine erste Reaktion vorzuschlagen und sofern möglich selbstständig auszuführen bzw. qualifiziert zur Ausführung an einen verantwortlichen Dritten (IR-Team), Service Level bzw. die AOK zu übergeben
- **Fehlerbehebungszeit:** Gesamte Zeitdauer, die benötigt wird, um nach dem Eintreffen eines Alarms den Vorfall innerhalb des Dienstleisters vollständig abzuschließen, sofern alle auszuführenden Tätigkeiten im Einflussbereich des Dienstleisters liegen. Die Zeit wird angehalten, wenn auf Zulieferung der AOK gewartet wird.

## 11. Vorrangige Klauseln

Im Falle von Widersprüchen zwischen dieser SLA-Vereinbarung und dem Hauptvertrag gehen die Regelungen dieser SLA-Vereinbarung hinsichtlich der Service- und Supportleistungen vor.