

# VERGABEUNTERLAGEN

2026THA000002

App-Katalog zum App-Security-Check; LSI

Offenes Verfahren (EU) (VgV)

Ausschreibung (Korrektur)

## AUFTRAGGEBER

Freistaat Bayern vertreten durch das Bayerische Landesamt für Steuern - Zentrale  
Vergabestelle -

Sophienstr. 6, 80333 München, Deutschland

---

08.06.2026

# Inhaltsverzeichnis

Vergabeunterlagen .....	1
Projektinformation .....	1
Vertragsbedingungen/Formulare .....	4
Bewerbungsbedingungen EU .....	4
Bewerbungsbedingungen .....	4
1. Angebotsabgabe .....	4
1.1. Fristen .....	4
1.2. Form und Übermittlung .....	4
1.2.1. Textform .....	5
1.3. Weitere Vorgaben .....	5
1.3.1. Angebot .....	5
1.3.2. Nachweise .....	6
2. Hinweise zu den Vergabeunterlagen .....	7
3. Besondere Beteiligungsformen: .....	8
3.1. Unterauftragnehmer .....	8
3.2. Bietergemeinschaften .....	9
3.3. Wettbewerbsbeschränkende Verhaltensweisen .....	9
4. Abschluss des Vergabeverfahrens .....	10
5. Nachprüfungsverfahren .....	10
6. Kommunikation im Vergabeverfahren .....	11
Ergänzende Bewerbungsbedingungen .....	12
1. Form und Frist des Angebotes .....	12
2. Eignungsbewertung .....	12
3. Ermittlung des wirtschaftlichsten Angebotes .....	12
3.1. Allgemeines .....	12
3.2. Wertung der Angebote .....	13
3.3. Ermittlung des für den Zuschlag vorgesehenen Angebots .....	14
4. vorläufige Zeitplanung .....	15
Angebotsaufforderung .....	16
Struktur Bieter .....	17
1. Angaben zur Struktur .....	17
2. Angaben zu Unterauftragnehmern .....	17
3. Angaben zur Eignungsleihe .....	18
4. Angaben zur Bietergemeinschaft .....	18
4.1. Mitglieder der Bietergemeinschaft .....	18
4.2. Bevollmächtigter Vertreter .....	18
Eigenerklärung .....	19
Eigenerklärung .....	19
Eigenerklärung RUS .....	21

Eigenerklärung russische Unternehmen .....	21
Artikel 5k der Verordnung (EU) Nr. 833/2014 in der Fassung des Art. 1 Ziff. 23 der Verordnung (EU) 2 .....	23
Eigenerklärung für Unterauftragnehmer und Eignungsverleiher .....	24
Eigenerklärung .....	24
Schutzerklärung Scientology .....	27
1. Erklärung zum Vergabeverfahren .....	27
2. Erklärung für den Fall der Zuschlagserteilung.....	27
3. Hinweis nach Art. 9 Abs. 2 des Bayerischen Datenschutzgesetzes: .....	27
EVB-IT digital Dienstvertrag .....	29
Anlage 01_Rahmenkonzept App-Security-Check v0.4 .....	41
Anlage 02_Leistungsbeschreibung App-Katalog 1. Korrekturzyklus.....	45
1 Hintergrund.....	47
2 Leistungsgegenstand .....	47
2.1 Überblick .....	47
2.2 Katalogumfang .....	47
2.3 Prüfzyklus.....	48
2.4 Webanwendung .....	48
2.5 Webservice (API) .....	49
2.6 Funktionen.....	49
2.7 Prüfverfahren.....	50
2.8 Prüfkriterien .....	50
2.8.1 Plattformsicherheit.....	50
2.8.2 Datensicherheit .....	51
2.8.3 Netzwerkkommunikation .....	51
2.8.4 Kommunikationsbeziehungen .....	51
2.8.5 Code .....	52
2.9 Prüfergebnisse .....	52
3 Rahmenbedingungen .....	53
3.1 Nutzungsvolumen.....	53
3.2 Anforderungen an den Auftragnehmer.....	53
3.3 Leistungszeitraum .....	54
3.4 Allgemeine technische Anforderungen.....	54
3.5 Anforderungen an Systemkomponenten.....	54
3.6 Projektkommunikation .....	55
3.7 Abrechnung .....	55
4 Glossar .....	55
Anlage 03_Datenschutz- und Vertraulichkeitsvereinbarung .....	57
Anlage 04_Vereinbarung zur Auftragsverarbeitung .....	59
Anlage 05_Datenschutzinformationen .....	66
Anlage 06e_PtA-Vorlage.....	69
Produkte/Leistungen .....	71
Eignungskriterien.....	74

Leistungskriterien .....	79
Anlagen .....	80



# INFORMATIONEN ZUR AUSSCHREIBUNG

Auftragsnummer	2026THA000002
Maßnahme	
Auftragsbezeichnung	App-Katalog zum App-Security-Check; LSI
Auftragsbeschreibung	Das Landesamt für Sicherheit in der Informationstechnik (LSI) unterstützt Behörden in Bayern mit dem Dienstleistungsangebot App-Security-Check. Dabei stellt das LSI sicherheitstechnische Bewertungen gängiger Smartphone-Apps zur Verfügung. Das LSI beabsichtigt, ein Unternehmen zu beauftragen, das Apps in großer Zahl automatisiert prüfen und die Ergebnisse zur Verfügung stellen wird. Der Leistungszeitraum umfasst zunächst 24 Monate (Grundvertragslaufzeit). Er verlängert sich bis zu dreimal um jeweils 12 Monate, falls der Auftraggeber nicht mindestens 3 Monate vor dem jeweiligen Verlängerungszeitpunkt ordentlich in Textform kündigt (2+1+1+1).

## ALLGEMEINES

### VERFAHREN

Auftraggeber	Freistaat Bayern vertreten durch das Bayerische Landesamt für Steuern - Zentrale Vergabestelle -
Liefer-/Ausführungsort	90489 Nürnberg
Leistungsart	Dienstleistung
Vertragsart	Dienstvertrag
Vergabeart	Offenes Verfahren (EU) (VgV)

### VERFAHRENSEIGENSCHAFTEN

Losweise Vergabe	Nein						
Art der losweisen Vergabe							
Höchstzahl der Lose pro Angebot							
Zuschlagskriterium	Wirtschaftlichstes Angebot Berechnungsmethode: UfAB 2018: Erweiterte Richtwertmethode Schwankung: 10% Entscheidungskriterium: Leistung						
Klassifizierungen	<table><thead><tr><th>Code</th><th>Bezeichnung</th></tr></thead><tbody><tr><td>72000000-5</td><td>IT-Dienste: Beratung, Software-Entwicklung, Internet und Hilfestellung</td></tr><tr><td>72200000-7</td><td>Softwareprogrammierung und -beratung</td></tr></tbody></table>	Code	Bezeichnung	72000000-5	IT-Dienste: Beratung, Software-Entwicklung, Internet und Hilfestellung	72200000-7	Softwareprogrammierung und -beratung
Code	Bezeichnung						
72000000-5	IT-Dienste: Beratung, Software-Entwicklung, Internet und Hilfestellung						
72200000-7	Softwareprogrammierung und -beratung						

### ANGEBOTE

Mehrere Hauptangebote zugelassen	Mehrere Hauptangebote sind nicht zulässig
Nebenangebote	Nebenangebote sind nicht zugelassen
Nachlass	Nein
Skonto zugelassen	Nein
Skonto Zahlungsziel	Tag(e)
Verwendung elektronischer Mittel	Die Einreichung der Angebote/Teilnahmeanträge darf nur elektronisch erfolgen
URL für elektronische Angebote	<a href="https://www.auftraege.bayern.de">https://www.auftraege.bayern.de</a>
Zulässige Signatur	Textform nach §126b BGB

## TERMINE

### ALLGEMEIN

Vorausgegangene Vorinformation	Nein
Besondere Dringlichkeit	Nein

### BEKANNTMACHUNG

Bekanntmachung	19.05.2026
Vorinformation	

### ANGEBOTE UND BEWERTUNG

Frist Bieterfragen	22.06.2026 11:00
Angebotsfrist	03.07.2026 11:00:00
Bindefrist	30.09.2026
Versand Vorabinformation	

### AUFTRAGSDAUER

Beginn	
--------	--

Ende

Anmerkungen

# DATENSCHUTZ

## DATENSCHUTZBEAUFTRAGTER

Name	Behördliche/r Datenschutzbeauftragte/r des BayLfSt
Anschrift	Krelingstraße 50, 90408 Nürnberg
Telefon	+49 9119911004
E-Mail	datenschutz@lfst.bayern.de

## DATENERHEBUNGSVERANTWORTLICHER

Name	Bayerisches Landesamt für Steuern
Anschrift	Sophienstraße 6, 80333 München
Telefon	+49 8999910
E-Mail	info-eVergabe@lfst.bayern.de

## ELEKTRONISCHE TEILNAHME

### BROWSEEREINSTELLUNGEN

Verwenden Sie zur Navigation in eVergabe nur die Menüpunkte der Anwendung. Wenn Sie über die Browser-Schaltflächen navigieren, werden die Informationen nicht zum Anwendungs-Server übertragen und eVergabe zeigt ggf. eine falsche Seite an.

Sicherheitseinstellungen an Ihrem Browser:

- JavaScript muss aktiviert sein
- Cookies müssen erlaubt sein; Cookies von Drittanbietern sollten erlaubt sein (empfohlen)
- Pop-Up-Fenster müssen erlaubt sein

PDF-Plugins:

- Die integrierte PDF-Ansicht sollte deaktiviert sein; ein PDF-Reader wird empfohlen

Empfohlene Browser:

- Aktuelle Versionen des Microsoft Edge, Google Chrome, Opera oder Mozilla Firefox

## KOMMUNIKATION

Die Kommunikation mit der Vergabestelle, insbesondere zu Nachforderungen, sowie das Stellen von Bieterfragen erfolgt grundsätzlich im jeweiligen Verfahren über den Bieterassistenten unter "Nachrichten".

Bei Nachrichten der Vergabestelle erhalten Sie unmittelbar eine Benachrichtigung per E-Mail. Bitte prüfen Sie in diesem Fall Ihren Posteingang unter "Nachrichten" und bestätigen dort die Kenntnisnahme.

Projekt-Nr.: 2026THA000002

Aktenzeichen: H 1620.2.1-2014

Projektname: App-Katalog zum App-Security-Check; LSI

## **Bewerbungsbedingungen**

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

### **1. Angebotsabgabe**

#### **1.1. Fristen**

Die **Angebotsfrist** endet am 03.07.2026 um 11:00:00 Uhr.

Eine Änderung oder Rücknahme eines bereits eingereichten Angebots durch den Bieter ist nur bis zum Ablauf dieser Angebotsfrist zulässig.

Der öffentliche Auftraggeber wird den Zuschlag spätestens am 30.09.2026 erteilen.

Der Bieter ist bis dahin an sein eingereichtes Angebot gebunden (**Bindefrist**).

Die **Frist für Bieterfragen** endet am 22.06.2026 11:00 Uhr.

Fragen, die dem öffentlichen Auftraggeber nach Ablauf dieses Termins zugehen, werden grundsätzlich nicht beantwortet.

#### **1.2. Form und Übermittlung**

Die Abgabe des Angebots hat unter Verwendung elektronischer Mittel zu erfolgen.

Nicht mittels elektronischer Datenübermittlung abgegebene Angebote werden nicht berücksichtigt.

Die wirksame Angebotsabgabe hat vollumfänglich und ausschließlich über die Vergabepattform zu erfolgen.

Die zur Erstellung eines elektronischen Angebots erforderlichen Arbeitsschritte können Sie dem Bieter-Handbuch entnehmen.

Die online-Bearbeitung der Angebotserstellung kann jederzeit unterbrochen werden. Zur Fortsetzung einer unterbrochenen Angebotserstellung bedarf es der nochmaligen Einwahl über die Vergabeplattform in den Angebotsassistenten (durch Auswahl des entsprechenden Verfahrens im Menüpunkt „meine Projekte“, Unterpunkt „Angebotsphase“).

Zur rechtsgültigen Angebotsabgabe bedarf es neben der Verwendung elektronischer Mittel der Einhaltung der **verfahrensspezifisch vorgegebenen Formerfordernisse**. Diese werden Ihnen im Schritt „Angebot einreichen“ zur Auswahl angeboten:

#### **1.2.1. Textform**

Dem Erfordernis der Textform nach § 126b BGB genügt die Angabe des Angebotserstellers im dafür vorgesehenen Feld und anschließende Bestätigung über den Button „Angebot einreichen“.

### **1.3. Weitere Vorgaben**

Die Angebote werden hinsichtlich

- Form und Vollständigkeit,
- Eignung der Bieter und des Nichtvorliegens von Ausschlussgründen,
- Angemessenheit und Wirtschaftlichkeit

geprüft und bewertet.

Soweit sich aus den übrigen Vergabeunterlagen nicht etwas anderes ergibt, wird für die Angebotsabgabe auf Folgendes hingewiesen:

#### **1.3.1. Angebot**

Das Angebot und dessen Anlagen sind in deutscher Sprache abzufassen.

Die im Angebot enthaltenen Preisangaben sind in Euro anzugeben.

Entspricht der Gesamtbetrag nicht dem Ergebnis der Multiplikation von Mengenansatz und Einheitspreis, ist der Einheitspreis maßgebend.

Die Abgabe von Doppelangeboten ist unzulässig.

Doppelangebote sind Angebote, die sich allein preislich von einem ansonsten inhaltlich identischen Angebot desselben Bieters unterscheiden.

Für die Erstellung des Angebots und aller übermittelten Unterlagen wird keine Vergütung gewährt.

Dem Angebot beigelegte Unterlagen, Muster usw. gehen mit Übermittlung in das Eigentum des Auftraggebers über.

Betriebs- und Geschäftsgeheimnisse sind kenntlich zu machen.

Im Angebot ist anzugeben, ob gewerbliche Schutzrechte bestehen oder vom Bieter oder anderen beantragt sind.

Bieter haben auf erkannte Widersprüche und Fehler in den Vergabeunterlagen hinzuweisen.

Die Rügeobliegenheit nach § 160 Abs. 3 GWB bleibt unberührt.

Antworten des Auftraggebers auf Bieterfragen werden Bestandteil der Vergabeunterlagen. Maßgeblich ist jeweils die jüngste Antwort des Auftraggebers.

Falls während der Angebotsphase die Vergabeunterlagen durch den Auftraggeber geändert werden sollten (sog. Korrekturzyklus), verlieren alle bis dahin abgegebenen Angebote automatisch ihre Gültigkeit.

Für den Fall, dass ein bereits abgegebenes Angebot aufrechterhalten werden soll, muss es über den Angebotsassistenten erneut abgegeben werden. Hierzu kann eine automatisch angelegte Kopie des bisherigen Angebots als gültiges Angebot bestätigt werden.

Es werden nur Angebote fachkundiger und leistungsfähiger (geeigneter) Bieter berücksichtigt, welche die festgelegten Kriterien zur ordnungsgemäßen Auftragsausführung erfüllen.

Die Eignung der Bieter wird anhand der geforderten Erklärungen und Nachweise beurteilt.

Im Falle der Bildung einer Bietergemeinschaft, der Unterbeauftragung oder sonstigen Berufung auf die Leistungsfähigkeit eines Dritten (sog. Eignungsleihe) können sich die Angaben und Erklärungen der einzelnen Unternehmen ergänzen, um die erforderliche Leistungsfähigkeit des Bieters insgesamt nachzuweisen.

Bei Vorliegen einer Bietergemeinschaft oder einer Eignungsleihe ist der Auftraggeber zur Einholung eines Auszugs aus dem Wettbewerbsregister hinsichtlich aller Beteiligten verpflichtet.

### **1.3.2. Nachweise**

Bei Beauftragung eines Dritten ist nachzuweisen, dass die für den Auftrag erforderliche Fachkunde und Leistungsfähigkeit bei der Ausführung des Auftrags tatsächlich zur Verfügung gestellt werden kann. Dieser Nachweis kann z.B. durch eine entsprechende unterschriebene Verpflichtungserklärung des Dritten erfolgen.

Nachweise, die bei Angebotsabgabe zu erbringen sind, müssen im Arbeitsschritt „Eigene Anlagen“ hochgeladen und elektronisch beigelegt werden. Dateien unterliegen hinsichtlich Größe und Benennung technischen Beschränkungen, auf die gesondert hingewiesen wird.

Unterlagen die nicht der vorgegebenen Form entsprechen gelten als nicht abgegeben und werden nicht berücksichtigt.

Sofern Nachweise oder Erklärungen gefordert sind, die ein Bieter eines europäischen Mitgliedstaates objektiv nicht beibringen kann, werden vergleichbare Nachweise oder Erklärungen nach dem Recht des Sitzes des Bieters anerkannt. Hierfür sind Übersetzungen vorzulegen, die durch einen amtlich vereidigten Übersetzer gefertigt wurden.

Bitte beachten Sie, dass Verweise auf Datenträger, Literatur, Broschüren usw. die geforderten Antworten und Erklärungen nicht ersetzen. Sie werden nicht bewertet.

## **2. Hinweise zu den Vergabeunterlagen**

Soweit sich aus den übrigen Vergabeunterlagen nicht etwas anderes ergibt, wird auf Folgendes hingewiesen:

Die Allgemeinen Vertragsbedingungen für die Ausführung von Leistungen (VOL/B) in der derzeit gültigen Fassung gelten nachrangig zu den Regelungen in den Vergabeunterlagen.

Änderungen und Ergänzungen an den Vergabeunterlagen sind unzulässig.

Abweichende Bestimmungen oder Regelungen im Zusammenhang mit dem Abschluss dieses Vertrages werden nicht Vertragsbestandteil.

Bitte bedenken Sie, dass dies insbesondere von Ihnen beigelegte Allgemeine Geschäftsbedingungen, Begleitschreiben oder Konzepte betrifft.

Die Vergabeunterlagen dürfen ausschließlich zur Angebotserstellung verwendet werden. Jede über diese Verwendung hinausgehende Nutzung, insbesondere Weitergabe oder Veröffentlichung (auch auszugsweise) ohne vorherige schriftliche Zustimmung des Auftraggebers, ist unzulässig. Bei Verzicht auf eine Angebotsabgabe oder für den Fall, dass das Angebot den Zuschlag nicht erhält, sind alle Vergabeunterlagen zu vernichten.

Der Bieter hat auch nach Beendigung des Verfahrens über die ihm bekannt gewordenen vertraulichen Informationen des Auftraggebers Verschwiegenheit zu wahren.

### **3. Besondere Beteiligungsformen:**

Soweit sich aus den übrigen Vergabeunterlagen nicht etwas anderes ergibt, wird auf Folgendes hingewiesen:

#### **3.1. Unterauftragnehmer**

Die Einschaltung von Unterauftragnehmern ist grundsätzlich zulässig.

**Unterauftragnehmer** ist derjenige, der von einem Bieter beauftragt wird, eine oder mehrere Aufgaben von diesem zu übernehmen.

Der Bieter / die Bietergemeinschaft führt die Leistung nicht selbstständig aus, sondern bedient sich ganz (sog. Generalübernehmer) oder teilweise (sog. Generalunternehmer) dem Einsatz von Unterauftragnehmern.

Grundsätzlich haftet der Generalübernehmer/-unternehmer für die ordnungsgemäße Vertragsabwicklung. Der Unterauftragnehmer steht in der Regel in keiner Vertragsbeziehung zum öffentlichen Auftraggeber.

Die Namen der Unterauftragnehmer und die jeweils zu erbringenden Leistungen sind im Angebot zu benennen.

Der Auftragnehmer bemüht sich bei der Einholung von Angeboten der Unterauftragnehmer regelmäßig Kleinst-, kleine und mittlere Unternehmen sowie Existenzgründungen angemessen zu beteiligen.

Er verpflichtet sich bei Weitergabe von Lieferleistungen die VOL/B zum Vertragsbestandteil zu machen.

Der Auftragnehmer verpflichtet sich außerdem den Unterauftragnehmern – insbesondere hinsichtlich Gewährleistung, Vertragsstrafe, Zahlungsweise und Sicherheitsleistungen – keine ungünstigeren Bedingungen aufzuerlegen, als zwischen ihm und dem Auftraggeber vereinbart sind.

Zur Bekämpfung der Verhinderung, Einschränkung oder Verfälschung des Wettbewerbs hat der Bieter auf Verlangen des Auftraggebers Auskunft darüber zu geben, ob und auf welche Art er wirtschaftlich und rechtlich mit Unternehmen verbunden ist.



### 3.2. Bietergemeinschaften

Die Bildung einer Bietergemeinschaft ist grundsätzlich zulässig.

Eine **Bietergemeinschaft** liegt vor, wenn sich mindestens zwei Einzelbieter zusammenschließen und im Rahmen einer Ausschreibung ein gemeinsames Angebot mit dem Ziel abgeben den Zuschlag zu erhalten.

Die Beteiligung in dieser Form ist möglich, soweit die Bildung der Bietergemeinschaft kartell- und wettbewerbsrechtlich zulässig ist. Das Vorliegen der kartell- und wettbewerbsrechtlichen Voraussetzungen ist dem Auftraggeber auf Verlangen nachzuweisen.

Eine Bietergemeinschaft hat mit ihrem Angebot eine, von allen Mitgliedern unterschriebene, Erklärung abzugeben, in welcher

- die Bildung einer Arbeitsgemeinschaft für den Fall der Zuschlagserteilung erklärt ist,
- alle Mitglieder mit postalischer Anschrift aufgeführt sind,
- ein Mitglied für den Abschluss und die Durchführung des Vertrages als bevollmächtigter Vertreter bezeichnet ist,
- alle Mitglieder die Haftung für die Erfüllung sämtlicher vertraglichen Verpflichtungen als Gesamtschuldner übernehmen,
- eine Kontonummer bei einem näher bezeichneten Kreditinstitut angegeben ist, auf die sämtliche Zahlungen des Auftraggebers mit befreiender Wirkung geleistet werden können.

### 3.3. Wettbewerbsbeschränkende Verhaltensweisen

Wettbewerbsbeschränkende Absprachen gem. § 1 des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) sind unzulässig und führen zwingend zum Ausschluss der Beteiligten.

Wenn der Auftragnehmer aus Anlass der Vergabe nachweislich eine Abrede getroffen hat, die eine unzulässige Wettbewerbsbeschränkung darstellt, hat er 5 % der Auftragssumme an den Auftraggeber zu zahlen, es sei denn, dass ein Schaden in anderer Höhe nachgewiesen wird. Dies gilt auch, wenn der Vertrag gekündigt wird oder bereits erfüllt ist.

#### **4. Abschluss des Vergabeverfahrens**

Der Auftraggeber weist auf seine gesetzliche Verpflichtung aus § 6 Abs. 1 des Wettbewerbsregistergesetzes hin. Demnach fordert der Auftraggeber bei Aufträgen ab einer Höhe von 30 000 Euro für den Bieter, der den Zuschlag erhalten soll, vor der Zuschlagserteilung eine Auskunft aus dem Wettbewerbsregister an.

#### **5. Nachprüfungsverfahren**

Das Vergabeverfahren unterliegt der Nachprüfung durch die Vergabekammern.

Ein Antrag auf Nachprüfung nach §§ 160 ff. GWB ist schriftlich zu stellen und an die  
Regierung von Oberbayern - Vergabekammer Südbayern  
Maximilianstr. 39, 80539 München

zu richten.

Die gesetzliche Frist für die Einlegung eines Nachprüfungsantrags richten sich nach § 160 Abs. 3 GWB, wonach der Antrag unzulässig ist, soweit

1. der Antragsteller den geltend gemachten Verstoß gegen Vergabevorschriften vor Einreichen des Nachprüfungsantrags erkannt und gegenüber dem Auftraggeber nicht innerhalb einer Frist von zehn Kalendertagen gerügt hat; der Ablauf der Frist nach § 134 Absatz 2 bleibt unberührt,
2. Verstöße gegen Vergabevorschriften, die aufgrund der Bekanntmachung erkennbar sind, nicht spätestens bis zum Ablauf der in der Bekanntmachung benannten Frist zur Bewerbung oder zur Angebotsabgabe gegenüber dem Auftraggeber gerügt werden,
3. Verstöße gegen Vergabevorschriften, die erst in den Vergabeunterlagen erkennbar sind, nicht spätestens bis zum Ablauf der Frist zur Bewerbung oder zur Angebotsabgabe gegenüber dem Auftraggeber gerügt werden,
4. mehr als 15 Kalendertage nach Eingang der Mitteilung des Auftraggebers, einer Rüge nicht abhelfen zu wollen, vergangen sind.

Für Amtshandlungen der Vergabekammern werden Kosten (Gebühren und Auslagen) zur Deckung des Verwaltungsaufwandes erhoben (§ 182 GWB).

Für das Vergabeverfahren gilt deutsches Recht.

## **6. Kommunikation im Vergabeverfahren**

Die Vergabestelle übermittelt Nachrichten aus dem Verfahren grundsätzlich nur über den Angebotsassistenten und versendet parallel – rein informatorisch – jeweils eine E-Mail-Nachricht (Info-E-Mail) an die in Ihrem Profil hinterlegte E-Mail-Adresse.

Erklärungen gelten mit Bereitstellung im Nachrichtenmodul des Angebotsassistenten als zugegangen.

Ein Anspruch auf den Erhalt von Info-E-Mails in Bezug auf neue Nachrichten der Vergabestelle besteht nicht.

Direkte Rückantworten auf diese Info-E-Mail-Nachrichten oder Anfragen über die dort verwendete System-E-Mail-Adresse sind nicht möglich. Verwenden Sie für die Kommunikation mit der Vergabestelle die Nachrichtenfunktion im Angebotsassistenten.

**Bitte sorgen Sie dafür, dass Sie während des Vergabeverfahrens unter den in Ihrem Firmen- bzw. Mitarbeiterprofil hinterlegten Kontaktdaten (insbesondere E-Mail-Adressen) auch tatsächlich erreichbar sind.**

**Über automatisch generierte Antworten (z.B. Abwesenheitsassistenten) mitgeteilte abweichende Kontaktdaten können nicht berücksichtigt werden.**

## Ergänzende Bewerbungsbedingungen

Die Vergabe über die Durchführung von Sicherheitsbewertungen für Smartphone-Applikationen unter Verwendung weitgehend automatisierter Prüfverfahren und Bereitstellung der Prüfergebnisse in einem Katalog (App-Katalog zum App-Security-Check) erfolgt in einem Offenen Verfahren.

### **1. Form und Frist des Angebotes**

Für die Einreichung des Angebotes ist ausschließlich das vom Auftraggeber vorgegebene eVergabe-System zu verwenden. Angebote, die auf anderem Weg (z.B. schriftlich per Post) eingereicht werden, werden ausgeschlossen.

Die Angebote sind bis zum Ablauf der Einreichungsfrist einzureichen. Angebote, die aus Gründen, die der Bieter zu vertreten hat, verspätet oder nicht formgerecht eingehen, werden nicht berücksichtigt. Angebote, deren verspäteter oder nicht formgerechter Eingang durch Umstände verursacht ist, die nicht vom Bieter zu vertreten sind, können berücksichtigt werden. Will sich ein Bieter darauf berufen, dass er den verspäteten oder nicht formgerechten Eingang seines Angebotes nicht zu vertreten hat, muss er diese Umstände, auf welche er diese Auffassung stützt, der Vergabestelle unverzüglich darlegen und glaubhaft machen.

### **2. Eignungsbewertung**

Die Eignungsbewertung erfolgt nach den in der „Bewertungsmatrix Eignung“ aufgeführten Kriterien. Eine Nichterfüllung der hierin enthaltenen Ausschlusskriterien (A-Kriterien) führt zum Ausschluss vom Vergabeverfahren.

### **3. Ermittlung des wirtschaftlichsten Angebotes**

#### **3.1. Allgemeines**

Bezugspunkt für die Ermittlung des wirtschaftlichsten Angebotes sind die im Rahmen des Vergabeverfahrens fristgerecht eingegangenen Angebote der Bieter, die als für die Auftragsdurchführung geeignet eingestuft wurden (vgl. Ziffer 2).

### **3.2. Wertung der Angebote**

Die Wertung der Angebote erfolgt anhand der Angaben des jeweiligen Bieters zu den Bewertungskriterien innerhalb der „Bewertungsmatrix Leistung und ggfs. anhand eindeutig referenzierter Anlagen.

Die Struktur der einzelnen Kriterien (Leistungsanforderungen) sowie deren Gewichtung untereinander und die ggfs. vorhandenen, jeweiligen Zielerfüllungsgrade sind in der „Bewertungsmatrix Leistung“ angegeben.

Die innerhalb der „Bewertungsmatrix Leistung“ mit „[A]“ gekennzeichneten Ausschlusskriterien müssen – sofern nicht explizit anderweitig angegeben – bereits zum Zeitpunkt der Abgabe des Angebots und zu jedem weiteren Zeitpunkt im Vergabeverfahren erfüllt sein. Als Ausschlusskriterien gelten auch alle festen Vorgaben (kein Bezug auf den Fragekatalog) in der Leistungsbeschreibung. Diese können nur im Wege von Bieterfragen vor Abgabe des Angebotes aufgrund berechtigter Einwände der Bieter geändert werden.

Die Bewertungskriterien sind innerhalb der „Bewertungsmatrix Leistung“ jeweils durch ein „[B]“ gekennzeichnet.

Verweise innerhalb von geforderten Antworten und Erklärungen, z.B. auf Broschüren, Literatur, Firmenberichte, Internetseiten etc., können diese nicht ersetzen und werden für sich allein genommen nicht bewertet. Verweise können geforderte Antworten oder Erklärungen jedoch ergänzen.

### 3.3. Ermittlung des für den Zuschlag vorgesehenen Angebots

Der Zuschlag wird auf der Grundlage der Angaben in den Vergabeunterlagen dem wirtschaftlichsten Angebot erteilt. Dieses wird nach der so genannten **erweiterten Richtwertmethode** gemäß der Unterlage für die Ausschreibung und Bewertung von IT-Leistungen, UfAB 2018 des Beauftragten der Bundesregierung für Informationstechnik ([www.cio.bund.de](http://www.cio.bund.de)) gebildet.

Dabei ergibt sich das wirtschaftlichste Angebot im ersten Schritt aus dem besten Leistungs-Preis-Verhältnis (Z), also einem möglichst großen Quotienten aus Leistung (L) und Angebotssumme (P).

$$Z = \frac{L}{P}$$

Z = Kennzahl für das Leistungs-Preis-Verhältnis

L = Leistung (Summe der Leistungspunkte aus der auf die Leistung bezogenen Bewertungsmatrix)

P = Angebotssumme (Euro)

In einem zweiten Schritt der Angebotswertung scheiden alle Angebote aus der Wertung aus, die außerhalb eines Schwankungsbereichs von 10,0 Prozent der besten Kennzahl Z im Wettbewerb liegen. Unter den danach in der Angebotswertung verbliebenen Angeboten erhält das Angebot den Zuschlag, das den besten Wert der Kennzahl L erreicht (Entscheidungskriterium). Für den Fall dann noch gleicher Kennzahlen entscheidet die günstigere Angebotssumme.

Die Leistungsbewertung erfolgt gemäß der im Arbeitsschritt „Leistungskriterien“ des eVergabe-Systems und der in der auf die Leistung bezogenen Bewertungsmatrix angegebenen Gewichtung und Bepunktung.

Der Gesamtangebotspreis als Wertungspreis P wird gemäß Arbeitsschritt „Produkte/Leistungen“ ermittelt.

#### 4. vorläufige Zeitplanung

Dem Vergabeverfahren liegt nachfolgender, vorläufiger Zeitplan zugrunde:

Verfahrensschritt	Termin
Auftragsbekanntmachung	19.05.2026
Frist für Bieterfragen	08.06.2026
Angebotsfrist	19.06.2026
Zuschlagserteilung	Vsl. in der KW 30

**Tabelle 1: vorläufiger Zeitplan**

Von dieser Zeitplanung kann bei Bedarf abgewichen werden.

Projekt-Nr.: 2026THA000002

Aktenzeichen: H 1620.2.1-2014

Projektname: App-Katalog zum App-Security-Check; LSI

Firmenbezeichnung und Anschrift

Angaben zu Fristen und Ansprechpartner

Ablauf der Angebotsfrist: 03.07.2026 11:00:00

voraussichtliche Ausführungsfrist:

Beginn:

Ende:

E-Mail: ausschreibung@lfst.bayern.de

Datum: 08.06.2026

## Aufforderung zur Angebotsabgabe

Sehr geehrte Damen und Herren,

die Vergabestelle beabsichtigt, einen öffentlichen Auftrag zu vergeben. Die Auftragsbekanntmachung und die Vergabeunterlagen sind unter [www.auftraege.bayern.de](http://www.auftraege.bayern.de) hinterlegt.

Falls Sie an diesem Auftrag interessiert sind, bitten wir Sie, ein Angebot abzugeben.

Soweit in den Vergabeunterlagen nicht anders vorgegeben, ist das Angebot in elektronischer Form und deutscher Sprache über das Portal [www.auftraege.bayern.de](http://www.auftraege.bayern.de) einzureichen.

Wir würden uns über ein Angebot Ihrerseits sehr freuen.

Freundliche Grüße

Tanja Hammerl



Projekt-Nr.: 2026THA000002

Aktenzeichen: H 1620.2.1-2014

Projektname: App-Katalog zum App-Security-Check; LSI

## Darstellung der Struktur des Bieters

### 1. Angaben zur Struktur

Name des Bieters / der Bietergemeinschaft:

Die Beteiligung erfolgt

- ☐ als Einzelbieter
- ☐ als Bietergemeinschaft
- ☐ unter Einbeziehung von Unterauftragnehmern

Auf die Ausführungen zu den besonderen Beteiligungsformen und zur Eignungsleihe in den Bewerbungsbedingungen wird ausdrücklich hingewiesen.

### 2. Angaben zu Unterauftragnehmern

Name, Vorname bzw. Firmenbezeichnung	Anschrift bzw. Firmensitz	Vorgesehene Aufgaben im Rahmen des Projekts (bei bevorzugten Bietern: Anteil am Gesamtangebot)
---	------------------------------	---


### 3. Angaben zur Eignungsleihe

Folgende Kapazitäten anderer Unternehmen sollen zum Nachweis der wirtschaftlichen und finanziellen bzw. technischen und beruflichen Leistungsfähigkeit in Anspruch genommen werden:

Name, Vorname bzw. Firmenbezeichnung	Anschrift bzw. Firmensitz	Kapazitäten des Unternehmens, die für die Eignungsleihe in Anspruch genommen werden
--------------------------------------	---------------------------	---


Entsprechend unterschriebene **Verpflichtungserklärungen** der Eignungsverleiher sind dem Angebot beizufügen.

### 4. Angaben zur Bietergemeinschaft

#### 4.1. Mitglieder der Bietergemeinschaft

Name, Vorname bzw. Firmenbezeichnung	Anschrift bzw. Firmensitz	Vorgesehene Aufgaben im Rahmen des Projekts (bei bevorzugten Bietern: Anteil am Gesamtangebot)
--------------------------------------	---------------------------	---


#### 4.2. Bevollmächtigter Vertreter

Angabe des von allen Mitgliedern für die Durchführung des Vergabeverfahrens und Vertrages gegenüber dem Auftraggeber bevollmächtigten Vertreters:

--

Projekt-Nr.: 2026THA000002

Aktenzeichen: H 1620.2.1-2014

Projektname: App-Katalog zum App-Security-Check; LSI

Firmenbezeichnung und -anschrift

## Eigenerklärung

mit Angebotsabgabe erklärt der Angebotsersteller oder bei Bewerber- / Bietergemeinschaften deren bevollmächtigter Vertreter für die beteiligten Unternehmen Folgendes:

- Es ist keine Person, deren Verhalten dem Unternehmen zuzurechnen ist, wegen einer der in § 123 Abs. 1 GWB genannten Straftaten (z.B. §§ 129 - 129b, 89c, 261, 263, 264, 299 - 299b, 108e, 108f, 333 - 335a, 232 - 233a StGB, Art. 2 § 2 IntBestG) oder vergleichbarer Vorschriften anderer Staaten verurteilt worden und es ist auch nicht aus denselben Gründen eine Geldbuße nach § 30 OWiG gegen das Unternehmen festgesetzt worden.
- Das Unternehmen hat seine Verpflichtungen zur Zahlung von Steuern, Abgaben und Beiträgen zur Sozialversicherung ordnungsgemäß erfüllt.
- Das Unternehmen hat bei der Ausführung öffentlicher Aufträge nicht gegen geltende menschen-, umwelt-, sozial- oder arbeitsrechtliche Verpflichtungen verstoßen. Insbesondere
  - wird gem. § 7 Abs. 1 AGG, § 3 Abs. 1 EntgTranspG und § 2 Nr. 7 AEntG Frauen und Männern für gleiche oder gleichwertige Arbeit gleiches Entgelt gewährt.
  - werden gem. § 3 Gesetz über die unternehmerischen Sorgfaltspflichten in Lieferketten die in Abschnitt 2 dieses Gesetzes festgelegten menschenrechtlichen und umweltbezogenen Sorgfaltspflichten in angemessener Weise beachtet.

- werden den Arbeitnehmerinnen und Arbeitnehmern wenigstens diejenigen Mindestarbeitsbedingungen einschließlich des Mindestentgelts gewährt, die nach dem Mindestlohngesetz (MiLoG), einem nach dem Tarifvertragsgesetz mit den Wirkungen des Arbeitnehmer-Entsendegesetzes (AEntG) für allgemein verbindlich erklärten Tarifvertrag, oder einer nach den §§ 7, 7a oder 11 AEntG oder § 3a des AÜG erlassenen Rechtsverordnung für die betreffende Leistung verbindlich vorgegeben werden.
- Das Unternehmen ist nicht zahlungsunfähig, es ist über das Vermögen des Unternehmens kein Insolvenzverfahren oder vergleichbares Verfahren beantragt oder eröffnet oder mangels Masse abgelehnt worden, und es befindet sich auch nicht in Liquidation oder hat seine Tätigkeit eingestellt.
- Das Unternehmen hat keine schweren Verfehlungen begangen, die seine Integrität als Auftragnehmer für öffentliche Aufträge in Frage stellen. Dies gilt auch für Personen, deren Verhalten dem Unternehmen zuzurechnen ist.
- Das Unternehmen hat im Vergabeverfahren keine vorsätzlich unzutreffenden Erklärungen abgegeben, keine irreführenden Informationen übermittelt und mit anderen Unternehmen keine Vereinbarungen getroffen, die eine Verhinderung, Einschränkung oder Verfälschung des Wettbewerbs bezwecken oder bewirken.
- Es liegt kein Ausschlussgrund nach § 21 AEntG, § 98c AufenthG, § 19 MiloG, § 21 SchwarzArbG und § 22 LkSG vor. Insbesondere wurde gegen das Unternehmen keine Geldbuße von mindestens 2.500 € wegen eines Verstoßes nach § 23 AEntG oder § 21 MiloG verhängt. Auch wurde gegen das Unternehmen oder einen Vertretungsberechtigten keine Freiheitsstrafe von mehr als drei Monaten und keine Geldstrafe von mehr als 90 Tagessätzen oder Geldbuße von mindestens 2.500 € wegen Verstoßes gegen eine in § 21 SchwarzArbG aufgeführte Vorschrift verhängt.

Tritt bei den vorgenannten Umständen zu einem späteren Zeitpunkt eine Änderung ein, so ist dies dem Auftraggeber unverzüglich mitzuteilen. Wesentlich falsche Erklärungen können den Ausschluss von diesem und weiteren Verfahren zur Folge haben. Werden diese Umstände nach Auftragserteilung bekannt, steht dem Auftraggeber ein außerordentliches Kündigungsrecht zu. Mögliche Schadensersatzforderungen bleiben davon unberührt.

Sollten für Sie bzw. Ihr Unternehmen fakultative Ausschlussgründe nach § 124 GWB vorliegen, schildern Sie bitte im Arbeitsschritt Eignungskriterien, weshalb diese nicht zu einem Ausschluss vom Verfahren führen sollen.

Der Auftraggeber entscheidet im Rahmen der Angebotsprüfung über den Ausschluss.

Projekt-Nr.: 2026THA000002

Aktenzeichen: H 1620.2.1-2014

Projektname: App-Katalog zum App-Security-Check; LSI

Firmenbezeichnung und -anschrift

## Eigenerklärung russische Unternehmen

mit Angebots- / Teilnahmeantragsabgabe erklärt der Angebotsersteller, bei Bewerber- / Bietergemeinschaften deren bevollmächtigter Vertreter Folgendes:

1. Der / die **Bewerber / Bieter** gehört / gehören nicht zu den in Artikel 5 k) Absatz 1 der Verordnung (EU) Nr. 833/2014 in der Fassung des Art. 1 Ziff. 23 der Verordnung (EU) 2022/576 des Rates vom 8. April 2022 über restriktive Maßnahmen angesichts der Handlungen Russlands, die die Lage in der Ukraine destabilisieren, genannten Personen oder Unternehmen, die einen **Bezug zu Russland** im Sinne der Vorschrift aufweisen,
  - a. durch die russische Staatsangehörigkeit des Bewerbers/Bieters oder die Niederlassung des Bewerbers / Bieters in Russland,
  - b. durch die Beteiligung einer natürlichen Person oder eines Unternehmens, auf die eines der Kriterien nach Buchstabe a zutrifft, am Bewerber / Bieter über das Halten von Anteilen im Umfang von mehr als 50 %,
  - c. durch das Handeln der Bewerber / Bieter im Namen oder auf Anweisung von Personen oder Unternehmen, auf die die Kriterien der Buchstaben a und / oder b zutrifft.

2. Es wird bestätigt, dass die am Auftrag beteiligten **Unterauftragnehmer, Lieferanten oder Unternehmen, deren Kapazitäten im Zusammenhang mit der Erbringung des Eignungsnachweises in Anspruch genommen werden**, auf die mehr als 10 % des Auftragswerts entfällt, ebenfalls nicht zu dem in der Vorschrift genannten Personenkreis mit einem Bezug zu Russland im Sinne der Vorschrift gehören.
3. Es wird bestätigt und sichergestellt, dass auch während der Vertragslaufzeit keine als **Unterauftragnehmer, Lieferanten oder Unternehmen, deren Kapazitäten im Zusammenhang mit der Erbringung des Eignungsnachweises in Anspruch genommen werden**, beteiligten Unternehmen eingesetzt werden, die zu dem in der Vorschrift genannten Personenkreis mit einem Bezug zu Russland im Sinne der Vorschrift gehören und auf die mehr als 10 % des Auftragswerts entfällt.

**Artikel 5k der Verordnung (EU) Nr. 833/2014 in der Fassung des Art. 1 Ziff. 23  
der Verordnung (EU) 2022/576 des Rates vom 8. April 2022 lautet wie folgt:**

- (1) Es ist verboten, öffentliche Aufträge oder Konzessionen, die in den Anwendungsbereich der Richtlinien über die öffentliche Auftragsvergabe sowie unter Artikel 10 Absatz 1, Absatz 3, Absatz 6 Buchstaben a bis e, Absatz 8, Absatz 9 und Absatz 10 und die Artikel 11, 12, 13 und 14 der Richtlinie 2014/23/EU, unter die Artikel 7 und 8, Artikel 10 Buchstaben b bis f und h bis j der Richtlinie 2014/24/EU, unter Artikel 18, Artikel 21 Buchstaben b bis e und g bis i, Artikel 29 und Artikel 30 der Richtlinie 2014/25/EU und unter Artikel 13 Buchstaben a bis d, f bis h und j der Richtlinie 2009/81/EG fallen, an folgende Personen, Organisationen oder Einrichtungen zu vergeben bzw. Verträge mit solchen Personen, Organisationen oder Einrichtungen weiterhin zu erfüllen:
- a) russische Staatsangehörige oder in Russland niedergelassene natürliche oder juristische Personen, Organisationen oder Einrichtungen,
  - b) juristische Personen, Organisationen oder Einrichtungen, deren Anteile zu über 50 % unmittelbar oder mittelbar von einer der unter Buchstabe a genannten Organisationen gehalten werden, oder
  - c) natürliche oder juristische Personen, Organisationen oder Einrichtungen, die im Namen oder auf Anweisung einer der unter Buchstabe a oder b genannten Organisationen handeln,
- auch solche, auf die mehr als 10 % des Auftragswerts entfällt, Unterauftragnehmer, Lieferanten oder Unternehmen, deren Kapazitäten im Sinne der Richtlinien über die öffentliche Auftragsvergabe in Anspruch genommen werden.
- (2) Abweichend von Absatz 1 können die zuständigen Behörden die Vergabe oder die Fortsetzung der Erfüllung von Verträgen genehmigen, die bestimmt sind für
- a) den Betrieb ziviler nuklearer Kapazitäten, ihre Instandhaltung, ihre Stilllegung, die Entsorgung ihrer radioaktiven Abfälle, ihre Versorgung mit und die Wiederaufbereitung von Brennelementen und die Weiterführung der Planung, des Baus und die Abnahmetests für die Indienststellung ziviler Atomanlagen und ihre Sicherheit sowie die Lieferung von Ausgangsstoffen zur Herstellung medizinischer Radioisotope und ähnlicher medizinischer Anwendungen, kritischer Technologien zur radiologischen Umweltüberwachung sowie für die zivile nukleare Zusammenarbeit, insbesondere im Bereich Forschung und Entwicklung,
  - b) die zwischenstaatliche Zusammenarbeit bei Raumfahrtprogrammen,
  - c) die Bereitstellung unbedingt notwendiger Güter oder Dienstleistungen, wenn sie ausschließlich oder nur in ausreichender Menge von den in Absatz 1 genannten Personen bereitgestellt werden können,
  - d) die Tätigkeit der diplomatischen und konsularischen Vertretungen der Union und der Mitgliedstaaten in Russland, einschließlich Delegationen, Botschaften und Missionen, oder internationaler Organisationen in Russland, die nach dem Völkerrecht Immunität genießen.
  - e) den Kauf, die Einfuhr oder die Beförderung von Erdgas und Erdöl, einschließlich raffinierter Erdölerzeugnisse, sowie von Titan, Aluminium, Kupfer, Nickel, Palladium und Eisenerz aus oder durch Russland in die Union, oder
  - f) den Kauf, die Einfuhr oder die Beförderung von Kohle und anderen festen fossile Brennstoffen, die in Anhang XXII aufgeführt sind, bis 10. August 2022.
- (3) Der betreffende Mitgliedstaat unterrichtet die anderen Mitgliedstaaten und die Kommission über jede nach diesem Artikel erteilte Genehmigung innerhalb von zwei Wochen nach deren Erteilung.
- (4) Die Verbote gemäß Absatz 1 gelten nicht für die Erfüllung — bis zum 10. Oktober 2022 — von Verträgen, die vor dem 9. April 2022 geschlossen wurden.

Projekt-Nr.: 2026THA000002

Aktenzeichen: H 1620.2.1-2014

Projektname: App-Katalog zum App-Security-Check; LSI

Firmenbezeichnung und –anschrift  
des Unterauftragnehmers oder Eignungsverleiher

## Eigenerklärung

Als Unterauftragnehmer oder Eignungsverleiher für

erkläre ich **für mein Unternehmen** Folgendes:

- Es ist keine Person, deren Verhalten dem Unternehmen zuzurechnen ist, wegen einer der in § 123 Abs. 1 GWB genannten Straftaten (z.B. §§ 129 - 129b, 89c, 261, 263, 264, 299 - 299b, 108e, 108f, 333 - 335a, 232 - 233a StGB, Art. 2 § 2 IntBestG) oder vergleichbarer Vorschriften anderer Staaten verurteilt worden und es ist auch nicht aus denselben Gründen eine Geldbuße nach § 30 OWiG gegen das Unternehmen festgesetzt worden.
- Das Unternehmen hat seine Verpflichtungen zur Zahlung von Steuern, Abgaben und Beiträgen zur Sozialversicherung ordnungsgemäß erfüllt.
- Das Unternehmen hat bei der Ausführung öffentlicher Aufträge nicht gegen geltende umwelt-, sozial- oder arbeitsrechtliche Verpflichtungen verstoßen. Insbesondere
  - wird gem. § 7 Abs. 1 AGG, § 3 Abs. 1 EntgTranspG und § 2 Nr. 7 AEntG Frauen und Männern für gleiche oder gleichwertige Arbeit gleiches Entgelt gewährt.



- werden gem. § 3 Gesetz über die unternehmerischen Sorgfaltspflichten in Lieferketten die in Abschnitt 2 dieses Gesetzes festgelegten menschenrechtlichen und umweltbezogenen Sorgfaltspflichten in angemessener Weise beachtet.
  - werden den Arbeitnehmerinnen und Arbeitnehmern wenigstens diejenigen Mindestarbeitsbedingungen einschließlich des Mindestentgelts gewährt, die nach dem Mindestlohngesetz (MiLoG), einem nach dem Tarifvertragsgesetz mit den Wirkungen des Arbeitnehmer-Entsendegesetzes (AEntG) für allgemein verbindlich erklärten Tarifvertrag, oder einer nach den §§ 7, 7a oder 11 AEntG oder § 3a des AÜG erlassenen Rechtsverordnung für die betreffende Leistung verbindlich vorgegeben werden.
- Das Unternehmen ist nicht zahlungsunfähig, es ist über das Vermögen des Unternehmens kein Insolvenzverfahren oder vergleichbares Verfahren beantragt oder eröffnet oder mangels Masse abgelehnt worden, und es befindet sich auch nicht in Liquidation oder hat seine Tätigkeit eingestellt.
  - Das Unternehmen hat keine schweren Verfehlungen begangen, die seine Integrität als Auftragnehmer für öffentliche Aufträge in Frage stellen. Dies gilt auch für Personen, deren Verhalten dem Unternehmen zuzurechnen ist.
  - Das Unternehmen hat im Vergabeverfahren keine vorsätzlich unzutreffenden Erklärungen abgegeben, keine irreführenden Informationen übermittelt und mit anderen Unternehmen keine Vereinbarungen getroffen, die eine Verhinderung, Einschränkung oder Verfälschung des Wettbewerbs bezwecken oder bewirken.
  - Es liegt kein Ausschlussgrund nach § 21 AEntG, § 98c AufenthG, § 19 MiloG, § 21 SchwarzArbG und § 22 LkSG vor. Insbesondere wurde gegen das Unternehmen keine Geldbuße von mindestens 2.500 € wegen eines Verstoßes nach § 23 AEntG oder § 21 MiloG verhängt. Auch wurde gegen das Unternehmen oder einen Vertretungsberechtigten keine Freiheitsstrafe von mehr als drei Monaten und keine Geldstrafe von mehr als 90 Tagessätzen oder Geldbuße von mindestens 2.500 € wegen Verstoßes gegen eine in § 21 SchwarzArbG aufgeführte Vorschrift verhängt.

Tritt bei den vorgenannten Umständen zu einem späteren Zeitpunkt eine Änderung ein, so ist dies dem Auftraggeber unverzüglich mitzuteilen. Wissentlich falsche Erklärungen können den Ausschluss von diesem und weiteren Verfahren zur Folge haben. Werden diese Umstände nach Auftragserteilung bekannt, steht dem Auftraggeber ein außerordentliches Kündigungsrecht zu. Mögliche Schadensersatzforderungen bleiben davon unberührt.

Sollten für Sie bzw. Ihr Unternehmen fakultative Ausschlussgründe nach § 124 GWB vorliegen, schildern Sie bitte in einem gesonderten Dokument, weshalb diese nicht zu einem Ausschluss vom Verfahren führen sollen.

Der Auftraggeber entscheidet im Rahmen der Angebotsprüfung über den Ausschluss.

Ort, Datum

Unterschrift

Projekt-Nr.: 2026THA000002

Aktenzeichen: H 1620.2.1-2014

Projektname: App-Katalog zum App-Security-Check; LSI

## **Schutzerklärung**

### **1. Erklärung zum Vergabeverfahren**

Der Bewerber / Bieter nimmt zur Kenntnis, dass die Nichtabgabe der Erklärung nach Nummer 2 oder die Abgabe einer wesentlich falschen Erklärung den Ausschluss von diesem Vergabeverfahren zur Folge hat.

### **2. Erklärung für den Fall der Zuschlagserteilung**

Der Bewerber / Bieter versichert,

- 2.1. dass er gegenwärtig sowie während der gesamten Vertragsdauer die Technologie von L. Ron Hubbard nicht anwendet, lehrt oder in sonstiger Weise verbreitet, er keine Kurse oder Seminare nach dieser Technologie besucht und Beschäftigte oder sonst zur Erfüllung des Vertrags eingesetzte Personen keine Kurse oder Seminare nach dieser Technologie besuchen lässt;
- 2.2. dass nach seiner Kenntnis keine der zur Erfüllung des Vertrags eingesetzten Personen die Technologie von L. Ron Hubbard anwendet, lehrt oder in sonstiger Weise verbreitet oder Kurse oder Seminare nach dieser Technologie besucht.
- 2.3. Der Bewerber / Bieter verpflichtet sich, solche zur Erfüllung des Vertrags eingesetzte Personen von der weiteren Durchführung des Vertrags unverzüglich auszuschließen, die während der Vertragsdauer die Technologie von L. Ron Hubbard anwenden, lehren, in sonstiger Weise verbreiten oder Kurse oder Seminare nach dieser Technologie besuchen.
- 2.4. Die Abgabe einer wesentlich falschen Erklärung nach Nummer 2.1 oder 2.2 sowie ein Verstoß gegen die Verpflichtung nach Nummer 2.3 berechtigen den Auftraggeber zur Kündigung aus wichtigem Grund ohne Einhaltung einer Frist. Weitergehende Rechte des Auftraggebers bleiben unberührt.

### **3. Hinweis nach Art. 9 Abs. 2 des Bayerischen Datenschutzgesetzes:**

Zur Erfüllung der Informationspflicht wird auf die folgende Bekanntmachung der Bayerischen Staatsregierung verwiesen.

## **Scientology-Organisation**

### **Verwendung von Schutzzerklärungen bei der Vergabe öffentlicher Aufträge**

**Bekanntmachung der Bayerischen Staatsregierung vom 29. Oktober 1996 Nr. 476-2-151 (AIIIMBI. S.701, StAnz. Nr. 44):**

Die Scientology-Organisation in allen ihren Erscheinungsformen ist eine Vereinigung, die unter dem Deckmantel einer Religionsgemeinschaft wirtschaftliche Ziele verfolgt und den einzelnen mittels rücksichtslos eingesetzter psycho- und sozial-technologischer Methoden einer totalen inneren und äußeren Kontrolle unterwirft, um ihn für ihre Ziele zu instrumentalisieren.

Auf Grund der jetzigen Erkenntnislage ist davon auszugehen, dass ein nach der Technologie von L. Ron Hubbard geführtes Unternehmen als Bestandteil der Gesamtorganisation Scientology zu betrachten ist. Ein derartiges Unternehmen übernimmt die Verpflichtung, die Technologie von L. Ron Hubbard und die Ideologie von Scientology zu verbreiten, ihren Bestand zu sichern und in der Gesellschaft als allgemeines Gedankengut zu etablieren. Dadurch droht auch öffentlichen Stellen bei Geschäftskontakten eine Infiltration und Ausforschung durch Scientology.

Um dieser Gefahr wirksam begegnen zu können, wird bestimmt:

1. Von Auftragnehmern ist bei der Vergabe öffentlicher Dienstleistungsaufträge in den nachfolgenden Fällen bei der Auftragsvergabe eine Schutzzerklärung gemäß Anlage zu verlangen, die bei Annahme des Angebots Vertragsbestandteil wird. Schutzzerklärungen sind zulässig und notwendig, um bei solchen Vertragsverhältnissen die Zuverlässigkeit und Leistungsfähigkeit des Auftragnehmers abzuklären, die
  - Möglichkeiten zur Einflussnahme auf die Organisation des Vertragspartners oder seine Beschäftigten eröffnen
  - ein besonderes Vertrauensverhältnis voraussetzen oder
  - die Offenlegung von wesentlichen internen Vorgängen und Daten gegenüber dem Vertragspartner erfordern.

Schutzzerklärungen kommen demnach regelmäßig in folgenden Vertragsverhältnissen in Betracht:

Unternehmensberatung, Personal- und Managementschulung, Fortbildungs- und Vortragsveranstaltungen, Softwareberatung, -entwicklung und -pflege, Projektentwicklung und -steuerung, Forschungs- und Untersuchungsaufträge.

2. Die Nichtabgabe der Erklärung oder die Abgabe einer wissenschaftlich falschen Erklärung hat den Ausschluss von dem laufenden Vergabeverfahren zur Folge.
3. Erweist sich nach Vertragsschluss, dass eine wissentlich falsche Erklärung abgegeben oder gegen die mit der Erklärung eingegangenen Verpflichtungen verstoßen wurde, so ist der Vertrag aus wichtigem Grund ohne Einhaltung einer Frist zu kündigen.
4. Den kommunalen Auftraggebern und den sonstigen der Aufsicht des Freistaates Bayern unterliegenden juristischen Personen des öffentlichen Rechts wird empfohlen, entsprechend zu verfahren. Das gleiche gilt für die Empfänger von Zuwendungen des Freistaates Bayern, wenn die Zuwendungen für Maßnahmen nach Nummer 1 gegeben werden.
5. Diese Bekanntmachung tritt am 1. November 1996 in Kraft.



## Dienstvertrag (Langfassung)

### Vertrag über IT-Dienstleistungen

#### Inhaltsangabe

1	Gegenstand und Bestandteile des Vertrages .....	2
1.1	Vertragsgegenstand .....	2
1.2	Vertragsbestandteile .....	2
2	Überblick über die vereinbarten Leistungen .....	3
3	Beschreibung der Leistungen/Laufzeit und Kündigung .....	4
3.1	Art, Umfang und Termine wird zur Zuschlagserteilung ergänzt .....	4
3.2	Einmalig zu erbringende Leistungen .....	4
3.3	Regelmäßig zu erbringende Leistungen .....	4
3.4	Leistungen, die nur auf Abruf erbracht werden sollen .....	5
3.5	Abweichende Kündigungsregelung .....	5
4	Vergütung .....	5
4.1	Vergütung nach Aufwand .....	5
4.1.1	Kategorien .....	6
4.1.2	Abweichende Regelungen für die Bestimmung und Vergütung von Personentagesätzen .....	6
4.1.3	Reisekosten/Nebenkosten*/Materialkosten/Reisezeiten .....	6
4.1.4	Preisanpassung .....	6
4.1.5	Fälligkeit und Zahlung .....	7
4.1.6	Besondere Bestimmungen zur Vergütung nach Aufwand .....	7
4.2	Vergütung zum Pauschalpreis .....	7
4.3	Rechnungsadresse .....	7
5	Service- und Reaktionszeiten* .....	7
5.1	Servicezeiten* .....	7
5.2	Reaktionszeiten* .....	8
6	Ansprechpartner .....	9
7	Besondere Anforderungen an Mitarbeiter des Auftragnehmers .....	9
8	Mitwirkungsleistungen des Auftraggebers .....	9
9	Abweichende Nutzungsrechte an den Leistungsergebnissen, Erfindungen .....	9
10	Quellcode* und Software Bill of Materials (SBOM) .....	10
11	Abweichende Haftungsregelungen .....	11
12	Vertragsstrafen .....	11
13	Weitere Regelungen .....	11
13.1	Datenschutz, Geheimhaltung und Sicherheit .....	11
13.2	Haftpflichtversicherung .....	11
13.3	Teleservice* .....	12
13.4	Dokumentations- und Berichtspflichten .....	12
13.5	Interessenkonflikt .....	12
14	Pflichten nach Vertragsende .....	12
15	Sonstige Vereinbarungen .....	12



## Dienstvertrag (Langfassung)

### Vertrag über IT-Dienstleistungen

zwischen Freistaat Bayern, vertreten durch das  
Landesamt für Sicherheit in der Informationstechnik  
Keßlerstraße 1  
90489 Nürnberg

Vertragsnummer/Kennung Auftraggeber: O 1088.7-1-7

„Auftraggeber“

und **wird zur Zuschlagserteilung ergänzt**

Vertragsnummer/Kennung Auftragnehmer: \_\_\_\_\_

„Auftragnehmer“

wird folgender Vertrag geschlossen:

#### 1 Gegenstand und Bestandteile des Vertrages

##### 1.1 Vertragsgegenstand

Gegenstand des Vertrages sind Dienstleistungen des Auftragnehmers Gegenstand dieses Vertrages sind Sicherheitsbewertungen für Smartphone-Applikationen unter Verwendung weitgehend automatisierter Prüfverfahren und Bereitstellung der Prüfergebnisse in einem Katalog.

##### 1.2 Vertragsbestandteile

Es gelten als Vertragsbestandteile:

##### 1.2.1 dieser Vertragstext mit den folgenden Anlagen: **wird zur Zuschlagserteilung ergänzt**

Anlage Nr.	Bezeichnung	Datum/Version	Anzahl Seiten
01	Rahmenkonzept		
02	Leistungsbeschreibung		
03	Datenschutz- und Vertraulichkeitsvereinbarung		
04	Vereinbarung zur Auftragsverarbeitung (AVV), verbindlicher Entwurf		
05	Datenschutzinformationen		
06	Angebot		
06a	Preiszusammenstellung		
06b	Bewertungsmatrix Eignung		

## Dienstvertrag (Langfassung)

Anlage Nr.	Bezeichnung	Datum/Version	Anzahl Seiten
06c	Bewertungsmatrix Leistung		
06d	Anforderungskatalog Barrierefreiheit		
06e	PTA		

☐ Es gelten die Anlagen in folgender Rangfolge \_\_\_\_\_.

**1.2.2 die Ergänzenden Vertragsbedingungen für IT-Dienstleistungen (EVB-IT Dienstleistungs-AGB) in der bei Bereitstellung der Vergabeunterlagen geltenden Fassung einschließlich der Muster 1 und 2**

**1.2.3 sowie nachrangig die Allgemeinen Vertragsbedingungen für die Ausführung von Leistungen (VOL/B) in der bei Bereitstellung der Vergabeunterlagen geltenden Fassung.**

Die EVB-IT Dienstleistungs-AGB stehen unter [evb-it.gov.de](http://evb-it.gov.de) zur Einsichtnahme bereit. Die VOL/B wurde im Bundesanzeiger AT Nr. 178a vom 23. September 2003 veröffentlicht.

Soweit Allgemeine Geschäftsbedingungen im Sinne von § 305 BGB in den hier referenzierten Dokumenten des Auftragnehmers bzw. den sonstigen vom Auftragnehmer beigefügten Anlagen zu diesem Vertrag Regelungen in den EVB-IT Dienstleistungs-AGB widersprechen, sind sie ausgeschlossen, soweit nicht eine anderweitige Vereinbarung in den EVB-IT Dienstleistungs-AGB zugelassen ist.

Weitere Geschäftsbedingungen sind ausgeschlossen, soweit in diesem Vertrag nichts anderes vereinbart ist.

Für alle in diesem Vertrag genannten Beträge gilt einheitlich der Euro als Währung. Die vereinbarten Vergütungen verstehen sich zuzüglich der gesetzlichen Umsatzsteuer, soweit Umsatzsteuerpflicht besteht.

Die mit \* gekennzeichneten Begriffe sind am Ende der EVB-IT Dienstleistungs-AGB definiert.

## 2 Überblick über die vereinbarten Leistungen

Der Auftragnehmer erbringt für den Auftraggeber folgende Dienstleistungen:

- ☐ Beratung
- ☐ Projektleitungsunterstützung
- ☐ Schulung
- ☐ Einführungsunterstützung
- ☐ Betreiberleistungen
- ☐ Benutzerunterstützungsleistungen
- ☐ Providerleistungen ohne Inhaltsverantwortlichkeit
- ☐ Unterstützung bei Planungsleistungen
- ☐ Unterstützung bei Softwareentwicklung
- ☐ Hotline
- ☒ sonstige Dienstleistungen

## Dienstvertrag (Langfassung)

### 3 Beschreibung der Leistungen/Laufzeit und Kündigung

#### 3.1 Art, Umfang und Termine wird zur Zuschlagserteilung ergänzt

Art, Umfang und Termine der zu erbringenden Leistungen ergeben sich aus der folgenden Tabelle (Termin- und Leistungsplan):

Lfd. Nr.	Leistung (ggf. Verweis auf Anlage)	Ort der Leistung	MVD <sup>1</sup>	Beginn <sup>2</sup>	Ende/Termin <sup>3</sup>
01	fortlaufende Prüfung gängiger Apps und Bereitstellung in einem Katalog gemäß Anlage 02 (Leistungsbeschreibung)	Nürnberg	24	Mit Zuschlag, frühestens 01.09.2026	Gemäß Nummer 3.5
02	Einmalige Leistungen gemäß Anlage 02 (Leistungsbeschreibung), z.B. Implementierung von Funktionen	Nürnberg	--	Mit lfd. Nr. 01	--
03	Arbeitsbesprechungen per Videokonferenz (Optional, gesonderter Abruf durch den Auftraggeber)	Nürnberg	--	--	--

Fußnote	Erläuterung
1	MVD = Mindestvertragsdauer
2	wenn keine Vorgabe für Beginn, dann Feld leer lassen
3	z. B. festes Datum ggf. mit Uhrzeit oder „nach 48 Monaten“ (wenn Vertrag unbefristet, dann Feld leer lassen)

- ☐ Feiertage im Sinne dieses Vertrages sind die Feiertage in \_\_\_\_\_ (siehe Ziffer 5.1 EVB-IT Dienstleistungs-AGB).

#### 3.2 Einmalig zu erbringende Leistungen

- ☒ Die Leistungen gemäß Nummer 3.1 lfd. Nr. 02 werden einmalig erbracht.

#### 3.3 Regelmäßig zu erbringende Leistungen

- ☒ Die Leistungen gemäß Nummer 3.1 lfd. Nr. 01 werden

- ☒ in folgendem Zyklus erbracht:

- ☒ regelmäßig/fortlaufend (gemäß Anlage 02 Leistungsbeschreibung)

- ☐ wöchentlich

- ☐ monatlich

jeweils

- ☐ an folgenden Tagen: \_\_\_\_\_ (Wochentag(e) bzw. bei monatlichen Zyklen auch „1. Montag im Monat“)

- ☐ in der Zeit von \_\_\_\_\_ bis \_\_\_\_\_ (Uhrzeit)

nicht jedoch an Feiertagen.





## Dienstvertrag (Langfassung)

- ☐ in folgenden Zyklen zu folgenden Zeiten erbracht: \_\_\_\_\_.

### 3.4 Leistungen, die nur auf Abruf erbracht werden sollen

- ☒ Die Leistungen gemäß Nummer 3.1 lfd. Nr. 03 werden nur auf Abruf erbracht.
- ☐ Der Mindestvorlauf für den Abruf beträgt \_\_\_\_\_ (Stunden/Tage).
- ☐ Die geschätzte Abnahme beträgt \_\_\_\_\_ (Stunden/Tage) pro \_\_\_\_\_ (z. B. Vertragsmonat/Vertragsquartal/Vertragsjahr/Vertragslaufzeit).
- ☐ Die vereinbarte Mindestabnahme beträgt \_\_\_\_\_ (Stunden/Tage) pro \_\_\_\_\_ (z. B. Vertragsmonat, Vertragsquartal, Vertragsjahr, Vertragslaufzeit).
- ☐ Die Mindestabnahme für Leistungen, die Reisen erforderlich machen, beträgt pro Abruf \_\_\_\_\_ (Stunden/Tage).

Soweit Leistungen nur auf Abruf zu erbringen sind, hält sich der Auftragnehmer in dem vorgenannten Zeitraum zur Leistungserbringung bereit.

### 3.5 Abweichende Kündigungsregelung

- ☐ Abweichend von Ziffer 15.1 EVB-IT Dienstleistungs-AGB beträgt die Kündigungsfrist \_\_\_\_\_ Monat(e) zum Ablauf eines \_\_\_\_\_ (z.B. Kalendermonats/Kalendervierteljahres/Kalenderjahres).
- ☐ Abweichend von Ziffer 15.1 EVB-IT Dienstleistungs-AGB wird bei vereinbarter fester Laufzeit ein Sonderkündigungsrecht gem. Anlage Nr. 02 vereinbart.
- ☒ Die Laufzeit dieses Vertrages mit allen enthaltenen Leistungen des Auftragnehmers gemäß Nummer 3.1 beginnt mit dem Anfang des übernächsten Kalendermonats nach Zuschlagserteilung, jedoch nicht vor dem 01.09.2026 und beträgt 24 Monate (Grundvertragslaufzeit).
- Der Vertrag verlängert sich 3mal jeweils um 12 Monate zu denselben Bedingungen, wenn er nicht mit einer Frist von 3 Monaten zu seinem Ende durch den Auftraggeber gekündigt wird. Er endet jedoch spätestens nach 60 Monaten, ohne dass es einer Kündigung bedarf. Eine Verlängerung aufgrund dieser Klausel erfolgt nicht, soweit der Vertrag vorzeitig endete.

## 4 Vergütung

### 4.1 Vergütung nach Aufwand

- ☐ Die Leistungen gemäß
- ☐ Nummer 3.1 lfd. Nr. \_\_\_\_\_ werden nach Aufwand gemäß Kategorie(n) \_\_\_\_\_ aus Nummer 4.1.1
- ☐ mit einer Obergrenze in Höhe von \_\_\_\_\_ Euro
- ☐ Nummer 3.1 lfd. Nr. \_\_\_\_\_ werden nach Aufwand gemäß Kategorie(n) \_\_\_\_\_ aus Nummer 4.1.1
- ☐ mit einer Obergrenze in Höhe von \_\_\_\_\_ Euro
- ☐ Nummer 3.1 lfd. Nr. \_\_\_\_\_ werden nach Aufwand gemäß Kategorie(n) \_\_\_\_\_ aus Nummer 4.1.1
- ☐ mit einer Obergrenze in Höhe von \_\_\_\_\_ Euro

vergütet.

## Dienstvertrag (Langfassung)

### 4.1.1 Kategorien

Lfd. Nr.	Bezeichnung der Kategorie	Stundensatz für Tätigkeiten innerhalb der zuschlagsfreien Zeiten	Tagessatz für Tätigkeiten innerhalb der zuschlagsfreien Zeiten	Zuschläge in Prozent auf die Stunden- und Tagessätze Montag bis Freitag (Arbeitstage) außerhalb der zuschlagsfreien Zeiten	Zuschläge in Prozent auf die Stunden- und Tagessätze Samstag von ____ bis ____	Zuschläge in Prozent auf die Stunden- und Tagessätze Samstag von ____ bis ____	Zuschläge in Prozent auf die Stunden- und Tagessätze Sonn- und Feiertage von ____ bis ____	Zuschläge in Prozent auf die Stunden- und Tagessätze Sonn- und Feiertage von ____ bis ____
				____ %	____ %	____ %	____ %	____ %

### Festlegung der zuschlagsfreien Zeiten:

Arbeitstag	zuschlagsfreie Zeiten
Montag bis Donnerstag	von ____ bis ____ Uhr
Freitag	von ____ bis ____ Uhr

- ☐ Weitere Vereinbarungen gemäß Anlage Nr. \_\_\_\_.

### 4.1.2 Abweichende Regelungen für die Bestimmung und Vergütung von Personentagesätzen

- ☐ Abweichend von Ziffer 9.2.4 Satz 2 EVB-IT Dienstleistungs-AGB können bei entsprechendem Nachweis pro Kalendertag bis zu 10 Stunden abgerechnet werden.
- ☐ Abweichend von Ziffer 9.2.4 Sätze 2 und 3 Dienstleistungs-AGB kann ein voller Tagessatz nur in Rechnung gestellt werden, wenn mindestens 10 Stunden geleistet wurden. Werden weniger als 10 Zeitstunden pro Tag geleistet, sind diese anteilig in Rechnung zu stellen.
- ☐ weitere Vereinbarungen gemäß Anlage Nr. \_\_\_\_.

### 4.1.3 Reisekosten/Nebenkosten\*/Materialkosten/Reisezeiten

- ☐ Reisekosten werden nicht gesondert vergütet.
- ☐ Reisekosten werden vergütet gemäß Anlage Nr. \_\_\_\_.
- ☐ Nebenkosten\* werden nicht gesondert vergütet.
- ☐ Nebenkosten\* werden vergütet gemäß Anlage Nr. \_\_\_\_.
- ☐ Materialkosten werden nicht gesondert vergütet.
- ☐ Materialkosten werden vergütet gemäß Anlage Nr. \_\_\_\_.
- ☐ Reisezeiten werden nicht gesondert vergütet.
- ☐ Reisezeiten werden zu 50 % als Arbeitszeiten vergütet.
- ☐ Reisezeiten werden vergütet gemäß Anlage Nr. \_\_\_\_.

### 4.1.4 Preisanpassung

- ☐ Es wird eine Preisanpassung



## Dienstvertrag (Langfassung)

- ☐ gemäß Ziffer 9.5 EVB-IT Dienstleistungs-AGB
- ☐ gemäß Anlage Nr. \_\_\_\_\_  
für die Kategorien gemäß Nummer 4.1.1 vereinbart.

### 4.1.5 Fälligkeit und Zahlung

Die Vergütung ist abweichend von Ziffer 9.3 EVB-IT Dienstleistungs-AGB nicht monatlich nachträglich fällig, sondern

- ☐ zum 15. des auf die Leistungserbringung folgenden Monats.
- ☐ wie folgt \_\_\_\_\_.
- ☐ gemäß Anlage Nr. \_\_\_\_\_.

### 4.1.6 Besondere Bestimmungen zur Vergütung nach Aufwand

- ☐ Besondere Bestimmungen zur Vergütung nach Aufwand sind in Anlage Nr. \_\_\_\_\_ vereinbart.

### 4.2 Vergütung zum Pauschalpreis

- ☒ Die Leistungen gemäß Nummer 3.1 lfd. Nr. 01, 02 und 03 werden mit jeweiligem Pauschalpreis vergütet.
- ☐ Es werden folgende Abschlagszahlungen vereinbart:

### 4.3 Rechnungsadresse

Rechnungen sind an folgende Anschrift zu richten:

Landesamt für Sicherheit in der Informationstechnik  
Referat 42  
Keßlerstraße 1  
90489 Nürnberg

USt-ID: DE316140712

Die Rechnung ist als eRechnung (XML oder ZUGFeRD) per E-Mail an [referat42@lsi.bayern.de](mailto:referat42@lsi.bayern.de) zu senden.

## 5 Service- und Reaktionszeiten\*

- ☐ Für die Leistungen gemäß Nummer 3.1 lfd. Nr. \_\_\_\_\_ werden folgende Service- und Reaktionszeiten\* vereinbart:

### 5.1 Servicezeiten\*

Tag	Uhrzeit
_____ bis _____	von _____ bis _____ Uhr
An Sonntagen	von _____ bis _____ Uhr
An Feiertagen	von _____ bis _____ Uhr

- ☐ Weitere Vereinbarungen zu Servicezeiten\* gemäß Anlage Nr. \_\_\_\_\_.



## Dienstvertrag (Langfassung)

### 5.2 Reaktionszeiten\*

Leistung gemäß Nummer 3.1	Anlass/Problemkategorie	Reaktionszeit* in Stunden

☐ Die Reaktionszeiten\* werden in Anlage Nr. \_\_\_\_\_ festgelegt.

Reaktionszeiten\* beginnen ausschließlich mit Zugang der entsprechenden Meldung oder dem Eintritt des vereinbarten Ereignisses während der vereinbarten Servicezeiten\* und laufen ausschließlich während der vereinbarten Servicezeiten\*.

Ergänzend können in Nummer 12 für die Nichteinhaltung der o.g. Zeiten Vertragsstrafen vereinbart werden.



## Dienstvertrag (Langfassung)

### 6 Ansprechpartner

Ansprechpartner des Auftraggebers (Name, Adresse, Abteilung, Telefon, Fax, E-Mail):

fachlich/technisch: wird zur Zuschlagserteilung ergänzt

vertraglich: wird zur Zuschlagserteilung ergänzt

Ansprechpartner des Auftragnehmers (Name, Adresse, Abteilung, Telefon, Fax, E-Mail):

wird zur Zuschlagserteilung ergänzt

### 7 Besondere Anforderungen an Mitarbeiter des Auftragnehmers

- ☐ Mindestanforderungen an das einzusetzende Personal des Auftragnehmers:

Lfd. Nr.	Position	Schlüsselposition gemäß Ziffer 8.3 EVB-IT Dienstleistungs-AGB (ja/nein)	Fachliche Qualifikation	Sicherheitsüberprüfung Ü 1, 2 oder 3 <sup>1</sup>	Sonstige Anforderungen, z. B. weitere Sicherheitsanforderungen

<sup>1</sup> Stufen der Sicherheitsüberprüfung gemäß Sicherheitsüberprüfungsgesetz

- ☐ Abweichend von Ziffer 8.1 EVB-IT Dienstleistungs-AGB ist der Auftragnehmer verpflichtet, für die Leistungen gemäß Nummer 3.1 lfd. Nr. 01 nur Personal einzusetzen, welches bereit ist, sich aufgrund des Verpflichtungsgesetzes verpflichten zu lassen.
- ☐ Abweichend von Ziffer 8.1 EVB-IT Dienstleistungs-AGB ist der Auftragnehmer berechtigt, für die Leistungen gemäß Nummer 3.1 lfd. Nr. \_\_\_\_\_ auch Personal einzusetzen, welches lediglich in folgender Sprache zu kommunizieren in der Lage ist: \_\_\_\_\_.
- ☐ Mindestanforderungen an das einzusetzende Personal des Auftragnehmers ergeben sich aus Anlage Nr. 02.

### 8 Mitwirkungsleistungen des Auftraggebers

- ☐ Folgende Mitwirkungsleistungen des Auftraggebers werden abweichend und zusätzlich zu Ziffer 14 EVB-IT Dienstleistungs-AGB vereinbart: \_\_\_\_\_.
- ☒ Die Mitwirkungsleistungen des Auftraggebers ergeben sich abweichend und zusätzlich zu Ziffer 14 EVB-IT Dienstleistungs-AGB aus Anlage Nr. 02 (Leistungsbeschreibung).

### 9 Abweichende Nutzungsrechte an den Leistungsergebnissen, Erfindungen

Für folgende Leistungsergebnisse werden von Ziffer 3.1 EVB-IT Dienstleistungs-AGB abweichende Nutzungsrechte vereinbart:

- ☐ Für alle Ergebnisse der Leistungen gemäß Nummer 3.1 lfd. Nr. \_\_\_\_\_ gilt Ziffer 3.1 EVB-IT Dienstleistungs-AGB mit der Maßgabe, dass statt des dort aufgeführten nicht ausschließlichen Nutzungsrechts ein ausschließliches Nutzungsrecht gewährt wird, vorbestehende Werke jedoch ausgenommen.
- ☐ Für folgende Ergebnisse der Leistungen gemäß Nummer 3.1 lfd. Nr. \_\_\_\_\_ gilt Ziffer 3.1 EVB-IT Dienstleistungs-AGB mit der Maßgabe, dass statt des dort aufgeführten nicht ausschließlichen Nutzungsrechts ein ausschließliches Nutzungsrecht gewährt wird, vorbestehende Werke jedoch ausgenommen: \_\_\_\_\_.
- ☐ Für alle Ergebnisse der Leistungen gemäß Nummer 3.1 lfd. Nr. \_\_\_\_\_ gilt Ziffer 3.1 EVB-IT Dienstleistungs-AGB mit der Maßgabe, dass eine gewerbliche Verbreitung uneingeschränkt möglich ist.



## Dienstvertrag (Langfassung)

- ☐ Für folgende Ergebnisse der Leistungen gemäß Nummer 3.1 lfd. Nr. \_\_\_\_\_ gilt Ziffer 3.1 EVB-IT Dienstleistungs-AGB mit der Maßgabe, dass eine gewerbliche Verbreitung uneingeschränkt möglich ist, \_\_\_\_\_.
- ☐ Für alle Ergebnisse der Leistungen gemäß Nummer 3.1 lfd. Nr. \_\_\_\_\_ gilt Ziffer 3.1 EVB-IT Dienstleistungs-AGB mit der Maßgabe, dass jegliche gewerbliche Verbreitung ausgeschlossen ist.
- ☐ Für folgende Ergebnisse der Leistungen gemäß Nummer 3.1 lfd. Nr. \_\_\_\_\_ gilt Ziffer 3.1 EVB-IT Dienstleistungs-AGB mit der Maßgabe, dass jegliche gewerbliche Verbreitung ausgeschlossen ist: \_\_\_\_\_.
- ☐ Für alle Ergebnisse der Leistungen (z.B. Dokumentationen) gemäß Nummer 3.1 lfd. Nr. \_\_\_\_\_ gilt abweichend von Ziffer 3.1 EVB-IT Dienstleistungs-AGB folgende von openCode\* freigegebene Lizenz: \_\_\_\_\_.
- ☐ **Bereitstellung als Open Source Software\***: Die Bereitstellung der Ergebnisse der Leistungen gemäß Nummer 3.1 lfd. Nr. \_\_\_\_\_ erfolgt als Open Source Software\* (ergänzend zur Rechteeinräumung gemäß Ziffer 3.1 EVB-IT Dienstleistungs-AGB und zu ggf. vorstehend vereinbarten Änderungen daran).  
Zusätzlich bzw. abweichend davon gilt folgendes. Die Bereitstellung der Software
  - ☐ muss wie vorstehend beschrieben, jedoch unter **von openCode\* freigegebenen Lizenzen** erfolgen.
  - ☐ muss wie vorstehend beschrieben, jedoch unter von openCode\* freigegebenen Lizenzen, **die keinen Copyleft\*-Effekt** haben, erfolgen (sog. permissive Lizenzen, z.B. MIT- oder Apachelizenz > Version 1.0).
  - ☐ muss wie vorstehend beschrieben, jedoch unter von openCode\* freigegebenen Lizenzen **mit Copyleft\*-Effekt** zur Verfügung gestellt werden (sog. reziproke Lizenzen, z.B. GNU GPL oder LGPL).
  - ☐ muss wie vorstehend beschrieben, jedoch unter der/den **folgenden Lizenz(en)** zur Verfügung gestellt werden, die den Anforderungen an **Open Source Software\*** entsprechen: \_\_\_\_\_.
  - ☐ Soweit die Ergebnisse der Leistungen als **Open Source Software\*** bereitgestellt werden müssen, wird vereinbart, dass diese ggf. gemeinsam mit folgender Software genutzt und verbreitet wird (siehe Ziffer 3.2 EVB-IT Dienstleistungs-AGB): \_\_\_\_\_.
- ☒ Von Ziffer 3.1 EVB-IT Dienstleistungs-AGB abweichende Nutzungsrechte sind in Anlage Nr. 02 (Leistungsbeschreibung) geregelt.
- ☐ Für Erfindungen, die anlässlich der Vertragserfüllung gemacht werden, gelten abweichend von Ziffer 4 EVB-IT Dienstleistungs-AGB die Regelungen in Anlage Nr. \_\_\_\_\_.
- ☐ Abweichend von Ziffer 3.4 EVB-IT Dienstleistungs-AGB darf der Auftragnehmer **vorbestehende Software bzw. Softwareteile** auch ohne Zustimmung des Auftraggebers in die Leistungsergebnisse integrieren, sofern daran Nutzungsrechte wie an den Leistungsergebnissen im Übrigen verschafft werden.

### 10 Quellcode\* und Software Bill of Materials (SBOM)

Im Falle der Erstellung oder Bearbeitung von Software:

- ☐ ist gemäß Ziffer 3.7 EVB-IT Dienstleistungs-AGB der jeweils aktuelle Stand der Software, einschließlich der Quellcodes\* auf folgendem vom Auftraggeber zur Verfügung gestellten Quellcoderepository zu speichern: \_\_\_\_\_.
- ☐ wird abweichend von Ziffer 3.7 EVB-IT Dienstleistungs-AGB der jeweils aktuelle Stand der Software, einschließlich der Quellcodes\* wie folgt gespeichert und dem Auftraggeber zur Verfügung gestellt: \_\_\_\_\_.
- ☐ wird abweichend von Ziffer 3.7 EVB-IT Dienstleistungs-AGB der jeweils aktuelle Stand der Software, einschließlich der Quellcodes\* nicht täglich sondern \_\_\_\_\_ (z.B. am Ende jeder Arbeitswoche) abgespeichert.
- ☐ erfolgt die Übergabe des Quellcodes\* auch am Ende jedes Leistungsmonats in elektronischer Form auf einem Datenträger.

Die Pflichten in Bezug auf die Übergabe des Quellcodes\* von Open Source Software\* bleiben von den vereinbarten Abweichungen nach dieser Nummer 10 unberührt.

- ☐ Der Auftragnehmer stellt dem Auftraggeber eine Software Bill of Materials (SBOM) gemäß BSI TR-03183-2 für den jeweils aktuellen Stand der Software
  - ☐ im Format SPDX
  - ☐ im Format CycloneDX



## Dienstvertrag (Langfassung)

zur Verfügung.

### 11 Abweichende Haftungsregelungen

- ☐ Abweichend von Ziffer 13.1 EVB-IT Dienstleistungs-AGB beträgt die Haftungsobergrenze bei leicht fahrlässigen Pflichtverletzungen
  - ☐ pro Schadensfall \_\_\_\_\_ Euro.
  - ☐ insgesamt für diesen Vertrag \_\_\_\_\_ Euro.
- ☐ Abweichend von Ziffer 13.1 EVB-IT Dienstleistungs-AGB gelten für die Haftung bei leicht fahrlässigen Pflichtverletzungen die Regelungen gemäß Anlage Nr. \_\_\_\_\_.
- ☐ Abweichend von Ziffer 13.3 EVB-IT Dienstleistungs-AGB haftet der Auftragnehmer auch für entgangenen Gewinn.

### 12 Vertragsstrafen

- ☐ Als vertragsstrafenrelevant im Sinne von Ziffer 10.3 EVB-IT Dienstleistungs-AGB gelten die in Nummer 3.1 lfd. Nr. \_\_\_\_\_ vereinbarten Leistungstermine.
- ☐ Abweichend von Ziffer 10.3 EVB-IT Dienstleistungs-AGB wird für Leistungen gemäß Nummer 3.1 lfd. Nr. \_\_\_\_\_ die Vertragsstrafenregelung gemäß Anlage Nr. \_\_\_\_\_ vereinbart.
- ☐ Für die Nichteinhaltung von Reaktionszeiten\* gilt die Vertragsstrafenregelung aus Ziffer 10.4 EVB-IT Dienstleistungs-AGB.
- ☐ Für die Nichteinhaltung von Reaktionszeiten\* gelten die Regelungen in Anlage Nr. \_\_\_\_\_.
- ☐ Für jeden Verstoß gegen Ziffer 1.5 oder Ziffer 1.6 der EVB-IT Dienstleistungs-AGB wird eine Vertragsstrafe in Höhe von \_\_\_\_\_ Euro vereinbart. Dies gilt nicht, wenn der Auftragnehmer den Verstoß nicht zu vertreten hat.
- ☐ Für jeden Verstoß des Auftragnehmers gegen die Regelung im ersten Aufzählungspunkt der Ziffer 8.3 EVB-IT Dienstleistungs-AGB wird eine Vertragsstrafe in Höhe von \_\_\_\_\_ Euro vereinbart. Dies gilt nicht, wenn der Auftragnehmer den Verstoß nicht zu vertreten hat.

### 13 Weitere Regelungen

#### 13.1 Datenschutz, Geheimhaltung und Sicherheit

Der Auftragnehmer verpflichtet sich für die Laufzeit des Vertrages

- ☐ bei der Erbringung der vertraglichen Leistungen die Regelungen zur IT-Sicherheit gemäß Anlage Nr. \_\_\_\_\_ zu beachten.
- ☐ der Geheimschutzbetreuung gemäß Anlage Nr. \_\_\_\_\_ zu unterstellen.
- ☐ die Regelungen des Auftraggebers zur Sicherheit am Einsatzort gemäß Anlage Nr. \_\_\_\_\_ zu beachten.
- ☐ folgende weitere Regelungen einzuhalten: \_\_\_\_\_.
- ☒ Ergänzend zu bzw. abweichend von Ziffer 19 EVB-IT Dienstleistungs-AGB ergeben sich Regelungen zur Geheimhaltung bzw. zur Sicherheit aus Anlage Nr. 03 (Datenschutz- und Vertraulichkeitsvereinbarung).
- ☒ Sofern im Rahmen der Auftragsausführung durch den Auftragnehmer personenbezogene Daten im Auftrag verarbeitet werden (Auftragsverarbeitung), treffen die Parteien eine schriftliche Vereinbarung gemäß Anlage 04 (Vereinbarung zur Auftragsverarbeitung), welche ausschließlich in den farbig markierten Bereichen entsprechend dem jeweiligen Anwendungszweck ergänzt wird.
- ☒ Die Parteien treffen sonstige Vereinbarungen zum Datenschutz gemäß Anlage Nr. 03 (Datenschutz- und Vertraulichkeitsvereinbarung).

#### 13.2 Haftpflichtversicherung

- ☐ Der Nachweis einer Haftpflichtversicherung gemäß Ziffer 18 EVB-IT Dienstleistungs-AGB wird vereinbart.



## Dienstvertrag (Langfassung)

### 13.3 Teleservice\*

- ☐ Soweit der Auftragnehmer zur Leistung durch Teleservice\* berechtigt ist, wird er diesen ausschließlich aufgrund der Teleservicevereinbarung gemäß Anlage Nr. \_\_\_\_\_ erbringen und darf dabei ausschließlich folgendes automatisiertes Verfahren einsetzen: \_\_\_\_\_ (Produktbezeichnung). Dieses Verfahren muss neben den Anforderungen aus Ziffer 1.5 EVB-IT Dienstleistungs-AGB auch den Anforderungen aus der Anlage Nr. \_\_\_\_\_ genügen.

### 13.4 Dokumentations- und Berichtspflichten

- ☐ Abweichend von Ziffer 6 EVB-IT Dienstleistungs-AGB dokumentiert der Auftragnehmer die Leistungen gemäß Nummer 3.1 lfd. Nr. \_\_\_\_\_ nicht in deutscher, sondern in \_\_\_\_\_ Sprache.
- ☒ Weitere Dokumentations- und Berichtspflichten des Auftragnehmers ergeben sich aus den Anlagen Nrn. 01 (Rahmenkonzept) und 02 (Leistungsbeschreibung).

### 13.5 Interessenkonflikt

- ☐ Regelungen zur Vermeidung eines Interessenskonfliktes ergeben sich aus Anlage Nr. \_\_\_\_\_.

### 14 Pflichten nach Vertragsende

- ☐ Ergänzend zu Ziffer 16 EVB-IT Dienstleistungs-AGB ergeben sich weitere Vereinbarungen zu den Pflichten des Auftragnehmers nach Vertragsende aus Anlage Nr. \_\_\_\_\_.

### 15 Sonstige Vereinbarungen

- ☒ Sonstige Vereinbarungen:

- ☒ Werbeverbot

Öffentliche Werbung, die auf einem Vertragsverhältnis mit dem Auftraggeber beruht, bedarf der ausdrücklichen schriftlichen Einwilligung (vorherige Zustimmung) des Auftraggebers. Eine erteilte Einwilligung kann vom Auftraggeber jederzeit ohne Angabe von Gründen zurückgenommen werden.

- ☒ Equal-Pay-Klausel

Der Auftragnehmer hat bei der Ausführung des öffentlichen Auftrags alle für ihn geltenden rechtlichen Verpflichtungen einzuhalten, insbesondere den Arbeitnehmerinnen und Arbeitnehmern wenigstens diejenigen Mindestbedingungen einschließlich des Mindestentgelts zu gewähren, die nach dem Mindestlohngesetz, einem nach dem Tarifvertragsgesetz mit den Wirkungen des Arbeitnehmerentsendegesetzes (AEntG) für allgemein verbindlich erklärten Tarifvertrag oder einer nach § 7, § 7a oder § 11 AEntG oder einer nach § 3a AÜG erlassenen Rechtsverordnung für die betreffende Leistung verbindlich vorgegeben werden, sowie gemäß § 7 Abs. 1 AGG und § 3 Abs. 1 EntgTranspG Frauen und Männern bei gleicher oder gleichwertiger Arbeit gleiches Entgelt zu bezahlen.

- ☐ Die sonstigen Vereinbarungen ergeben sich aus Anlage Nr. \_\_\_\_\_.

Unterschrift Auftraggeber

Unterschrift Auftragnehmer

Datum, Name

Datum, Name





## Rahmenkonzept App-Security-Check 2026

### INHALT

1	Hintergrund.....	2
2	Überblick.....	2
2.1	App-Prüfungen.....	2
2.2	Prozesse und Rollen.....	2
3	Umsetzung.....	3
3.1	LSI-Portal.....	3
3.2	Beteiligung externer Dienstleister.....	3
4	Glossar .....	4

## 1 Hintergrund

In vielen Bereichen der bayerischen Staatsverwaltung werden dienstliche Smartphones und andere mobile Endgeräte auf Android- oder iOS-Basis genutzt. Auf den Geräten werden verschiedene „Apps“ (Anwendungsprogramme) installiert, die in der Regel aus den App-Stores der Hersteller bezogen werden. In den einzelnen Behörden bestimmen jeweils Informationssicherheitsbeauftragte (ISBs) oder andere Entscheidungsträger, welche Apps zum Einsatz auf den Dienstgeräten freigegeben werden.

Das Landesamt für Sicherheit in der Informationstechnik (LSI) unterstützt Behörden im Freistaat Bayern mit dem Dienstleistungsangebot *App-Security-Check*. Dabei stellt das LSI sicherheitstechnische Bewertungen gängiger Apps zur Verfügung. Diese Bewertungen sollen den Entscheidungsträgern als Orientierungshilfe bei der Freigabe und Nutzung von Apps dienen.

Das LSI plant, dieses Angebot neu auszurichten, damit es durch Automatisierung künftig einfacher genutzt werden kann und vielfältigere Möglichkeiten bietet.

Dieses Dokument soll einen Überblick über das geplante Portfolio des LSI geben, welches den Zielgruppen des LSI zur Verfügung gestellt wird. Anforderungen an die erforderliche Leistung späterer Auftragnehmer ergeben sich aus den Vertragsunterlagen und insbesondere aus der jeweiligen Leistungsbeschreibung.

## 2 Überblick

### 2.1 App-Prüfungen

Apps, die potenziell auf Dienstgeräten genutzt werden, sind laufend auf sicherheitstechnische Schwachstellen und sonstige Risiken (insbesondere auch hinsichtlich Datensicherheit und Datenschutz) zu prüfen. Die Prüfergebnisse werden den LSI-Kunden zur Verfügung gestellt.

Für diese Prüfungen sollen grundsätzlich zwei verschiedene Verfahren verfügbar sein:

- **Schnellprüfungen** werden in großer Zahl automatisiert durchgeführt und liefern zeitnah Ergebnisse. Diese werden in einem **App-Katalog** festgehalten, der viele gängige Apps umfasst. Der App-Katalog wird laufend aktuell gehalten; Updates werden unmittelbar nach Erscheinen neu geprüft.
- **Expertenprüfungen** werden jeweils einzeln nach Bedarf beauftragt und von qualifizierten Experten durchgeführt. Dabei werden sowohl manuelle als auch automatisierte Methoden angewendet.

Eine einzelne Prüfung hat grundsätzlich nur eine bestimmte App-Version für ein einziges Betriebssystem zum Gegenstand. In vielen Fällen wird sowohl die Android- als auch die iOS-Version einer App zu prüfen sein; dafür werden dann jeweils zwei Prüfaufträge erteilt.

Die Prüfergebnisse sollen jeweils so aufbereitet werden, dass sie sowohl eine unmittelbar ablesbare Gesamtbewertung als auch weitere Einzelheiten dazu liefern. Die LSI-Kunden sollen sämtliche Prüfergebnisse einfach und unmittelbar selbst abrufen können.

### 2.2 Prozesse und Rollen

Der App-Security-Check richtet sich derzeit primär an die Ressort-ISBs der unmittelbaren Staatsverwaltung. Die Ressort-ISBs können aus ihrem jeweiligen Verantwortungsbereich weitere Nutzer benennen, die ebenfalls direkten Zugriff auf die Funktionen des App-Security-Checks erhalten sollen. Dies können zum Beispiel ISBs nachgeordneter Behörden oder sonstige IT-Verantwortliche sein. All diese Personen sind *LSI-Kunden* (siehe Glossar). Das LSI kann den Kundenkreis künftig auf Kommunen und andere Stellen im Rahmen seines gesetzlichen Auftrags ausweiten (Art. 42 Abs. 2, Art. 45 Abs. 2 Satz 2 BayDiG).

Die LSI-Kunden können auf den App-Katalog und auf sämtliche Prüfergebnisse zugreifen; bei Bedarf können sie selbst ausgewählte Apps zum Katalog hinzufügen. Expertenprüfungen können sie beim LSI anregen; eine Beauftragung von Expertentests erfolgt ausschließlich durch das LSI.

Mit der technischen Durchführung der App-Prüfungen werden externe Dienstleistungsunternehmen beauftragt (siehe Abschnitt 3.2). Das LSI wird insbesondere folgende Aufgaben wahrnehmen:

- Beratung der LSI-Kunden zum App-Security-Check
- Bewertung von Anfragen der LSI-Kunden für Expertenprüfungen
- Beauftragung von Expertenprüfungen beim Dienstleister
- Administration der Benutzerkonten (soweit es dafür keine andere Regelung gibt)
- Bereitstellung eigener Systemkomponenten für das LSI-Portal (siehe 3.1)
- Kommunikation mit den beauftragten Dienstleistern
- Qualitätssicherung der Prüfergebnisse

## 3 Umsetzung

### 3.1 LSI-Portal

Der *App-Security-Check* soll in das **LSI-Portal** integriert werden. Das LSI-Portal ist eine Webanwendung, die den LSI-Kunden mehrere Dienstleistungen des LSI auf einer gemeinsamen Plattform bereitstellen soll.

Das LSI-Portal stellt ein Basis-Framework bereit, in das sich verschiedene Frontend-Bausteine einbetten lassen. Außerdem bietet es grundlegende Funktionen, insbesondere zur Administration und Authentifizierung der Benutzer. Das LSI-Portal wird ganz oder überwiegend vom LSI selbst entwickelt.

Im LSI-Portal soll der *App-Security-Check* als ein Baustein implementiert werden, der den Nutzern folgende Funktionen bietet:

- Übersicht sämtlicher Apps – dies umfasst den gesamten App-Katalog sowie alle Apps, die Gegenstand von Expertenprüfungen sind oder waren
- Abruf aller vorhandenen Prüfergebnisse (aus Schnell- und Expertenprüfungen)
- Hinzufügen einer App zum App-Katalog für Schnellprüfungen
- Anfordern einer Expertenprüfung für eine App

Das LSI-Portal wird dabei im Hintergrund über einen Webservice (API) auf den App-Katalog zugreifen. Solange die erforderliche Funktionalität im LSI-Portal noch nicht vollständig bereitsteht, können die LSI-Kunden stattdessen direkt auf die Webanwendung des App-Katalogs zugreifen.

Zugriffe auf das LSI-Portal sind nur innerhalb des Bayerischen Behördennetzes möglich.

### 3.2 Beteiligung externer Dienstleister

Mit folgenden Leistungspaketen werden externe Dienstleistungsunternehmen beauftragt:

- Im Paket **App-Katalog** sind Apps in großer Zahl mit weitgehend automatisierten Verfahren zu prüfen. Vorrangiges Ziel ist hier, mit vertretbarem Aufwand viele Apps abzudecken, zeitnah Ergebnisse zu erhalten und dabei auch fortlaufend alle Versions-Updates zu verfolgen.

Der App-Katalog umfasst sowohl einen Grundbestand an marktgängigen Apps, die der jeweilige Dienstleister bereitstellt, als auch Apps, die Nutzer individuell hinzufügen können (Wahlbestand).

- Im Paket **Expertenprüfungen** sind Apps von qualifizierten Experten zu untersuchen. Diese Prüfungen werden einzeln beauftragt und beinhalten auch Methoden der manuellen Analyse. Hier sollen die Apps gründlich geprüft werden, um möglichst aussagekräftige Ergebnisse zu erhalten.

Zusätzlich soll das LSI im Rahmen der Expertenprüfungen auch die Möglichkeit haben, selbst entwickelte Apps des Freistaats Bayern prüfen zu lassen. Dabei sind die zu prüfenden App-Versionen oft noch nicht in einem App Store veröffentlicht. Diese Prüfungen werden vertraulich behandelt und sind nicht für alle **LSI-Kunden** sichtbar. Die Ergebnisse werden nur den Personen mitgeteilt, die unmittelbar für Entwicklung und Sicherheit der jeweiligen App verantwortlich sind.

Jedes Leistungspaket (App-Katalog und Expertenprüfungen) wird durch ein eigenständiges Vergabeverfahren ausgeschrieben. Die Leistungspakete können unabhängig voneinander an verschiedene Auftragnehmer vergeben werden.

Die jeweiligen Leistungsanforderungen ergeben sich aus den jeweils spezifischen Vergabe- und Vertragsunterlagen.

## 4 Glossar

App	Anwendungsprogramm für mobile Endgeräte
ISB	Informationssicherheitsbeauftragter
LSI	Landesamt für Sicherheit in der Informationstechnik
LSI-Kunden	Nutzer, die Leistungen des LSI in Anspruch nehmen. Dies sind insbesondere Ressort-ISBs der unmittelbaren Staatsverwaltung, ISBs nachgeordneter Behörden oder sonstige IT-Verantwortliche, künftig evtl. auch Kommunen und andere Stellen im Rahmen des gesetzlichen Auftrags des LSI.
Ressort	Oberste Landesbehörde, für die ein Ressort-ISB bestellt ist. Ressorts in diesem Sinne sind insbesondere Staatskanzlei, Staatsministerien und Bayerischer Oberster Rechnungshof.



## Leistungsbeschreibung App-Katalog zum App-Security-Check

### INHALT

1	Hintergrund .....	3
2	Leistungsgegenstand .....	3
2.1	Überblick.....	3
2.2	Katalogumfang .....	3
2.3	Prüfzyklus.....	4
2.4	Webanwendung.....	4
2.5	Webservice (API).....	5
2.6	Funktionen .....	5
2.7	Prüfverfahren.....	6
2.8	Prüfkriterien .....	6
2.8.1	Plattformsicherheit.....	6
2.8.2	Datensicherheit .....	7
2.8.3	Netzwerkkommunikation .....	7
2.8.4	Kommunikationsbeziehungen.....	7
2.8.5	Code .....	8
2.9	Prüfergebnisse .....	8
3	Rahmenbedingungen .....	9
3.1	Nutzungsvolumen.....	9
3.2	Anforderungen an den Auftragnehmer .....	9
3.3	Leistungszeitraum .....	10
3.4	Allgemeine technische Anforderungen .....	10
3.5	Anforderungen an Systemkomponenten.....	10

3.6	Projektkommunikation .....	11
3.7	Abrechnung .....	11
4	Glossar .....	11

## 1 Hintergrund

Das Landesamt für Sicherheit in der Informationstechnik (LSI) unterstützt Behörden in Bayern mit dem Dienstleistungsangebot *App-Security-Check*. Dabei stellt das LSI sicherheitstechnische Bewertungen gängiger Smartphone-Apps zur Verfügung. Diese Bewertungen sollen den Entscheidungsträgern als Orientierungshilfe bei der Freigabe und Nutzung von Apps für Dienstgeräte dienen.

Das LSI plant, dieses Angebot neu auszurichten. Einen Gesamtüberblick der geplanten künftigen Ausgestaltung gibt das separate Dokument „Rahmenkonzept App-Security-Check 2026“.

Ein App-Katalog soll künftig das Basisangebot des LSI darstellen. Dieser umfasst Sicherheitsbewertungen für viele gängige Apps. Die Apps werden mit weitgehend automatisierten Verfahren geprüft. Diese Prüfungen sollen möglichst schnell und effizient ablaufen und alle Versions-Updates jeweils zeitnah einbeziehen.

Das LSI beabsichtigt, ein Unternehmen zu beauftragen, das Apps in großer Zahl automatisiert prüfen und die Ergebnisse zur Verfügung stellen wird.

## 2 Leistungsgegenstand

### 2.1 Überblick

Der Auftragnehmer prüft Apps nach Kriterien, die sicherheitstechnische Bewertungen ermöglichen. Dazu nutzt er ein effizientes Verfahren, das weitgehend oder vollständig automatisiert abläuft. Die Prüfergebnisse sollen zeitnah vorliegen – in der Regel innerhalb weniger Tage.

Es wird ein App-Katalog geführt, der viele marktgängige Apps umfasst. Apps, die noch nicht im Katalog vorhanden sind, können von Nutzern zum Katalog hinzugefügt werden.

Apps aus diesem Katalog werden ohne manuelles Zutun regelmäßig neu überprüft – mindestens sobald eine neue Version einer App erscheint. Für alle Apps aus diesem Katalog lassen sich aktuelle und historische Prüfergebnisse und daraus resultierende Risikobewertungen jederzeit in Echtzeit abrufen.

Der Auftragnehmer stellt eine Webanwendung und einen Webservice zur Verfügung, über die der App-Katalog abgerufen und ergänzt werden kann, und über die sich Prüfergebnisse abrufen lassen. Auf die Webanwendung können Endbenutzer per Browser zugreifen; der Webservice dient als Schnittstelle zur Anbindung eigener Anwendungskomponenten des Auftraggebers (insbesondere des LSI-Portals).

### 2.2 Katalogumfang

Der App-Katalog umfasst

- einen *Grundbestand* von weit verbreiteten Apps, die der Auftragnehmer auswählt, und
- einen *Wahlbestand* von Apps, die Nutzer selbst auswählen können.

Der **Grundbestand** muss während des gesamten Leistungszeitraums mindestens 1.000 Apps umfassen, die der Auftragnehmer in nachvollziehbarer Weise systematisch auswählt. Hauptkriterium muss dabei die Verbreitung der Apps bei Smartphone-Nutzern in Deutschland sein. Apps, die nach ihrer Art nicht zum Einsatz auf Dienstgeräten in Frage kommen (z.B. Spiele), können unberücksichtigt bleiben; andernfalls werden diese nicht auf die Mindestanzahl angerechnet. Mit dem Angebot ist eine detaillierte Beschreibung einzureichen, aus der die Auswahlkriterien nachvollziehbar und vollständig hervorgehen.

Der Grundbestand soll die Betriebssysteme Android und iOS gleichermaßen abdecken. Wenn funktional weitgehend ähnliche Apps für beide Betriebssysteme erscheinen, sind beide in den Grundbestand aufzu-



nehmen, sofern dem keine besonderen Gründe entgegenstehen. Der Grundbestand muss mindestens 400 Android-Apps und mindestens 400 iOS-Apps enthalten.

Der Auftragnehmer hält den Grundbestand fortlaufend aktuell. Insbesondere wird er Apps unverzüglich in den Grundbestand aufnehmen, sobald sie am Markt erschienen sind und die vereinbarten Auswahlkriterien erfüllen. Sofern erforderlich, können Apps aus dem Grundbestand entfernt werden, die nicht mehr den Auswahlkriterien entsprechen. Die Mindestanzahlen von 1.000 Apps (gesamt), 400 Android-Apps und 400 iOS-Apps dürfen zu keinem Zeitpunkt unterschritten werden.

Zum **Wahlbestand** können Nutzer jederzeit weitere, selbst ausgewählte Apps hinzufügen.

Beim Hinzufügen einer App sollen Nutzer bestimmen können, dass die App nur einmal geprüft wird und danach automatisch wieder aus dem Wahlbestand entfernt wird.

Falls der Wahlbestand zahlenmäßig begrenzt ist, muss er insgesamt mindestens 1.000 Apps erlauben, und Apps müssen sich jederzeit wieder entfernen oder deaktivieren lassen, sodass sie nicht mehr auf das Limit angerechnet werden. Dabei muss jeder Nutzer Apps entfernen können, die er selbst hinzugefügt hat; Administratoren müssen beliebige Apps entfernen können.

Die Bezugskosten für kostenpflichtige Apps trägt der Auftragnehmer. Für Apps im Wahlbestand kann dabei eine jährliche Höchstgrenze vereinbart werden, die mindestens 2 % vom jeweiligen Gesamtauftragswert des Jahres betragen muss.

## 2.3 Prüfzyklus

Sobald eine App neu zum Katalog hinzugekommen ist, wird diese unverzüglich erstmals geprüft.

Außerdem prüft der Auftragnehmer regelmäßig alle Apps aus dem Katalog, ohne dass der Auftraggeber dazu aktiv werden muss. Zumindest wird die jeweils neueste Version einer App baldmöglichst geprüft, sobald eine neue Version erschienen ist.

Für Apps, die sich zu Beginn des Leistungszeitraums bereits im Katalog befinden, können die Nutzer von Anfang an zumindest die jeweils neuesten Prüfergebnisse abrufen. Später hinzukommende Prüfergebnisse werden den Nutzern jeweils unverzüglich zum Abruf bereitgestellt.

## 2.4 Webanwendung

Die Webanwendung ist per HTTPS über eine öffentlich zugängliche URL erreichbar. Sie bietet den Nutzern eine intuitive deutsch- oder englischsprachige Oberfläche. Nutzer können mit jedem gängigen Browser darauf zugreifen. Für alle wesentlichen Funktionen müssen mindestens die aktuellen Versionen der Browser Google Chrome, Microsoft Edge und Mozilla Firefox vollständig unterstützt werden.

Die Webanwendung unterscheidet mindestens die Benutzerrollen *Kunde* und *Administrator*:

Benutzer der Rolle **Kunde** können mindestens

- auf den App-Katalog zugreifen und alle Prüfergebnisse abrufen,
- selbst ausgewählte Apps zum Wahlbestand hinzufügen und
- von ihnen selbst hinzugefügte Apps wieder aus dem Wahlbestand entfernen.

Benutzer der Rolle *Kunde* haben keinen Zugriff auf administrative Funktionen, insbesondere nicht auf die Benutzerverwaltung.

Benutzer der Rolle **Administrator** können außerdem mindestens

- beliebige Apps aus dem Wahlbestand entfernen und
- Benutzerkonten unmittelbar in der Webanwendung verwalten. Auf diesem Weg muss zumindest die Verwaltung von Benutzerkonten der Rolle *Kunde* möglich sein.



Die Funktionen zum Entfernen von Apps sind optional, falls der Wahlbestand zahlenmäßig unbegrenzt ist.

Falls Benutzerkonten der Rolle *Administrator* nicht vom Auftraggeber selbst verwaltet werden können, muss der Auftragnehmer dafür eine andere kostenfreie Möglichkeit bereitstellen; alle Änderungen sind spätestens innerhalb von 24 Stunden durchzuführen.

Alle Nutzer authentifizieren sich gegenüber der Webanwendung mindestens mit Benutzernamen und Passwort. Die Webanwendung muss außerdem für alle Benutzerkonten die Möglichkeit bieten, den Zugang durch Multi-Faktor-Authentifizierung (MFA) abzusichern; für Administratorkonten soll MFA verpflichtend sein.

Die Webanwendung soll eine Möglichkeit zum Abruf von Zugriffsstatistiken bieten.

Die Webanwendung muss barrierefrei ausgestaltet und zugänglich sein und sich dabei an der Norm EN 301 549 orientieren. Insbesondere sind folgende Kriterien zu berücksichtigen:

- Zugänglichkeit für assistive Technologien, insbesondere Braillezeile und Sprachausgabe
- Zugriffsmöglichkeit mit aktuellen Versionen der Screenreader JAWS und SuperNova (siehe Glossar)

Die Regeln und Anforderungen der BayDiV (siehe Glossar) zur Barrierefreiheit sind zu beachten und umzusetzen. Die Realisierung der Barrierefreiheit ist mit dem jeweiligen Angebot detailliert darzustellen.

Für den Nachweis der Einhaltung der Anforderungen zur Barrierefreiheit ist der Anforderungskatalog Barrierefreiheit gemäß Anlage 06d zum EVB-IT Vertrag vollständig auszufüllen. Für alle Punkte, die mit "Nein" ausgefüllt werden, muss ein Fahrplan vorgelegt werden, wann und durch welche Schritte diese erfüllt werden, um somit einen Zeithorizont für eine vollständige, gesetzeskonforme Barrierefreiheit darzustellen. Die Erfüllung aller Punkte wird dabei in maximal 12 Monaten nach Beginn des Leistungszeitraums geplant.

## 2.5 Webservice (API)

Der Webservice ist per HTTPS über eine öffentlich zugängliche URL erreichbar und wird durch geeignete Maßnahmen nach dem Stand der Technik gegen unbefugte Zugriffe geschützt. Die verwendeten Authentifizierungsdaten (z.B. API-Schlüssel, Zertifikate) müssen sich jederzeit austauschen lassen, sobald es der Auftraggeber oder der Auftragnehmer für erforderlich hält.

Der Auftragnehmer stellt eine vollständige Dokumentation zur Verfügung, die alle Endpunkte und Parameter umfasst. Dazu gehört auch eine Beschreibung des strukturierten Formats für Prüfergebnisse (siehe Abschnitt 2.9). Der Auftraggeber muss anhand dieser Dokumentation ohne Weiteres in der Lage sein, zumindest den wesentlichen Funktionsumfang (siehe Abschnitt 2.6) zu nutzen. Die Dokumentation wird dem Auftraggeber so früh wie möglich bereitgestellt, spätestens zu Beginn des Leistungszeitraums (bzw. bei späterer Fertigstellung des Webservices nach Abschnitt 3.3).

## 2.6 Funktionen

Sowohl die Webanwendung als auch der Webservice bieten mindestens folgende Funktionen:

- Abruf einer Liste aller Apps des App-Katalogs
- Abruf einer Liste aller Apps, die einem vom Nutzer angegebenen Suchbegriff entsprechen
- Abruf aller vorhandenen Prüfergebnisse für einzelne, durch den Nutzer frei auswählbare Apps aus dem Katalog
- Hinzufügen einer neuen App zum Wahlbestand des Katalogs
- Entfernen einer App aus dem Wahlbestand des Katalogs (optional, falls der Wahlbestand zahlenmäßig unbegrenzt ist)

In der Webanwendung werden abgerufene App-Listen in Tabellenform angezeigt. Dabei müssen für jede App mindestens die Bezeichnung und das Betriebssystem ersichtlich sein; die Listen müssen mindestens nach der App-Bezeichnung sortierbar sein. Aus der Listenansicht können die Nutzer weitere Details und Prüfergebnisse einzelner Apps unmittelbar aufrufen.

Die Webanwendung bietet außerdem folgende Funktionen:

- Benutzerverwaltung mit Neuanlage, Bearbeiten, Löschen, Zurücksetzen von Authentifizierungsdaten (Passwort, MFA-Schlüssel)

Benutzerkonten, die eine gewisse Zeit (z.B. 3 Monate) nicht genutzt worden sind, sollen automatisch deaktiviert werden. Alternativ kann die Benutzerverwaltung eine Möglichkeit bieten, solche Benutzerkonten abzufragen.

## 2.7 Prüfverfahren

Der Auftragnehmer prüft Apps mit einem weitgehend oder vollständig automatisierten Verfahren. Der gesamte Prüfprozess ist dabei auf hohe Effizienz ausgerichtet, um sowohl ein hohes Volumen an Prüfungen zu ermöglichen als auch die Prüfergebnisse zeitnah zu liefern.

Jede App wird sowohl statischen als auch dynamischen Analysen unterzogen. Die Prüfschritte werden systematisch abgearbeitet und unter Anwendung nachvollziehbarer Kriterien ausgewertet. Diese sollen möglichst umfassend alle relevanten Sicherheitsrisiken berücksichtigen, die sich nach dem Stand der Technik mit automatisierten Methoden ermitteln lassen.

Mit dem Angebot ist eine detaillierte, nachvollziehbare Beschreibung über das angebotene Prüfverfahren einzureichen. In dieser Beschreibung ist auch auf die im folgenden Kapitel näher beschriebenen Prüfkriterien und deren Berücksichtigung einzugehen.

## 2.8 Prüfkriterien

Im Folgenden werden konkrete Prüfpunkte benannt, die das Prüfverfahren möglichst weitgehend abdecken soll. Dabei sind Mindestabdeckungen zu erfüllen, die sich im Einzelnen aus den Kriterien in der Leistungsmatrix ergeben.

Dabei sind teilweise Referenzen auf den OWASP Testing Guide angegeben (z.B. „MASTG-TEST-0052“). Diese beziehen sich auf den Versionsstand des OWASP Testing Guide vom Oktober 2025 und dienen nur als weiterführende Hinweise auf den Inhalt der jeweiligen Prüfpunkte. Eine Abdeckung der genannten OWASP-MAS-Tests wird nur soweit gefordert, wie sich die Testinhalte auf den jeweils genannten Prüfpunkt beziehen und wie es im Rahmen automatisierter Testverfahren möglich ist.

### 2.8.1 Plattformsicherheit

Es muss festgestellt werden, welche Versionen des jeweiligen Betriebssystems die App zulässt (Android: „minSdkVersion“ bzw. „targetSdkVersion“, iOS: „IPHONE\_DEPLOYMENT\_TARGET“).

Es muss ermittelt werden, welche Berechtigungen die App anfordert (MASTG-TEST-0069, MASTG-TEST-0254). Unter Berücksichtigung des Einsatzzwecks der App soll geprüft werden, ob die angeforderten Berechtigungen erforderlich sind. Zusätzlich muss geprüft werden, ob die App in sensible Funktionen der Plattform eingreifen kann, z.B. als „Custom Keyboard“, durch App Extensions (MASTG-TEST-0072) oder per „Share“-Funktion.

Die App ist auf folgende Schwachstellen zu prüfen:

- (a) Fest kodierte Passwörter oder kryptografische Schlüssel (MASTG-TEST-0212, -0213, -0214)
- (b) Unsichere Verwendung kryptografischer Funktionen, z.B. veraltete Algorithmen oder unzureichende Schlüssellängen (MASTG-TEST-0014, -0210, -0211, -0221)

Außerdem soll die App auf folgende Funktionselemente geprüft werden:

- (c) Deep Links und eigene URL-Schemas (MASTG-TEST-0028, -0075)
- (d) Rooting- oder Jailbreak-Erkennung (MASTG-TEST-0045, -0240)
- (e) Beschränkung von Screenshots (MASTG-TEST-0292, -0293, -0294)

- (f) Verwendung von Mechanismen zur sicheren Speicherung von Daten (z.B. Android Keystore, Android EncryptedSharedPreferences oder iOS Keychain), ggf. Prüfung auf Schwächen der Implementierung
- (g) Biometrische Authentifizierung (MASTG-TEST-0018, -0266 bis -0271)

Für WebViews sollen folgende Punkte geprüft werden:

- (h) Ausführung von JavaScript-Code (MASTG-TEST-0076)
- (i) Safe Browsing (MASTG-TEST-0027)
- (j) Content Security Policy (CSP)
- (k) Zugriff auf lokale Dateien/Ressourcen (MASTG-TEST-0252, -0253)
- (l) Zugriff auf native Funktionen über JavaScript Bridges (MASTG-TEST-0078)
- (m) Behandlung von TLS-Fehlern (MASTG-TEST-0284)

### 2.8.2 Datensicherheit

Es ist zu prüfen, ob (potenziell sensible) Benutzerdaten unsicher gespeichert oder verarbeitet werden. Dabei sollen insbesondere folgende Stellen betrachtet werden:

- (a) Lokales Dateisystem allgemein (MASTG-TEST-0052)
- (b) App Cache
- (c) Datenbanken
- (d) Shared Preferences (MASTG-KNOW-0036)
- (e) UserDefaults (MASTG-KNOW-0093)
- (f) Tastatur-Cache (MASTG-TEST-0055)
- (g) Backups (MASTG-TEST-0058, -0215, -0216, -0262, -0290)
- (h) Logs (MASTG-TEST-0053)
- (i) Arbeitsspeicher (MASTG-TEST-0011, -0060)
- (j) IPC-Mechanismen (z.B. Android Content Provider, MASTG-TEST-0007, -0029, -0056)
- (k) Zwischenablage

### 2.8.3 Netzwerkkommunikation

In der Konfiguration und im Code der App sind Hinweise auf unsichere Kommunikation zu suchen. Dazu zählen z.B.:

- (a) Unverschlüsselte Übermittlung von Benutzerdaten
- (b) Verwendung von HTTP- statt HTTPS-URLs
- (c) Konfigurierte Ausnahmen in der iOS App Transport Security (MASTG-KNOW-0071)
- (d) Zulassen unverschlüsselter Verbindungen in der Android Network Security Configuration (MASTG-KNOW-0014)
- (e) Eigene (evtl. unsichere) SSL-Trust-Manager-Implementierung (Android, MASTG-TEST-0282)

Generell ist zu prüfen, ob TLS-Versionen und sonstige Parameter nach dem Stand der Technik genutzt werden und ob Zertifikate der Gegenstellen korrekt geprüft werden, ggf. durch Zertifikats-Pinning.

Es soll geprüft werden, ob URLs dynamisch mit Daten externen Ursprungs gebildet werden, und ob diese Daten dabei sicher verwendet (insbesondere korrekt maskiert) werden.

### 2.8.4 Kommunikationsbeziehungen

Durch statische und dynamische Analyse muss ermittelt werden, mit welchen Gegenstellen die App kommuniziert. Dabei sind URLs und IP-Adressen zu bestimmen. Soweit bekannt, sind Kategorien anzugeben (z.B. Werbung, Telemetrie). Zumindest ist auf problematische Ziele zu prüfen (z.B. durch Abgleich mit Listen bekannter Malware-Domains). Zu jeder IP-Adresse ist der Standort zu bestimmen; die Vertrauenswürdigkeit soll jeweils dementsprechend (nach Land oder Region) bewertet werden.

### 2.8.5 Code

Es ist zu ermitteln, auf welchen Frameworks die App basiert und welche Bibliotheken sie referenziert. Für jede Komponente ist zu prüfen, ob sie veraltet ist oder bekannte Schwachstellen hat (möglichst mit Verweis auf CVEs). Komponenten, die generell unerwünscht sind (z.B. Spyware, Adware, Tracker), sind entsprechend zu kennzeichnen.

Die App ist daraufhin zu überprüfen, ob Debugging zulässig ist (MASTG-TEST-0226, -0227, -0261) und ob sie Debugging-Funktionen enthält.

Außerdem soll der Code generell auf die Verwendung potenziell gefährlicher Muster gescannt werden (z.B. auf veraltete Methoden der Speicherverwaltung, Kryptografie usw.).

## 2.9 Prüfergebnisse

Webanwendung und Webservice stellen die Ergebnisse einer Prüfung grundsätzlich im HTML-Format in einer Weise bereit, die bei Darstellung in einem Browser für Nutzer unmittelbar verständlich ist. Über den Webservice muss außerdem der wesentliche Informationsgehalt eines jeden Prüfergebnisses (mindestens die Zusammenfassung sowie Details aller Findings) auch in einem strukturierten Format bereitgestellt werden, das sich zur automatisierten Auswertung eignet und auf JSON, XML oder ähnlichen Standards basiert. Zusätzlich soll sich der wesentliche Inhalt auch als PDF-Dokument abrufen lassen.

Das Prüfergebnis muss eine Zusammenfassung enthalten, die mindestens folgende Informationen umfasst:

- Bezeichnung der App
- Anbieter
- App-ID (z.B. com.example.app) oder alternativ App-Store-URL
- Versionsnummer (z.B. 1.2.0)
- Übersicht der Findings, möglichst sortiert nach Risikobewertung
- Gesamtbewertung der App

Aus der Gesamtbewertung muss unmittelbar auf einen Blick ablesbar sein, ob aufgrund des Prüfergebnisses vom Einsatz der App abgeraten wird. Die Gesamtbewertung ist mit nachvollziehbaren Regeln aus den Ergebnissen der einzelnen Prüfpunkte abzuleiten. Der Auftraggeber muss bei Bedarf in der Lage sein, diese Regeln individuell anzupassen.

Darüber hinaus sind die folgenden weitergehenden Details zu liefern:

- Allgemeine Angaben zur Technologie, z.B. Framework, Programmiersprache
- Unterstützte Android- oder iOS-Versionen
- Schwachstellen und sonstige Findings mit Detailbeschreibung und Bewertung
- URLs und IP-Adressen von potenziellen Netzwerk-Gegenstellen, jeweils mit Kategorisierung, Geolokalisierung und Vertrauenseinschätzung
- Genutzte SDKs und Bibliotheken, jeweils mit verwendeter Version und aktueller Version sowie ggf. bekannten Schwachstellen, möglichst mit CVE-Angabe

Die Prüfergebnisse (Zusammenfassung und Details) werden in deutscher oder englischer Sprache geliefert.

Der Auftraggeber erlangt dauerhaft alle Nutzungsrechte an den Prüfergebnissen. Insbesondere darf er den Inhalt auf eigenen Systemen verarbeiten und unbeschränkt im gesamten Bereich der bayerischen Staatsverwaltung und an sonstige an das Behördennetz angeschlossene Stellen weitergeben (Art. 42 Abs. 2, Art. 45 Abs. 2 Satz 2 BayDiG). Der zahlenmäßige Umfang des Nutzerkreises ergibt sich aus Abschnitt 3.1.

### 3 Rahmenbedingungen

#### 3.1 Nutzungsvolumen

Hinsichtlich der nachfolgend dargestellten Zahlen weist der Auftraggeber ausdrücklich darauf hin, dass es sich trotz größtmöglicher Sorgfalt um geschätzte Zahlen handelt. Der Auftragnehmer muss seine Leistungen so anbieten, dass sie auch bei ggf. eintretenden Überschreitungen dieser Zahlen ohne Einschränkungen vollständig erbracht werden.

Der Auftraggeber erwartet im Leistungszeitraum folgende Nutzerzahlen (Grundvolumen):

	Jahr 1	Jahr 2	Jahr 3	Jahr 4	Jahr 5
Benutzer der Rolle <i>Administrator</i>	5	5	5	5	5
Benutzer der Rolle <i>Kunde</i>	100	120	130	140	150
Partizipierende Endgeräte	80.000	84.000	88.000	92.000	96.000

Falls der Auftragnehmer zum angebotenen Pauschalpreis eine oder mehrere dieser Nutzungsgrößen begrenzt, muss er für jede begrenzte Größe eine Zusatzoption vorsehen, um gegen Aufpreis auch eine höhere Nutzung abzudecken, und zwar mindestens in folgendem Umfang:

##### **Nutzungsoption 1 – Benutzer der Rolle *Administrator***

	Jahr 1	Jahr 2	Jahr 3	Jahr 4	Jahr 5
Zusatzvolumen der Option	10	10	10	10	10
rechnerisches Gesamtvolumen	15	15	15	15	15

##### **Nutzungsoption 2 – Benutzer der Rolle *Kunde***

	Jahr 1	Jahr 2	Jahr 3	Jahr 4	Jahr 5
Zusatzvolumen der Option	400	500	520	540	560
rechnerisches Gesamtvolumen	500	620	650	680	710

##### **Nutzungsoption 3 – Partizipierende Endgeräte**

	Jahr 1	Jahr 2	Jahr 3	Jahr 4	Jahr 5
Zusatzvolumen der Option	240.000	252.000	264.000	278.000	292.000
rechnerisches Gesamtvolumen	320.000	336.000	352.000	370.000	388.000

Der jeweils für eine Option vereinbarte Aufpreis wird anteilig entsprechend dem Grad der Inanspruchnahme des jeweiligen Zusatzvolumens in einem Jahr berechnet. Der volle Aufpreis einer Option wird demgemäß erst fällig, wenn das Zusatzvolumen vollständig ausgeschöpft wird.

Bei weiteren Überschreitungen einer Nutzerzahl über das volle Zusatzvolumen einer Option hinaus erhöht sich der Aufpreis entsprechend im Verhältnis der Überschreitung des Zusatzvolumens.

#### 3.2 Anforderungen an den Auftragnehmer

Der Auftragnehmer muss über mehrjährige Erfahrung in der automatisierten sicherheitstechnischen Prüfung von Android- und iOS-Apps verfügen. Er muss mindestens seit dem Jahr 2023 auf diesem Gebiet im Markt

tätig sein. Er muss technisch, wirtschaftlich und personell in der Lage sein, während der gesamten Vertragslaufzeit die vereinbarten Leistungen in vollem Umfang zu erfüllen. Weitere Eignungskriterien ergeben sich aus der Eignungsmatrix.

### 3.3 Leistungszeitraum

Der Leistungszeitraum beginnt mit dem Anfang des übernächsten Kalendermonats nach Zuschlagserteilung, jedoch nicht vor dem 1. September 2026. Auftraggeber und Auftragnehmer können einvernehmlich einen bis zu drei Monate späteren Beginn vereinbaren, z.B. wenn noch Zeit für erhebliche Vorbereitungen benötigt wird.

Der Auftragnehmer wird die vereinbarten Leistungen ab dem Beginn des Leistungszeitraums in vollem Umfang erbringen. Abweichend davon kann der Webservice (siehe Abschnitt 2.5) bis zu zwei Monate später bereitgestellt werden. Für jeden Monat, in dem der Webservice noch nicht voll zur Verfügung steht oder die Dokumentation dazu noch nicht vollständig vorliegt, mindert sich der monatliche Pauschalpreis um 10 %.

Der Leistungszeitraum umfasst zunächst 24 Monate (Grundvertragslaufzeit). Er verlängert sich bis zu dreimal um jeweils 12 Monate, falls der Auftraggeber nicht mindestens 3 Monate vor dem jeweiligen Verlängerungszeitpunkt ordentlich in Textform kündigt. Der Vertrag endet spätestens nach insgesamt 60 Monaten, ohne dass es einer Kündigung bedarf. Weitere Regelungen zur Kündigung (insbesondere nach Abschnitt 15 der EVB-IT Dienstleistungs-AGB) bleiben unberührt.

### 3.4 Allgemeine technische Anforderungen

Sowohl die Prüfverfahren als auch die bereitgestellten oder verwendeten Systemkomponenten sind stets auf dem aktuellen Stand der Technik zu halten und dazu auch fortlaufend weiterzuentwickeln.

### 3.5 Anforderungen an Systemkomponenten

Der Auftragnehmer gewährleistet, dass die Webanwendung und der Webservice an Arbeitstagen (siehe Glossar) von 6 bis 20 Uhr im Jahresmittel mindestens zu 96 % vollständig verfügbar sind. Er soll über ungeplante Störungen auf einem gesonderten Weg informieren (z.B. auf einer Statusseite). Geplante Einschränkungen sind rechtzeitig vorher anzukündigen und sollen möglichst außerhalb dieser Hauptnutzungszeiten erfolgen. Das Gesamtsystem ist kontinuierlich zu überwachen, um Störungen frühzeitig zu erkennen und schnell beheben zu können.

Die Webanwendung und der Webservice sollen bei durchschnittlicher Nutzung innerhalb von höchstens zwei Sekunden auf Nutzeranfragen reagieren. Auch bei hoher Auslastung muss eine Antwortzeit von höchstens sechs Sekunden eingehalten werden. Ausnahmen sind nur für außerordentliche, besonders aufwändige Aktionen zulässig (z.B. komplexe Suchanfragen, umfangreiche Downloads).

Sämtliche Komponenten sind nach den anerkannten aktuellen Regeln der IT-Sicherheit abgesichert zu betreiben. Der Auftragnehmer erklärt sich bereit, mindestens die Webanwendung und den Webservice durch einen Penetrationstest nach Vorgaben des LSI überprüfen zu lassen und dafür die Erlaubnis als PtA nach LSI-Vorlage zu erteilen (siehe Anlage 06e zum EVB-IT Vertrag). Den Penetrationstest wird das LSI oder ein vom LSI beauftragter Dienstleister durchführen. Der Auftragnehmer wird für die Behebung identifizierter Schwachstellen sorgen; dabei ist ein angemessener Zeitrahmen einzuhalten, der sich jeweils nach dem Schweregrad der einzelnen Schwachstellen richtet. Nach einer angemessenen Zeit (mindestens alle zwei Jahre) oder unmittelbar nach Behebung der Schwachstellen darf der Auftraggeber einen erneuten Penetrationstest veranlassen.

Der Auftragnehmer hat ein Betriebs- und Sicherheitskonzept zu erstellen und mit dem Auftraggeber abzustimmen. Er muss insbesondere Backup-Strategien sowie Notfall- und Wiederherstellungspläne haben, um nach einem Ausfall den Betrieb schnell wieder aufnehmen zu können.



Alle Systemkomponenten, die wesentlichen Anteil an der Leistungserbringung haben, müssen sich innerhalb der Europäischen Union befinden. Der Auftragnehmer stellt sicher, dass alle Daten, die einen konkreten Bezug zum Auftraggeber haben (insbesondere alle personenbezogenen Daten sowie der Inhalt des Wahlbestands), ausschließlich innerhalb der Europäischen Union verarbeitet werden.

### 3.6 Projektkommunikation

Der Auftragnehmer stellt geeignete Ansprechpartner bereit, an die sich der Auftraggeber bei auftreten Fragen jederzeit wenden kann. Dazu nennt der Auftragnehmer mindestens eine E-Mail-Adresse und eine Telefonnummer, über die er eine unmittelbare Kontaktaufnahme zumindest an Arbeitstagen (siehe Glossar) in der Zeit von 9 bis 17 Uhr ermöglicht. Die Reaktionszeit für Antworten und Rückrufe darf einen Arbeitstag nicht überschreiten. Eine gesonderte Vergütung erhält der Auftragnehmer dafür nicht.

Es finden regelmäßige Arbeitsbesprechungen zwischen den Projektverantwortlichen von Auftraggeber und Auftragnehmer statt. Dabei ist folgender Rhythmus vorgesehen:

- Spätestens drei Wochen nach Zuschlagserteilung werden in einem Kick-Off-Termin erste Einzelheiten zum Projektablauf und zu fachlichen Fragen abgestimmt.
- In den folgenden drei Monaten finden zwei weitere Besprechungen statt.
- Danach sind Besprechungen je nach Bedarf mindestens einmal pro Quartal möglich.

Dem Auftraggeber steht es jeweils frei, ob er die einzelnen Besprechungstermine in Anspruch nimmt. Die konkreten Termine werden einvernehmlich geplant; der Auftraggeber wird dazu jeweils mindestens drei Terminvorschläge vorgeben. Die Besprechungen werden in der Regel über ein Videokonferenzsystem des Auftraggebers durchgeführt. Abweichungen können im Einzelfall nach Bedarf vereinbart werden.

Auftraggeber und Auftragnehmer kommunizieren in deutscher Sprache. In begründeten Ausnahmefällen ist auch Kommunikation in englischer Sprache möglich.

### 3.7 Abrechnung

Der Auftraggeber soll quartalsweise oder monatliche Sammelrechnungen erstellen, die alle fortlaufend bereitgestellten Leistungen des jeweiligen Abrechnungszeitraums umfassen. Einmalige Leistungen werden jeweils nach Abschluss abgerechnet.

Anforderungen zur Rechnungsstellung ergeben sich aus dem Vertrag.

## 4 Glossar

Arbeitstag	Als Arbeitstage gelten die Wochentage von Montag bis Freitag, mit Ausnahme der gesetzlichen Feiertage am Hauptsitz des LSI (Nürnberg) sowie 24. und 31. Dezember.
BayDiV	Verordnung über die Digitalisierung im Freistaat Bayern (Bayerische Digitalverordnung)
CVE	<i>Common Vulnerabilities and Exposures</i> , ein System zur standardisierten Identifikation und Benennung von öffentlich bekannten Schwachstellen
JAWS	<i>Job Access With Speech</i> , eine Screenreader-Software von Freedom Scientific bzw. Vispero
MASTG	<i>Mobile Application Security Testing Guide</i> , ein OWASP-Leitfaden zur Prüfung der Sicherheit von Mobilanwendungen
MFA	Multi-Faktor-Authentifizierung
OWASP	Open Worldwide Application Security Project
PtA	Permission to Attack, Erlaubnis zur Durchführung von Penetrationstests

SuperNova      Screenreader-Software von Dolphin Computer Access Ltd.





## Datenschutz- und Vertraulichkeitsvereinbarung

zwischen

dem **Freistaat Bayern**,  
vertreten durch das Landesamt für Sicherheit in der Informationstechnik,  
Keßlerstraße 1,  
90489 Nürnberg

- im Folgenden „**Auftraggeber**“ genannt -

und

>> wird zur Zuschlagserteilung ergänzt <<

- im Folgenden „**Auftragnehmer**“ genannt -

wird folgende Vereinbarung geschlossen:

1. Der Auftragnehmer sorgt dafür, dass alle Personen, die von ihm mit der Bearbeitung oder Erfüllung des Vertrages betraut sind, die gesetzlichen Bestimmungen über den Datenschutz beachten. Die nach Datenschutzrecht erforderliche Verpflichtung auf das Datengeheimnis ist spätestens vor der erstmaligen Aufnahme der Tätigkeit vorzunehmen und dem Auftraggeber auf Verlangen nachzuweisen.
2. Der Auftragnehmer verarbeitet Daten nur soweit er hierzu beauftragt wurde und nur auf ausdrückliche Weisung des Auftraggebers.
3. Der Auftragnehmer darf sich weder unbefugten Zugang zu Informationen des Auftraggebers verschaffen noch sich diese unbefugt aneignen oder kopieren. Darüber hinaus wird der Auftragnehmer alle zumutbaren Vorkehrungen treffen, um in seinem Wirkungskreis einen unbefugten Zugriff Dritter auf sensible Daten des Auftraggebers zu verhindern. Auf Verlangen des Auftraggebers hat der Auftragnehmer die entsprechenden Maßnahmen nachzuweisen.

4. Soweit der Auftragnehmer Einblick in die Betriebsabläufe des Auftraggebers bzw. Zugang zu nicht allgemein zugänglichem Know-how oder sonstigen schützenswerten Daten und Informationen des Auftraggebers erhält, ist der Auftragnehmer zur Verschwiegenheit hierüber verpflichtet. Diese Verpflichtung besteht auch über das Vertragsverhältnis fort. Der Auftragnehmer hat die von ihm beim Auftraggeber eingesetzten Mitarbeiter entsprechend der in der Anlage beigefügten Verschwiegenheitserklärung zu verpflichten. Auf Verlangen ist dem Auftraggeber eine Abschrift der unterschriebenen Verschwiegenheitserklärung zu überlassen.
5. Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten vertraulichen Informationen, Geschäfts- und Betriebsgeheimnisse vertraulich zu behandeln, insbesondere nicht an Dritte weiterzugeben oder anders als zu vertraglichen Zwecken zu verwenden. Vertrauliche Informationen sind Informationen, die ein verständiger Dritter als schützenswert ansehen würde oder die als vertraulich gekennzeichnet sind; dies können auch solche Informationen sein, die während einer mündlichen Präsentation oder Diskussion bekannt werden. Die Verpflichtung zur Vertraulichkeit gilt nicht für Informationen, die den Parteien bereits rechtmäßig bekannt sind oder außerhalb des Vertrages ohne Verstoß gegen eine Vertraulichkeitsverpflichtung bekannt werden.
6. Der Auftragnehmer ist berechtigt, vertrauliche Informationen an solche Unterauftragnehmer weiterzugeben, deren Einsatz der Auftraggeber ausdrücklich zugestimmt hat, wenn und soweit diese vertraulichen Informationen für die Erbringung der jeweiligen Leistungen durch den Unterauftragnehmer erforderlich sind („need-to-know“-Prinzip). Dies gilt nur, wenn sich der Unterauftragnehmer zuvor dem Auftragnehmer gegenüber mindestens in gleichem Umfang zur Vertraulichkeit verpflichtet hat, wie der Auftragnehmer gegenüber dem Auftraggeber. Dabei muss die Weitergabe der vertraulichen Informationen durch den Unterauftragnehmer ausgeschlossen sein; soweit nicht der Auftraggeber jeweils zuvor einer Weitergabe ausdrücklich zugestimmt hat.
7. Werden dem Auftragnehmer Speichermedien des Auftraggebers für die Erfüllung seiner Verpflichtung übergeben, so sind diese nach Erfüllung unverzüglich an den Auftraggeber zurückzugeben. Alle Daten des Auftraggebers in Speichermedien des Auftragnehmers sind unverzüglich nach Erfüllung sach- und fachgerecht sowie datenschutzkonform und nach dem Stand der Technik sicher zu löschen. Die Löschung ist durch den Auftragnehmer zu dokumentieren und auf Verlangen des Auftraggebers durch einen Löschbericht nachzuweisen.

---

Ort, Datum

---

Ort, Datum

---

Unterschrift(en) Auftragnehmer

---

Unterschrift(en) Auftraggeber

# Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag nach Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO)

zwischen

dem **Freistaat Bayern**,  
vertreten durch das Landesamt für Sicherheit in der Informationstechnik,  
Keßlerstraße 1,  
90489 Nürnberg

- Verantwortlicher (nachfolgend „**Auftraggeber**“ genannt) -

und

>> wird zur Zuschlagserteilung ergänzt <<

- Auftragsverarbeiter (nachfolgend „**Auftragnehmer**“ genannt) -

## Präambel

Diese Vereinbarung regelt die Verpflichtungen der Vertragsparteien nach Art. 28 Abs. 3 DSGVO und ergänzt insoweit den Vertrag vom ..... (**Datum**) (im Folgenden „Auftrag“ genannt). Sie findet Anwendung auf alle Verarbeitungen personenbezogener Daten, die mit dem Auftrag in Zusammenhang stehen und bei denen der Auftragnehmer oder durch den Auftragnehmer beauftragte Dritte personenbezogene Daten für den Auftraggeber verarbeiten.

## 1. Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

### 1.1

Art, Zweck und Gegenstand der Verarbeitung

Dauer der Verarbeitung

Art der verarbeiteten personenbezogenen Daten

Kategorien der betroffenen Personen

### 1.2

Die in diesem Vertrag vereinbarten Leistungen werden ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Leistungen oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

## 2. Rechte und Pflichten des Auftragnehmers

### 2.1

Der Auftragnehmer verarbeitet Daten von betroffenen Personen ausschließlich im Rahmen der getroffenen Vereinbarungen und der dokumentierten Weisungen des Auftraggebers sowie entsprechend den datenschutzrechtlichen Regelungen, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, verpflichtet ist. In letzteren Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 Buchst. a DSGVO). Der Auftragnehmer verwendet die zur Verarbeitung überlassenen Daten für keine anderen Zwecke und insbesondere nicht für eigene Zwecke. Kopien der Daten werden, ohne dass sie im Auftrag oder in diesem Vertrag geregelt sind, nicht erstellt.

Sofern Weisungen des Auftraggebers zunächst mündlich erfolgen, sind sie unverzüglich schriftlich oder elektronisch zu bestätigen.

### 2.2

Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Ist die Rechtmäßigkeit einer Weisung zweifelhaft, ist der Auftragnehmer berechtigt, die Durchführung der Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Stehen schwere Persönlichkeitsrechtsverletzungen im Raum oder nimmt der Auftragnehmer bei weisungsgemäßem Handeln das Risiko einer strafbaren Handlung auf sich, darf er die Umsetzung der Weisung darüber hinaus aussetzen, bis die Parteien eine einvernehmliche Lösung gefunden haben.

### 2.3

Der Auftragnehmer gestaltet seine innerbetriebliche Organisation so, dass sie den Anforderungen des Datenschutzes gerecht wird. Er trifft insbesondere geeignete technische und organisatorische Maßnahmen, um einen dem Risiko angemessenen Schutz der Daten des Auftraggebers zu gewährleisten (Art. 32 Abs. 1 DSGVO). Sofern personenbezogene Daten in Telearbeit und Heimarbeit verarbeitet werden, ist er verpflichtet, dies dem Auftraggeber mitzuteilen. Er trifft diese technischen und organisatorischen Maßnahmen so, dass die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicher gestellt sind. Die entsprechenden technischen und organisatorischen Maßnahmen ergeben sich aus *(bitte ausführen - ggf. mit Verweisung -, z. B. aus der Anlage zu dieser Vereinbarung, dem Sicherheitskonzept etc.)*. Änderungen der getroffenen Maßnahmen durch den Auftragnehmer sind nur zulässig, wenn sichergestellt ist, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind dem Auftraggeber mitzuteilen und mit diesem abzustimmen.

### 2.4

Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von Anträgen betroffener Personen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte (Art. 28 Abs. 3 Buchst. e DSGVO) und unterstützt den Auftraggeber unter Berücksichtigung der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten, wie etwa bei erforderlichen Datenschutz-Folgenabschätzungen (Art. 28 Abs. 3 Satz 2 Buchst. f DSGVO).

### 2.5

Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Beschäftigten und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten

Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheit unterliegen. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

## 2.6

Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm im Rahmen des Auftragsverhältnisses Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Er trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen.

## 2.7

Der Auftragnehmer nennt dem Auftraggeber Ansprechpartner für im Rahmen des Vertrages anfallende Weisungen sowie einen etwaigen Datenschutzbeauftragten. Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Auftraggeber die Kontaktdaten eines neuen, zuständigen Ansprechpartners bzw. etwaigen Datenschutzbeauftragten unverzüglich anzuzeigen.

### Ansprechpartner des Auftragnehmers:

*(Name, Vorname und Funktion, Organisationseinheit, Telefon, E-Mail)*

### Datenschutzbeauftragter des Auftragnehmers

*(Name, Vorname und Funktion, Organisationseinheit, Telefon, E-Mail)*

## 2.8

Der Auftragnehmer berichtigt, löscht oder sperrt die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist, es sei denn, die Weisung widerspricht etwaigen gesetzlichen Aufbewahrungspflichten.

## 2.9

Nach Auftragsende sind Daten, Datenträger sowie sonstige Materialien auf Verlangen und nach Wahl des Auftraggebers entweder zurückzugeben oder zu löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur weiteren Speicherung der personenbezogenen Daten besteht.

## 2.10

Im Falle einer Inanspruchnahme des Auftraggebers durch eine Person hinsichtlich etwaiger Schadensersatzansprüche nach Art. 82 DSGVO verpflichtet sich der Auftragnehmer, den Auftraggeber bei der Abwehr der Ansprüche im Rahmen seiner Möglichkeiten zu unterstützen.

## **3. Rechte und Pflichten des Auftraggebers**

### 3.1

Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Beurteilung der Rechtmäßigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO, die Datenweitergabe an den Auftragnehmer sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DSGVO).

### 3.2

Der Auftraggeber informiert den Auftragnehmer unverzüglich, falls er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

### 3.3

Im Falle einer Inanspruchnahme des Auftragnehmers durch eine Person hinsichtlich etwaiger Schadensersatzansprüche nach Art. 82 DSGVO verpflichtet sich der Auftraggeber, den

Auftragnehmer bei der Abwehr der Ansprüche im Rahmen seiner Möglichkeiten zu unterstützen.

#### 3.4

Der Auftraggeber nennt dem Auftragnehmer weisungsberechtigte Personen für im Rahmen des Vertrages anfallende Weisungen sowie den Datenschutzbeauftragten. Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Auftragnehmer unverzüglich die Kontaktdaten eines neuen, zuständigen Ansprechpartners bzw. Datenschutzbeauftragten anzuzeigen.

Weisungsberechtigte Personen des Auftraggebers sind:

(Name, Vorname und Funktion, Organisationseinheit, Telefon, E-Mail)

Datenschutzbeauftragter des Auftraggebers

(Name, Vorname und Funktion, Organisationseinheit, Telefon, E-Mail)

#### 3.5

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieser Vereinbarung bestehen. Die Befugnisse der Aufsichtsbehörden – insbesondere nach Art. 58 Abs. 1 DSGVO – bleiben hiervon unberührt.

### 4. Anfragen betroffener Personen

Macht eine betroffene Person ihre Rechte gemäß Art. 15 ff. DSGVO gegenüber dem Auftragnehmer geltend, wird dieser die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber auf Basis der Angaben der betroffenen Person möglich ist. Gemäß Nr. 2.4 dieser Vereinbarung unterstützt der Auftragnehmer den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen.

### 5. Kontrollrechte des Auftraggebers

#### 5.1

Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung (Art. 28 Abs. 3 Satz 2 Buchst. h DSGVO). Ggf.: Folgende Nachweise sind diesem Vertrag als Anlage beigelegt:

- ☐ Ergebnisse eines Selbstaudits (Anlage )
- ☐ Zertifikat zu Datenschutz- und / oder Informationssicherheit (z.B. ISO 27001) (Anlage )
- ☐ Genehmigte Verhaltensregeln (Art. 40 DSGVO) vom ... (Datum) (Anlage )
- ☐ Verbindliche interne Datenschutzvorschriften (Art. 47 DSGVO) vom ... (Datum). (Anlage )
- ☐ Zertifizierungen gemäß Art. 42 DSGVO (Anlage )
- ☐ aktuelles Testat und/oder Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditor, Qualitätsauditor, Anlage )
- ☐ Datenschutz- und Vertraulichkeitsvereinbarung (Anlage XX zum EVB-IT \_\_\_\_ vertrag)
- ☐ .... (Anlage ).

#### 5.2

Sofern einschlägig, verpflichtet sich der Auftragnehmer, den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DSGVO und den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DSGVO unverzüglich zu informieren.

### 5.3

Der Auftraggeber ist berechtigt, sich vor Beginn und während der Verarbeitung von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in dieser Vereinbarung festgelegten Verpflichtungen zu überzeugen. Dies und Maßnahmen nach Nr. 5.4 werden nicht durch die Vorlage von Nachweisen nach Nr. 5.1 ausgeschlossen.

### 5.4

Inspektionen durch den Auftraggeber oder durch einen von diesem beauftragten Prüfer werden grundsätzlich nach vorheriger Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit zu den üblichen Geschäftszeiten durchgeführt. Der Auftragnehmer hat die Inspektion von der Unterzeichnung einer Verschwiegenheitserklärung abhängig zu machen, wenn die Möglichkeit besteht, dass der Auftraggeber oder ein von diesem beauftragter Prüfer im Rahmen seiner Inspektion auch Kenntnis von Daten erlangt, die der Auftragnehmer im Auftrag eines anderen Verantwortlichen verarbeitet. Der Auftraggeber stellt sicher, dass ein von ihm beauftragter Prüfer in keinem Wettbewerbsverhältnis zu dem Auftragnehmer steht.

## **6. Subunternehmer (weitere Auftragsverarbeiter)**

### 6.1

Ein Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt.

Der Auftragnehmer trägt bei der Auswahl eines Subunternehmers insbesondere Sorge dafür, dass dieser hinreichende Garantien dafür bietet, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung personenbezogener Daten entsprechend den Anforderungen der Datenschutz-Grundverordnung erfolgt.

Nicht als Subunternehmerverhältnis im Sinne dieser Regelung sind solche Leistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Hierzu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice (wenn ein Zugriff auf personenbezogene Daten des Auftraggebers ausgeschlossen ist), Reinigungskräfte und Prüfer. Der Auftragnehmer trifft mit diesen Dritten im erforderlichen Umfang schriftliche Vereinbarungen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten und behält sich Kontrollmaßnahmen vor, um den Schutz und die Sicherheit der Daten des Auftraggebers zu gewährleisten.

### 6.2

Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO). In dem Vertrag mit dem Subunternehmer sind dieselben datenschutzrechtlichen Pflichten aus der vorliegenden Vereinbarung dem Subunternehmer wirksam aufzuerlegen. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

### 6.3

Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Abschnitt vertraglich auferlegt wurden.

## 6.4

Der Auftragnehmer nimmt keinen Subunternehmer ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung in Anspruch. Der Auftragnehmer teilt dem Auftraggeber die bereits bei Abschluss dieses Vertrags bestehenden Subunternehmer vorab mit. Die bei Vertragsbeginn bestehenden Subunternehmer sind in **Anlage ... zu dieser Vereinbarung zur Auftragsverarbeitung** aufgeführt. Diese gelten als von Beginn des Auftrages an genehmigt.

## 6.5

### Weitere Subunternehmer

#### **Alternative 1:**

- ☒ Der Auftragnehmer nimmt einen Subunternehmer nur in Anspruch, wenn der Auftraggeber dies zuvor gesondert schriftlich genehmigt hat (Art. 28 Abs. 2 Satz 1 Alt. 1 DSGVO). Der Auftragnehmer informiert den Auftraggeber frühzeitig, wenn er Änderungen in Bezug auf die Hinzuziehung oder die Ersetzung Subunternehmer beabsichtigt.

#### **Alternative 2:**

- ☐ Gemäß den vorgenannten Regelungen erteilt der Auftraggeber dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter im Sinne des Art. 28 Abs. 2 DSGVO in Anspruch zu nehmen (Art. 28 Abs. 2 Satz 1 Alt. 2, Satz 2 DSGVO). Dies gilt nicht für Subunternehmer in Drittstaaten. Der Auftragnehmer informiert den Auftraggeber frühzeitig, wenn er Änderungen in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter beabsichtigt. Der Auftraggeber kann gegen derartige Änderungen Einspruch erheben. Der Einspruch ist innerhalb von einem Monat nach Zugang der Information über die Änderungen schriftlich gegenüber dem Auftragnehmer einzulegen. Kann keine einvernehmliche Lösung erzielt werden, erfolgt eine Einschränkung oder Beendigung der Auftragsverarbeitung.

## 6.6

Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind und der Auftraggeber vorab gesondert schriftlich zustimmt.

## **7. Haftung und Schadensersatz**

Die Vertragsparteien haften entsprechend den einschlägigen gesetzlichen Bestimmungen bzw. gegenüber betroffenen Personen gemäß Art. 82 DSGVO.

## **8. Schlussbestimmungen**

### 8.1

**Die Laufzeit und das Recht zur ordentlichen Kündigung dieser Vereinbarung zur Auftragsverarbeitung richtet sich nach dem zugrundeliegenden EVB-IT \_\_\_\_vertrag (Az.: \_\_\_\_\_)**

**(Bitte eine Regelung zu Laufzeit und Kündigungsmöglichkeiten ergänzen)**

### 8.2

Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn die Daten des Auftraggebers durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter beim



Auftragnehmer gefährdet werden. Der Auftragnehmer informiert in diesem Fall alle Beteiligten unverzüglich darüber, dass das Eigentum an den Daten ausschließlich beim Auftraggeber liegt.

### 8.3

Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen oder in einem elektronischen Format abgefassten Vereinbarung, die den ausdrücklichen Hinweis darauf enthält, dass es sich um eine Änderung bzw. Ergänzung dieser Vereinbarung handelt.

### 8.4

Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise unwirksam oder undurchführbar sein oder werden, so ist die Wirksamkeit der übrigen Regelungen hiervon nicht betroffen. In diesem Falle werden die Parteien einvernehmlich eine neue Regelung oder Ergänzung der bestehenden Regelung vereinbaren, die die unwirksame oder undurchführbare Regelung in einer Art und Weise ersetzt bzw. ergänzt, die der ursprünglich von den Parteien bei Abfassung dieser Anlage beabsichtigten Regelung am nächsten kommt, hätten sie denn die Unwirksamkeit oder Undurchführbarkeit bedacht. Dies gilt auch für Regelungslücken.

\_\_\_\_\_, den \_\_\_\_\_  
Ort Datum

\_\_\_\_\_, den \_\_\_\_\_  
Ort Datum

\_\_\_\_\_  
- Auftraggeber -

\_\_\_\_\_  
- Auftragnehmer -



## Information über die Verarbeitung personenbezogener Daten von Externen im Landesamt für Sicherheit in der Informationstechnik

### 1. Name und Kontaktdaten des Verantwortlichen

Das Landesamt für Sicherheit in der Informationstechnik (LSI) nimmt auf vertraglicher Grundlage Leistungen von Externen in Anspruch. Soweit das LSI im Rahmen dieser vertraglichen Beziehung personenbezogene Daten des Externen und/oder seiner Mitarbeiterinnen und Mitarbeiter verarbeitet, ist das LSI hierfür datenschutzrechtlich verantwortlich.

**Landesamt für Sicherheit in der Informationstechnik**  
**Keßlerstraße 1**  
**90489 Nürnberg**  
**Telefon: 0911/21549-0**  
**E-Mail: [poststelle@lsi.bayern.de](mailto:poststelle@lsi.bayern.de)**

### 2. Kategorien von Daten, die durch das LSI verarbeitet werden:

Je nach Erforderlichkeit werden hierbei folgende Kategorien von Daten durch das LSI verarbeitet:

- Anrede, Vorname, Nachname, ggf. Geburtsname
- Geburtsdatum
- Geburtsort
- Lichtbild
- Einverständniserklärung zur Sicherheitsüberprüfung
- Kopie eines Ausweisdokuments zur Sicherheitsüberprüfung
- Ergebnis der Sicherheitsüberprüfung
- Verpflichtungserklärung nach dem Verpflichtungsgesetz
- Verschwiegenheitserklärung
- sonstige Nachweise zur Eignung (z.B. Nachweis über Berufserfahrung, Qualifikation, Sprachkenntnisse, Sicherheitsüberprüfung)
- ggf. Zeiterfassungsdaten
- ggf. Sozialversicherungsnachweis
- ggf. Lohnabrechnungen
- ggf. Aufenthalts- und Arbeitserlaubnis
- ggf. Kontaktdaten

### 3. Zweck der Verarbeitung

Zweck der Verarbeitung ist die Durchführung des Vertrags. Die Verarbeitung der Daten erfolgt beispielsweise

- zur Identifikation einer Person,
- zur Feststellung der individuellen Eignung für eine konkrete Tätigkeit,
- zur Überprüfung von An- und Abwesenheitszeiten,
- aus Brandschutzgründen.

#### **4. Rechtsgrundlagen der Verarbeitung**

Die Rechtsgrundlagen für die Verarbeitung ergeben sich aus **Art. 6 Abs. 1 S. 1 Buchstabe b, c, und e, Abs. 2, Abs. 3 Satz 2 Buchstabe b Datenschutz-Grundverordnung (DSGVO) i. V. m. Art. 4 Abs. 1 Bayerisches Datenschutzgesetz (BayDSG).**

#### **5. Empfänger oder Kategorien von Empfängern der personenbezogenen Daten**

Soweit erforderlich werden einzelne Kategorien von Daten bestimmten Empfängern offengelegt. Dies geschieht beispielsweise zur Zeiterfassung gegenüber dem Betreiber des Zeiterfassungssystems oder zur Sicherheitsüberprüfung gegenüber den zuständigen Sicherheitsbehörden, wenn eine solche veranlasst ist.

#### **6. Dauer der Speicherung der personenbezogenen Daten**

Soweit die personenbezogenen Daten als Anlagen zum Vertrag gemeinsam mit diesem in der elektronischen Akte gespeichert werden, richtet sich die Dauer der Speicherung nach dem allgemein gültigen Löschkonzept für die elektronische Akte.

Personenbezogene Daten, die zum Zweck der Sicherheitsüberprüfung erhoben werden, werden außerhalb der elektronischen Akte gespeichert und spätestens drei Jahre nach Auslaufen des Vertrags gelöscht. In der elektronischen Akte wird lediglich Name, Datum und Einverständnis mit sowie Ergebnis der Sicherheitsüberprüfung vermerkt.

#### **7. Rechte der Betroffenen**

Soweit durch das LSI personenbezogene Daten verarbeitet werden, stehen den Betroffenen nachfolgende Rechte zu:

- Es besteht ein Recht auf Auskunft über die zur eigenen Person gespeicherten Daten (Art. 15 DSGVO).
- Sollten unrichtige oder unvollständige personenbezogene Daten verarbeitet werden, gibt es ein Recht auf Berichtigung bzw. Vervollständigung (Art. 16 DSGVO).
- Liegen die gesetzlichen Voraussetzungen vor, kann die Löschung oder Einschränkung der Verarbeitung verlangt werden (Art. 17 und 18 DSGVO).
- Die Betroffenen haben das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung ihrer Daten Widerspruch einzulegen, wenn die Verarbeitung ausschließlich auf Grundlage des Art. 6 Abs. 1 Buchst. e oder f DSGVO erfolgt (Art. 21 Abs. 1 DSGVO).
- Wenn in die Verarbeitung eingewilligt worden ist oder sie zur Vertragserfüllung erforderlich ist und die Datenverarbeitung mithilfe automatisierter Verfahren durchgeführt wird, besteht gegebenenfalls ein Recht auf Datenübertragbarkeit (Art. 20 DSGVO).

## **8. Beschwerderecht bei der Aufsichtsbehörde**

Es besteht außerdem ein Beschwerderecht bei der Aufsichtsbehörde, die unter folgenden Kontaktdaten erreichbar ist:

**Der Bayerische Landesbeauftragte für den Datenschutz**  
**Postanschrift: Postfach 22 12 19, 80502 München**  
**Adresse: Wagmüllerstraße 18, 80538 München**  
**Telefon: 089 212672-0**  
**Telefax: 089 212672-50**  
**E-Mail: [poststelle@datenschutz-bayern.de](mailto:poststelle@datenschutz-bayern.de)**  
**Internet: <https://www.datenschutz-bayern.de/>**

## **9. Kontaktdaten der / des Datenschutzbeauftragten im LSI**

Diese Information erfolgt gemäß Art. 13, Art. 14 EU-Datenschutz-Grundverordnung (DSGVO) und Art. 9 Bayerisches Datenschutzgesetz (BayDSG). Für weitere Fragen zum Datenschutz steht der/die behördliche Datenschutzbeauftragte des LSI gerne zur Verfügung:

**Behördliche/r Datenschutzbeauftragte/r des**  
**Landesamts für Sicherheit in der Informationstechnik**  
**- persönlich -**  
**Keßlerstraße 1**  
**90489 Nürnberg**  
**Telefon: 0911/21549-0**  
**E-Mail: [datenschutz@lsi.bayern.de](mailto:datenschutz@lsi.bayern.de)**

# Permission To Attack (PTA)

Berechtigung zur Durchführung eines Penetrationstests von Webanwendungen, die nicht in einem staatlichen Rechenzentrum des Freistaats Bayern gehostet werden

Zu testende URL(s) (Scope): (umfasst alle unter der jeweils genannten URL liegenden Dateipfade)

[https://www.example.com]

Explizit vom Test ausgenommene URL(s) (nicht im Scope):

Auftraggeber des Penetrationstests:

Auftraggeber des Penetrationstests ist der Anbieter der zu testenden Webanwendung. Anbieter im Sinne von § 18 des Medienstaatsvertrags (MStV) ist:

[BEHÖRDE/FIRMA], [ADRESSE]

[VERTRETUNGSBERECHTIGTE PERSON mit VORNAME und NACHNAME]

Anwendungsbetreiber der zu testenden Webanwendung:

[BEHÖRDE/FIRMA], [ADRESSE]

[VERTRETUNGSBERECHTIGTE PERSON mit VORNAME und NACHNAME]

Betreiber der physischen Infrastruktur der zu testenden Webanwendung:

[BEHÖRDE/FIRMA], [ADRESSE]

[VERTRETUNGSBERECHTIGTE PERSON mit VORNAME und NACHNAME]

Auftragnehmer und Unterauftragnehmer

Der Penetrationstest wird durch das Landesamt für Sicherheit in der Informationstechnik (LSI), Keßlerstraße 1, 90489 Nürnberg, Vertretungsberechtigter Bernd Geisler, durchgeführt. Das LSI ist insofern Auftragnehmer und kann seinerseits einen oder mehrere Unterauftragnehmer einsetzen. Mit Antragstellung wird das LSI mit der Durchführung des Penetrationstests gemäß BayITSir-14 der oben genannten URL(s) beauftragt.

Geplante Aktivitäten

Das Ziel des Penetrationstests ist die Webanwendung. Hierfür wird ein nicht invasiver Blackbox- oder Greybox-Test auf Anwendungsebene durchgeführt. Sofern Sicherheitsmechanismen der Webanwendung überwunden werden können, wird der Test abgebrochen. Dedizierte Angriffsversuche auf den Server, das Betriebssystem oder die physische Infrastruktur des Betreibers sind nicht Teil der geplanten Aktivitäten des Penetrationstests. Die Sicherheitsüberprüfung der Webanwendung umfasst insbesondere folgende Aktivitäten:

- Automatisiertes Crawlen der Webanwendung
- Webserver Configuration Testing
- Identity Management Testing
- Authentication Testing
- Authorization Testing
- Session Management Testing
- Input Validation Testing
- Error Handling Testing
- Weak Cryptography Testing
- Business Logic Testing
- API Testing (sofern vorhanden)

### Zeitraum und Modalitäten der Durchführung des Penetrationstests

Der Auftragnehmer führt den Penetrationstest für den Auftraggeber durch. Der Testzeitraum wird dem Auftraggeber vor dem Test mitgeteilt, soweit dies möglich ist. Bei der Durchführung des Penetrationstests wird die Webanwendung insbesondere auf gängige Schwachstellen geprüft. Hierzu ist es gegebenenfalls notwendig eine erhöhte Anzahl von Anfragen abzusenden. Es wird aber darauf geachtet, dass die Frequenz der gesendeten Anfragen im Bereich dessen liegt, welche die Systeme üblicherweise ohne Schwierigkeiten verarbeiten können. Ein Denial-of-Service- Angriff ist explizit nicht Bestandteil des Tests. Es kann jedoch nicht ausgeschlossen werden, dass es bei Fehlverhalten der Anwendung beim Betreiber der physischen Infrastruktur und gegebenenfalls beim Anwendungsbetreiber der zu testenden Webanwendung zu Beeinträchtigungen kommt.

### Erklärung:

**Das Einverständnis mit dem externen Penetrationstest wird hiermit ausdrücklich zugesichert. Alle Beteiligten sind sich der möglichen Auswirkungen bewusst. Diese können sowohl die Anwendung als auch darüber hinaus ungewollt u.a. die Plattform und die Infrastruktur betreffen. Es liegt in der jeweiligen Verantwortung von Auftraggeber, Betreiber der physischen Infrastruktur und Anwendungsbetreiber der zu testenden Webanwendung im Vorfeld marktübliche Vorkehrungen zu treffen, um mögliche negative Folgen wie Datenverlust, Manipulation von Daten oder einen Verlust an Verfügbarkeit zu vermeiden oder zu minimieren.**

**Diese Einverständniserklärung umfasst alle für einen Penetrationstest notwendigen Handlungen, insbesondere solche, die strafrechtlich relevant, oder nach anderen Vorschriften und Gesetzen, insbesondere dem TKG und dem ZKDSG ohne Genehmigung rechtswidrig sein können.**

Der **Betreiber der physischen Infrastruktur** stimmt oben genannter Erklärung zu.

---

Ort, Datum

---

Unterschrift des Betreibers der physischen Infrastruktur der Webanwendung

Der **Anwendungsbetreiber** stimmt oben genannter Erklärung zu.

---

Ort, Datum

---

Unterschrift des Anwendungsbetreibers der Webanwendung

Der **Auftraggeber** stimmt oben genannter Erklärung zu.

---

Ort, Datum

---

Unterschrift des Auftraggebers des Penetrationstests

# LEISTUNGSVERZEICHNIS

Ausschreibung (Korrektur)

08.06.2026

Verfahren: 2026THA000002 - App-Katalog zum App-Security-Check; LSI

## SKONTO

Skonto zugelassen	Nein
Zahlungsziel (falls zugelassen)	Tag(e)
Skonto	_____ %

## AUFLISTUNG ALLER POSITIONEN

ALLE PREISE SIND OHNE UMSATZSTEUER ANZUGEBEN

1	Angebotspreis gem. Anlage 06a Preiszusammenstellung	USt. [%]	Menge	Einheit	Einzelpreis [EUR]	Gesamtpreis [EUR]
		19%	1,00	Summe	..... pro 1,00 Summe	.....

Die Anlage 06a Preiszusammenstellung muss vom Bieter ausgefüllt und im Arbeitsschritt "Eigene Anlagen" in den Angebotsassistenten hochgeladen werden.

Der "Angebotspreis (netto) gesamt" aus Zelle F46 des Preisblattes ist in dieser Produktposition in das Feld "Preis" einzutragen.

WICHTIGER HINWEIS: Das Fehlen der ausgefüllten Anlage Preisblatt oder Differenzen zum hier angegebenen Gesamtangebotspreis führen möglicherweise zum Angebotsausschluss.

### Hinweis zur Umsatzsteuer

Bei der Ermittlung des wirtschaftlichsten Angebotes werden die Bruttopreise berücksichtigt.

Der Bruttopreis beinhaltet bei Übergang der Steuerschuld auf den Auftraggeber (z. B. gem. § 13b UStG) auch die von diesem an das zuständige Finanzamt abzuführende Umsatzsteuer.

Hinweis: Der Umsatzsteuersatz in den Produktpositionen darf vom Bieter nur angepasst werden, sofern ein ermäßigter Steuersatz (z.B. Leistungen von Behindertenwerkstätten) oder eine Umsatzsteuerbefreiung (§§ 4, 19 UStG) vorliegt.

Zusammenfassung: Wertungspreis = Angebotsnettopreis + (Einfuhr-/)Umsatzsteuer unabhängig davon, ob Auftraggeber oder Auftragnehmer Steuerschuldner ist.

## ANGEBOTSSUMME(N)

Summe exkl. Nachlass (netto)	_____
Nachlass (netto)	_____
Summe inkl. Nachlass (netto)	_____
Umsatzsteuer	_____
<b>Summe (brutto)</b>	_____



## AUFLISTUNG ALLER DATEIANLAGEN ZU DEN POSITIONEN

Name	Dateiname	Größe	MIME-Type
------	-----------	-------	-----------

Verfahren: 2026THA000002 - App-Katalog zum App-Security-Check; LSI

### EIGNUNGSKRITERIEN

<b>1</b>	<b>statistische Angaben</b> Gewichtung: 0,00%
<b>1.1</b>	<b>Unternehmensgröße [Mussangabe]</b> Zur Kontrolle der öffentlichen Vergabeverfahren und zur Überprüfung ihrer Mittelstandsförderungsmaßnahmen erhebt die Europäische Union (EU) bei allen ausschreibenden Stellen verschiedene Daten zum Ergebnis von Vergabeverfahren. Bitte geben Sie hierzu Ihre Unternehmensgrößenklasse an. Nähere Informationen, ob Ihr Unternehmen die Eigenschaft als Kleinst-, kleines oder mittleres Unternehmen erfüllt, finden Sie in dem vom Amt für Veröffentlichungen der Europäischen Union herausgegebenen Benutzerleitfaden zur Definition von KMU. Es handelt sich um einen rein statistischen Wert, d.h. die Angabe zu diesem Punkt hat keinerlei Auswirkung auf die Zulässigkeit Ihres Angebots oder die Bewertung der Wirtschaftlichkeit.  <input type="checkbox"/> Keine Angabe (0) <input type="checkbox"/> Kleinstunternehmen (0) <input type="checkbox"/> Kleines Unternehmen (0) <input type="checkbox"/> Mittleres Unternehmen (0) <input type="checkbox"/> Großunternehmen (0)  Nur eine Antwort wählbar
<b>2</b>	<b>Ausschlussgründe nach den §§ 123, 124 GWB</b> Gewichtung: 0,00%
<b>2.1</b>	<b>Hinweis</b> Hinweis: Ein Eintrag zu den folgenden Punkten erfolgt erst bei der Angebotsprüfung durch den Auftraggeber, es ist kein Eintrag durch den Bieter zulässig.
<b>2.2</b>	<b>Ausschlussgründe nach § 123 GWB</b> Ausschlusskriterium Der Auftraggeber hat keine Kenntnis von zwingenden Ausschlussgründen nach §123 GWB?  <input type="checkbox"/> Keine Angabe <input type="checkbox"/> Ja <input type="checkbox"/> Nein  Nur eine Antwort wählbar
<b>2.3</b>	<b>Ausschluss nach § 124 GWB</b> Ausschlusskriterium Der Auftraggeber hat keine Kenntnis von fakultativen Ausschlussgründen nach § 124 GWB, die zum Ausschluss führen?  <input type="checkbox"/> Keine Angabe <input type="checkbox"/> Ja <input type="checkbox"/> Nein  Nur eine Antwort wählbar
<b>3</b>	<b>Eigenerklärung</b> Gewichtung: 0,00%
<b>3.1</b>	<b>Bestätigung der Kenntnisnahme [Mussangabe]</b> Ausschlusskriterium Die Eigenerklärung habe ich zur Kenntnis genommen und bestätige ihren Inhalt.  <input type="checkbox"/> Keine Angabe <input type="checkbox"/> Ja <input type="checkbox"/> Nein  Nur eine Antwort wählbar
<b>3.2</b>	<b>Bestätigung zu Bewerber- / Bietergemeinschaften</b> Als bevollmächtigter Vertreter bestätige ich, dass auch sämtliche beteiligte Unternehmen den Inhalt der Eigenerklärung zur Kenntnis genommen und bestätigt haben.  (Anmerkung: liegt keine Beteiligung als Bewerber- / Bietergemeinschaft vor, ist keine Angabe zu machen.)

- ☐ Keine Angabe (0)
- ☐ Ja (0)
- ☐ Nein (0)

Nur eine Antwort wählbar

### 3.3 Bestätigung der Kenntnisnahme RUS [Mussangabe]

Ausschlusskriterium

Die Eigenerklärung zu russischen Unternehmen habe ich zur Kenntnis genommen und bestätige ihren Inhalt.

- ☐ Keine Angabe
- ☐ Ja
- ☐ Nein

Nur eine Antwort wählbar

### 3.4 Angaben zu fakultativen Ausschlussgründen

Sollten für Sie bzw. Ihr Unternehmen fakultative Ausschlussgründe nach § 124 GWB vorliegen, schildern Sie bitte, warum diese nicht zu einem Ausschluss vom Verfahren führen sollen.  
Der Auftraggeber entscheidet im Rahmen der Angebotsprüfung über den Ausschluss.  
Sie können ausführlichere Angaben zum Sachverhalt auch im Arbeitsschritt Eigene Anlagen als Dokument hochladen.

## 4 Angaben Wettbewerbsregister

Gewichtung: 0,00%

### 4.1 Grundlage Auskunft Wettbewerbsregister

Öffentliche Auftraggeber sind nach § 6 Abs. 1 des Wettbewerbsregistergesetzes ab einer Höhe von 30.000 € verpflichtet, für den Bieter, der den Zuschlag erhalten soll, vor der Zuschlagserteilung eine Auskunft aus dem Wettbewerbsregister anzufordern.

### 4.2 Name des Unternehmens [Mussangabe]

Name des Unternehmens:

## 4.3 Postanschrift

Gewichtung: 0,00%

### 4.3.1 Sitz des Unternehmens [Mussangabe]

Sitz des Unternehmens / der Firma:

### 4.3.2 Straße [Mussangabe]

Straße:

### 4.3.3 Hausnummer [Mussangabe]

Hausnummer:

### 4.3.4 Postleitzahl [Mussangabe]

Postleitzahl:

Hinweis: Es sind nur Hauszustellungs-Postleitzahlen zulässig!

### 4.3.5 Ort [Mussangabe]

Ort:

### 4.3.6 Land [Mussangabe]

In welchem Land / Staat ist Ihr Unternehmen ansässig?

### 4.4 Rechtsform [Mussangabe]

Welche Rechtsform hat Ihr Unternehmen?

- ☐ Keine Angabe (0)
- ☐ Natürliche Person (0)
- ☐ AG (0)
- ☐ AG (England) (0)
- ☐ AG (Schottland) (0)
- ☐ AG (Schweiz) (0)
- ☐ AG & Co. KG (0)
- ☐ AG & Co. KG i. L. (0)
- ☐ AG & Co. oHG (0)
- ☐ AG & Co. oHG i. L. (0)
- ☐ AG i. Gr. (0)
- ☐ AG i. L. (0)
- ☐ AöR (0)

☐ BV (0)  
☐ Corp. (0)  
☐ e.K. (0)  
☐ e.V. (0)  
☐ e.V. i. L. (0)  
☐ eG (0)  
☐ eG i. Gr. (0)  
☐ eG i. L. (0)  
☐ eGbR (0)  
☐ Einzelunternehmer (0)  
☐ EWIV (0)  
☐ GbR (0)  
☐ gGmbH (0)  
☐ GmbH (0)  
☐ GmbH (Österreich) (0)  
☐ GmbH (Schweiz) (0)  
☐ GmbH & Co. KG (0)  
☐ GmbH & Co. KG i. L. (0)  
☐ GmbH & Co. OHG (0)  
☐ GmbH & Co. OHG i. L. (0)  
☐ GmbH i. Gr. (0)  
☐ GmbH i. L. (0)  
☐ Inc. (0)  
☐ KG (0)  
☐ KG i. L. (0)  
☐ KGaA (0)  
☐ KöR (0)  
☐ LLP (0)  
☐ Ltd. (0)  
☐ n.e.V. (0)  
☐ NV (0)  
☐ OHG (0)  
☐ OHG i. L. (0)  
☐ Oy (0)  
☐ PartG (0)  
☐ PartG i. L. (0)  
☐ PartGmbH (0)  
☐ S.L. (0)  
☐ SA (0)  
☐ SARL (0)  
☐ SE (0)  
☐ SNC (0)  
☐ sp. z.o.o. (0)  
☐ SpA (0)  
☐ SRL (0)  
☐ Stiftung & Co. KG (0)  
☐ Stiftung & Co. KG i. L. (0)  
☐ Stiftung & Co. OHG (0)  
☐ Stiftung & Co. OHG i. L. (0)  
☐ Stiftung bR (0)  
☐ Stiftung öR (0)  
☐ UG (haftungsbeschränkt) (0)  
☐ UG (haftungsbeschränkt) & Co. KG (0)  
☐ VEB (0)  
☐ VVaG (0)  
☐ WEG (0)  
☐ Rechtsform nicht gelistet (0)

Nur eine Antwort wählbar

## 4.5 Registerangaben

Gewichtung: 0,00%

### 4.5.1 Registerangaben

Ist das zuständige Registergericht / die zuständige Registerstelle im In- oder im Ausland angesiedelt?

- ☐ *Keine Angabe* (0)  
☐ Register in der Bundesrepublik Deutschland (= Inländisches Register). Bitte füllen Sie die Felder unter 'Inländisches Register' aus. (0)  
☐ Register außerhalb der Bundesrepublik Deutschland (= Ausländisches Register). Bitte füllen Sie die Felder unter 'Ausländisches Register' aus. (0)  
☐ Für mein Unternehmen existiert kein Registereintrag, da natürliche Person/Personenvereinigung. Bitte füllen Sie die Felder unter 'Keine Registerangabe' aus. (0)

Nur eine Antwort wählbar

### 4.5.2 Inländisches Register

Gewichtung: 0,00%

#### 4.5.2.1 Registergericht

Zuständiges Registergericht:

#### 4.5.2.2 Registerart

Zutreffende Registerart:

- ☐ *Keine Angabe* (0)  
☐ HRA (0)  
☐ HRB (0)

☐ GnR (0)  
☐ GsR (0)  
☐ PR (0)  
☐ VR (0)

Nur eine Antwort wählbar

#### 4.5.2.3 Registernummer

Angabe zur Registernummer:

#### 4.5.3 Ausländisches Register

Gewichtung: 0,00%

##### 4.5.3.1 Ausländische Registernummer

Ausländische Registernummer:

##### 4.5.3.2 Registerbezeichnung

Registerbezeichnung:

##### 4.5.3.3 Registerführende Stelle

Registerführende Stelle:

#### 4.5.4 Keine Registerangabe

Gewichtung: 0,00%

##### 4.5.4.1 Keine Registerangabe

Für Einzelunternehmer (Freiberufler oder Selbstständige) werden folgende Angaben benötigt.

##### 4.5.4.2 Einzelunternehmer

Gewichtung: 0,00%

###### 4.5.4.2.1 Familienname

Familienname:

###### 4.5.4.2.2 Vorname

Vorname:

##### 4.5.4.3 Sonstige Gründe

Bitte erläutern Sie, weshalb keine der vorhergehenden Auswahlmöglichkeiten zutreffen:

#### 4.5.5 Umsatzsteueridentifikationsnummer

Falls Sie eine Umsatzsteueridentifikationsnummer besitzen, dann geben Sie diese bitte an:

#### 5 Eigenerklärung für Unterauftragnehmer

Gewichtung: 0,00%

##### 5.1 Eigenerklärung Unterauftragnehmer Eignungsverl.

Ich bestätige, dass ich die Anlage "Eigenerklärung für Unterauftragnehmer und Eignungsverleiher" jedem Unterauftragnehmer oder Eignungsverleiher zur Bestätigung weitergeleitet habe. Sie wurde von diesen um Firmenbezeichnung und -anschrift ergänzt, unterschrieben und anschließend im Arbeitsschritt "Eigene Anlagen" als pdf-Datei hochgeladen.

(Anmerkung: Liegt keine Einbeziehung von Unterauftragnehmern oder Eignungsverleihern vor, ist keine Angabe zu machen.)

☐ Keine Angabe (0)  
☐ Ja (0)  
☐ Nein (0)

Nur eine Antwort wählbar

#### 6 Anlage 06b Bewertungsmatrix Eignung App-Katalog [Mussangabe]

Ausschlusskriterium

Die Anlage "06b Bewertungsmatrix Eignung App-Katalog" muss vom Bieter vollständig ausgefüllt (d.h. es sind alle Fragen zu beantworten) und im Angebotsassistenten im Arbeitsschritt „Eigene Anlagen“ als Excel-Datei hochgeladen werden. Der Bieter kann für die Beantwortung der Fragen auch eigene Dokumente erstellen und dem Angebot elektronisch im Arbeitsschritt „Eigene Anlagen“ beifügen. Bei jeder Antwort muss der Bieter die jeweilige Referenznummer in der Bewertungsmatrix (z.B. Kriterium 2.1.) angeben, damit ein eindeutiger Bezug seiner Ausführungen zum jeweiligen Kriterium hergestellt werden kann. Bitte bestätigen Sie die Kenntnisnahme.

- ☐ *Keine Angabe*
- ☐ Ja
- ☐ Nein

Nur eine Antwort wählbar

## 7 **Ausschlusskriterien erfüllt**

Ausschlusskriterium

Alle in der „Bewertungsmatrix Eignung“ angegebenen Ausschlusskriterien werden erfüllt.  
Die Überprüfung und Bewertung erfolgt durch den Auftraggeber auf Basis der Bieterangaben. (=Auswertungskriterium für Auftraggeber).

- ☐ *Keine Angabe*
- ☐ Ja
- ☐ Nein

Nur eine Antwort wählbar

Verfahren: 2026THA000002 - App-Katalog zum App-Security-Check; LSI

---

## LEISTUNGSKRITERIEN

### 1 Anlage 06c Bewertungsmatrix Leistung App Katalog [Mussangabe]

Ausschlusskriterium

Die Anlage 06c Bewertungsmatrix Leistung App Katalog muss vom Bieter vollständig ausgefüllt (d.h. es sind alle Fragen zu beantworten) und im Angebotsassistenten im Arbeitsschritt „Eigene Anlagen“ als Excel-Datei hochgeladen werden.

Der Bieter kann für die Beantwortung der Fragen auch eigene Dokumente erstellen und dem Angebot elektronisch im Arbeitsschritt „Eigene Anlagen“ beifügen. Bei jeder Antwort muss der Bieter die jeweilige Referenznummer in der Bewertungsmatrix (z.B. Kriterium L 2.3) angeben, damit ein eindeutiger Bezug seiner Ausführungen zum jeweiligen Kriterium hergestellt werden kann.

Bitte bestätigen Sie die Kenntnisnahme.

- ☐ Keine Angabe
- ☐ Ja
- ☐ Nein

Nur eine Antwort wählbar

### 2 Ausschlusskriterien erfüllt

Ausschlusskriterium

Alle in der „Bewertungsmatrix Leistung“ angegebenen Ausschlusskriterien werden erfüllt.

Die Überprüfung und Bewertung erfolgt durch den Auftraggeber auf Basis der Bieterangaben. (=Auswertungskriterium für Auftraggeber).

- ☐ Keine Angabe
- ☐ Ja
- ☐ Nein

Nur eine Antwort wählbar

### 3 Erzielte Leistungspunktzahl

Gewichtung: 100,00%

Maximalpunktzahl: 1.000

In der Anlage 06c Bewertungsmatrix Leistung App Katalog erzielte Leistungspunktzahl. (=Auswertungskriterium für Auftraggeber).

### 4 Anlage 06d Anforderungskatalog Barrierefreiheit [Mussangabe]

Ausschlusskriterium

Die Anlage 06d Anforderungskatalog Barrierefreiheit muss vom Bieter vollständig ausgefüllt (d.h. es sind alle Fragen zu beantworten) und im Angebotsassistenten im Arbeitsschritt „Eigene Anlagen“ als Excel-Datei hochgeladen werden.

Der Bieter kann für die Beantwortung der Fragen auch eigene Dokumente erstellen und dem Angebot elektronisch im Arbeitsschritt „Eigene Anlagen“ beifügen. Bei jeder Antwort muss der Bieter die jeweilige Referenznummer des Anforderungskatalogs angeben, damit ein eindeutiger Bezug seiner Ausführungen zum jeweiligen Kriterium hergestellt werden kann

- ☐ Keine Angabe
- ☐ Ja
- ☐ Nein

Nur eine Antwort wählbar

Typ	Dateiname	Größe	MIME-Type
Dateianlage	Anlage 06aPreiszusammenstellung.xlsx	21,20 KB	xlsx
Dateianlage	Anlage 06b_Bewertungsmatrix Eignung App-Katalog.xlsx	22,14 KB	xlsx
Dateianlage	Anlage 06c_Bewertungsmatrix Leistung App-Katalog 1. Korrekturzyklus.xlsx	53,88 KB	xlsx
Dateianlage	Anlage 06d_Anforderungskatalog Barrierefreiheit.xlsx	38,11 KB	xlsx