Fragebogen für die Deklaration des Restrisikos (Stand 22.11.2022)

Zertifizierung	
Für die Hosting- / Cloud-Lösung liegt eine Zertifizierung vor nach	
• ISO 27001 auf Basis IT-Grundschutz	Ja [ ]
• ISO 27001 in Kombination mit Vorgaben für die technische Umsetzung	Ja [ ]
• C5-Testierung (Typ1/Typ2)	Ja [ ]
• Trusted Cloud Data Protection Profile (TCDP) mit Listung beim BMWi	Ja [ ]
→ **bitte beilegen**	
Für die Hosting- / Cloud-Lösung liegt **keine** der oben genannten Zertifizierung vor	Ja [ ]
Kommunikation zwischen Client und Server	
die Kommunikation zw. Client und Server erfolgt immer verschlüsselt via HTTPS	erfüllt [ ]
Verschlüsselung kommt mindestens **TLS 1.2 oder neuer ohne SSL-Fallback** zum Einsatz	erfüllt [ ]
es kommen Zertifikate, die von einer gültigen und vertrauenswürdigen CA signiert wurden, zum Einsatz	erfüllt [ ] nicht erfüllt [ ]
Die Benutzeranmeldung erfolgt verschlüsselt, samt sicher erzeugter Session-IDs	erfüllt [ ] nicht erfüllt [ ]
Client-Technologie	
es kommt lediglich HTML(5) - pur oder mit JavaScript - zum Einsatz	erfüllt [ ]
es kommen **keine** Browser-Plugins oder Thick-Clients zum Einsatz	erfüllt [ ] nicht erfüllt [ ]
der WebClient des Auftragnehmers **versucht nicht**, Komponenten per Sideloading auf dem Client zu installieren	erfüllt [ ] nicht erfüllt [ ]
der WebClient des Auftragnehmers beinhaltet **keine** Cookies von Dritt-Anbietern	erfüllt [ ] nicht erfüllt [ ]
Vorkehrungen gegen Sicherheitslücken, Bufferoverflow und Code-Injection	
ein Patch-Management (Server-Betriebssystem, WebServer, Usermanagment, WebClient) zur **schnellstmöglichen Behebung von Sicherheitslücken** ist etabliert	erfüllt [ ] nicht erfüllt [ ]
Es besteht eine kontextsensitive Filterung der Eingaben, Uploads und Downloads oder vergleichbare Mechanismen zur Verhinderung des Einschleusens von Ausführbaren Code	erfüllt [ ] nicht erfüllt [ ]
die Hintergrundsysteme sind gegenüber Zugriffen unbefugter Dritter abgesichert (d.h. kein Zugriff auf Backup-Systeme, Benutzerverwaltung, Datenprozessierungssysteme - dies gilt insbesondere für unverschlüsselte oder nicht unkenntliche gemachte datenschutzrelevante Daten)	erfüllt [ ] nicht erfüllt [ ]
Verfügbarkeit und Backup	
6:00 Uhr bis 19:00 Uhr mit einer Verfügbarkeit von mindestens 98 % (im Jahresmittel)	erfüllt [ ]
Es werden Backups angelegt, die den jeweils letzten Stand der Daten und des Benutzermanagements entsprechen; die Wiederherstellung des letzten Standes liegt innerhalb der definierten Gesamtverfügbarkeit	erfüllt [ ] nicht erfüllt [ ]
Zugriffskontrolle	
nur durch den Auftraggeber berechtigte Nutzer haben Zugriff auf bestimmte Inhalte anhand ihrer Rollen	erfüllt [ ] nicht erfüllt [ ]
ein Zugriff von Nutzern anderer Dienste auf dem Server / Server-Umfeld ist nicht möglich	erfüllt [ ] nicht erfüllt [ ]
der Auftraggeber hat den vollen Einfluss und die volle Transparenz, wer auf die Daten zugreifen darf und wer nicht	erfüllt [ ] nicht erfüllt [ ]

Die Server stehen in Deutschland oder der EU ODER in einem sicheren Drittstaat im Sinne des Bundesdatenschutzgesetzes, nämlich**:** _____	erfüllt [ ]
Kennwörter, die den Zugriff auf die Applikation bzw. deren Daten ermöglichen, werden nicht im Klartext gespeichert. Es wird ein Hash-Wert durch eine dem aktuellen Industriestandard entsprechende Hash-Funktion generiert.	erfüllt [ ] nicht erfüllt [ ]
Der Zugriff auf Hosting- / Cloud-Lösung des Auftragnehmers kann mittels IP-Adresse (IPv4 und IPv6) zusätzlich eingeschränkt werden	möglich [ ] nicht möglich [ ]
Nichtfunktionale Anforderungen	
eine aussagekräftige Systembeschreibung der Hosting- / Cloud-Lösung liegt bei	Ja [ ] Nein [ ]
die Hosting- / Cloud-Lösung wird unter Einbindung von einem oder mehreren Unterauftragnehmern / externen Dritten erbracht ***falls Ja*** • die Deklaration von Art und Umfang, sowie vollständige Nennung (inkl. Anschrift) der Dritten liegt bei • es wird zugesichert, dass alle erbrachten Leistungen ebenfalls die zuvor abgefragten Kriterien erfüllen	Ja [ ] Nein [ ] Ja [ ] Nein [ ] Ja [ ] Nein [ ]
Alle Vereinbarungen erfolgen ausschließlich nach deutschen Recht und deutschen Gerichtsstand und ohne obligatorisch vorab zu betreibende Schlichtungsverfahren.	Ja [ ] Nein [ ]

Der Auftragnehmer verpflichtet sich:

- fremd-staatliche Offenbarungspflichten und Ermittlungsbefugnisse offenzulegen
- sicherheitsrelevante Vorfälle (sowie ggf. andere Vorfälle) im Zusammenhang mit den von der LHM genutzten Hosting- / Cloud-Lösung der LHM zu melden
- eine Datenrückgabe und Datenlöschung bei Beendigung des Vertragsverhältnisses zu gewährleisten
- die Löschung aller Daten, einschließlich vorhandener Datensicherungen, zu bestätigen.

Unterschrift: _____