ANHANG I

Technische und organisatorische Maßnahmen, einschließlich zur Gewährleistung der Sicherheit der Daten

Beschreibung der von dem/den Verantwortlichen ergriffenen technischen und organisatorischen Sicherheitsmaßnahmen (einschließlich aller relevanten Zertifizierungen) zur Gewährleistung eines angemessenen Schutzniveaus unter Berücksichtigung der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen Beispiele für mögliche Maßnahmen:

Der Serverstandort der genutzten Auftragsdatenweiterverarbeitung durch die AWS ist Frankfurt am Main. Hier besteht eine BSI-Zertifizierung sowie erweiterte Zertifizierungen zur Sicherung der Daten durch TOM. Der Serverstandort der optional einsetzbaren Back-up-Speicherung ist Karlsruhe. Der Serverstandort der genutzten Auftragsdatenweiterverarbeitung durch die CRM ist Aachen. Hier besteht eine BSI-Zertifizierung sowie erweiterte Zertifizierungen zur Sicherung der Daten durch TOM. Darüber hinaus existiert eine Zugangsbeschränkung auf zwei Personen bezogen auf die Zugangsdaten zum Server.

Maßnahmen der Pseudonymisierung und Verschlüsselung personenbezogener Daten

Es werden die in der AWS sowie der CRM als standardisierte Tools angebotenen Pseudonymisierung und Verschlüsselungen für ruhende Daten und Datenabrufe eingesetzt.

Maßnahmen zur fortdauernden Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung

Es werden die in der AWS sowie der CRM als standardisierte Tools angebotene Überwachung und Konfiguration sowie Updates eingesetzt.

Maßnahmen zur Sicherstellung der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen

Es werden die in der AWS sowie des CRM als standardisierte Tools angebotenen Versionierungen und Datenwiederherstellungen eingesetzt. Zusätzlich besteht die Option eines Back-Ups bei einem weiteren Serverstandort in Karlsruhe.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Es werden regelmäßige Admin-Kontrollen der AWS-Config sowie der CRM Unterauftragsnehmer durchgeführt und es werden die Updates regelmäßig durchgeführt.

Maßnahmen zur Identifizierung und Autorisierung der Nutzer

Es wird ein double-opt-in-Verfahren zur Registrierung eingesetzt. Die AWS COGNITO bildet den Kern der Nutzerverwaltung mit den standardmäßigen Tools zur Passwortwiederherstellung.

Maßnahmen zum Schutz der Daten während der Übermittlung

Es werden die AWS und CRM standardisierten Sicherheitsprotokolle zum Datenabruf genutzt.

Maßnahmen zum Schutz der Daten während der Speicherung

Es werden die AWS und CRM standardisierten Sicherheitsprotokolle für ruhende Daten genutzt.

Maßnahmen zur Gewährleistung der physischen Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden

Der Zugriff auf die AWS CONFIG ist lediglich zwei Personen vorbehalten. Es werden außerhalb der AWS und CRM keine Daten vorgehalten.

Maßnahmen zur Gewährleistung der Protokollierung von Ereignissen

Es werden die standardmäßig in der AWS und CRM eingesetzten Protokolle eingesetzt und regelmäßig über Stichproben geprüft.

Maßnahmen zur Gewährleistung der Systemkonfiguration, einschließlich der Standardkonfiguration

Es werden die standardmäßig in der AWS eingesetzten Zugangsmöglichkeiten zur AWS CONFIG sowie der CRM eingesetzt und regelmäßig über Stichproben geprüft.

Maßnahmen für die interne Governance und Verwaltung der IT und der IT-Sicherheit

Es werden die standardmäßig in der AWS und CRM eingesetzten Standards eingesetzt und regelmäßig über Stichproben geprüft.

Maßnahmen zur Zertifizierung/Qualitätssicherung von Prozessen und Produkten

Es werden die standardmäßig in der AWS und CRM eingesetzten Protokolle eingesetzt und regelmäßig über Stichproben geprüft.

Maßnahmen zur Gewährleistung der Datenminimierung

Die Daten sind auf ein Minimum nach den beschriebenen Datenkategorien beschränkt.

Maßnahmen zur Gewährleistung der Datenqualität

Die Datenqualität der erhobenen Daten wird durch das double-opt-in-Verfahren gewährleistet.

Maßnahmen zur Gewährleistung einer begrenzten Vorratsdatenspeicherung

Die Daten sind auf ein Minimum nach den beschriebenen Datenkategorien beschränkt.

Maßnahmen zur Gewährleistung der Rechenschaftspflicht

Durch den Einsatz der AWS COGNITO ist die Benutzerverwaltung über die AWS-Konsole den beiden zugangsberechtigten Mitarbeitern gewährleistet. Innerhalb des CRM sind lediglich legitimierte Leserechte für Mitarbeiter eingerichtet.

Maßnahmen zur Ermöglichung der Datenübertragbarkeit und zur Gewährleistung der Löschung

Durch den Einsatz der AWS COGNITO ist die Benutzerverwaltung über die AWS-Konsole den beiden zugangsberechtigten Mitarbeitern gewährleistet. Das CRM der CRM ist lediglich angebunden und diese Daten werden über AWS COGNITO in CRM synchronisiert.

Bei Datenübermittlungen an (Unter-)Auftragsverarbeiter sind auch die spezifischen technischen und organisatorischen Maßnahmen zu beschreiben, die der (Unter-)Auftragsverarbeiter zur Unterstützung des Verantwortlichen ergreifen muss.

Durch den Einsatz der Registrierung ausschließlich auf der AWS und deren Benutzerverwaltung entfällt dieser Punkt.

ANHANG II

Liste der **Unterauftragsverarbeiter**

ERLÄUTERUNG:

Dieser Anhang muss im Falle einer gesonderten Genehmigung von Unterauftragsverarbeitern ausgefüllt werden (Klausel 10 – Anhang III).

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

1. Amazon Web Services EMEA SARL (Hosting)
2. IONOS SE (Domain-Management und *optionales* Back-up Hosting)
3. Geno Portaltechnologie GmbH (Admin des Hosting)
4. Spacedatists GmbH (Expertenbüro, Beratung und Digitalisierung)
5. onOffice GmbH (Admin des CRM)
6. twenty.com PBC (*optionales* CRM für Expertenbüros – Hosting in Frankfurt am Main)

Beschreibung der Verarbeitung (einschließlich einer klaren Abgrenzung der Verantwortlichkeiten, falls mehrere Unterauftragsverarbeiter genehmigt werden):

https://aws.amazon.com/de/compliance/iso-certified/
https://cloud.ionos.de/datensicherheit
https://www.xplanung24.de/datenschutz/
https://onoffice.com/datenschutz/
https://twenty.com/privacy-policy/

ANHANG III

Zusatzoffenlegung in Anlehnung an **EVB-IT**

1-Ort der Cloudleistungen

1.1 Der Auftragnehmer hostet die Daten in Frankfurt am Main.

1.2 Generell gilt: Die Speicherung und sonstige Verarbeitung von Daten des Auftraggebers durch den Auftragnehmer erfolgt ausschließlich innerhalb der EU und des EWR sowie, sofern ein Angemessenheitsbeschluss gem. Art. 45 DSGVO besteht, der Schweiz. Die Verarbeitung von Metadaten im Sinne des Anforderungskataloges C 5 ist unabhängig von Satz 1 nach dessen Maßgabe möglich, soweit die dort geforderten Maßnahmen zur sicheren Handhabung der Metadaten tatsächlich umgesetzt sind; für personenbezogene Metadaten gelten die Regelungen zur Verarbeitung personenbezogener Daten vorrangig.

2-Zugriff / Speicherplatz

2.1 Der Zugriff auf das Portal erfolgt über das öffentliche Internet mit einem marktüblichen Web-Browser ohne unangemessene oder marktunübliche Browser-Einstellungen und ohne spezielle Zugriffssoftware.

Der Übergabepunkt ist das Gateway des Rechenzentrums des Auftragnehmers in das Internet.

2.2 Der Auftragnehmer ist verpflichtet, den Zugriff auf die Daten des Auftraggebers durch unberechtigte Stellen und Personen mit angemessenen Maßnahmen zu verhindern.

3-Datenschutz

3.1 Die Parteien werden die bei der Erbringung der Leistung jeweils auf sie anwendbaren Bestimmungen über den Datenschutz in der jeweils geltenden Fassung einhalten. Der Auftragnehmer verfügt über eine hinreichende Dokumentation über die Umsetzung der gesetzlichen Anforderungen, die der Auftragnehmer dem Auftraggeber auf Anforderung zugänglich macht.

3.2 Der Auftragnehmer sorgt dafür, dass alle Personen, die von ihm mit der Verarbeitung personenbezogener Daten des Auftraggebers betraut sind, die auf den Auftragnehmer anwendbaren Bestimmungen über den Datenschutz beachten. Soweit eine Verpflichtung auf das Datengeheimnis erforderlich ist, ist diese spätestens vor der erstmaligen Aufnahme der Tätigkeit vorzunehmen und dem Auftraggeber auf Verlangen vorzulegen.

4-IT-Sicherheit

4.1 Der Auftragnehmer verfügt über ein angemessenes und dokumentiertes Sicherheitskonzept einschließlich Notfall-Management.

4.2 Das vom Auftragnehmer mit der Bereitstellung der Rechenzentrumsleistungen unterbeauftragte Unternehmen muss nach ISO 27001 zertifiziert sein. Dessen Sicherheitskonzept hat sich nach ISO 27017 und bei der Verarbeitung personenbezogener Daten nach ISO 27018 auszurichten.

5-Vertraulichkeit

5.1 Die Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten vertraulichen Informationen, Geschäfts- und Betriebsgeheimnisse vertraulich zu behandeln, insbesondere nicht an unberechtigte Dritte weiterzugeben oder anders als zu vertraglichen Zwecken zu verwerten. Die vorgenannte Pflicht zur Vertraulichkeit schränkt jedoch keine Partei darin ein, für sie tätige Personen, die Zugang zu vertraulichen Informationen hatten, in anderen Projekten einzusetzen.

5.2 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. Vertrauliche Informationen dürfen ausschließlich zum Zweck der Erfüllung der Verpflichtungen aus dem Vertrag eingesetzt bzw. verwertet 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-Datensicherung

6.1 Der Auftragnehmer ist zur regelmäßigen Sicherung der Daten des Auftraggebers verpflichtet.

6.2 Der Auftragnehmer ist verpflichtet, auf Anforderung des Auftraggebers in angemessener Frist eine Wiederherstellung von Dateien aus einem Backup auf den vom Auftraggeber gewünschten vorhandenen Stand vorzunehmen.

7-Verfügbarkeit

7.1 Der Auftragnehmer schuldet die vereinbarte Verfügbarkeit der Leistung am geschuldeten Übergabepunkt unter Verwendung des vereinbarten Zugriffs während der Betriebszeit.

7.2 Zeiten der geplanten Nichtverfügbarkeit mindern die Verfügbarkeit nicht.

7.3 Bezüglich der Verfügbarkeit gilt Folgendes:

o Probleme innerhalb des Netzwerks oder der Infrastruktur des Auftraggebers oder von vom Auftraggeber beauftragten Dritten,

o Ausfall/Beeinträchtigung der Netzanbindung des Auftraggebers,

o Ausfälle/Beeinträchtigungen, die auf Fehlern der Vertragssoftware oder dem Handeln oder Unterlassen des Auftraggebers oder eines nicht vom Auftragnehmer beauftragten Dritten beruhen, einschließlich der der mangelhaften Pflege der Vertragssoftware,

o nicht vertragsgemäße Nutzung der Leistung des Auftragnehmers durch den Auftraggeber,

Betriebszeit die Zeit von Montag bis Sonntag von 0:00 bis 24:00 Uhr (MEZ bzw. MESZ).

Der Prozentsatz der Verfügbarkeit wird nach folgender Formel berechnet:

Die Gesamtzeit Minuten ergibt sich aus der vereinbarten Betriebszeit je Kalendermonat. Ausfallzeit sind diejenigen Minuten, an denen der Auftraggeber innerhalb der Betriebszeiten keine Konnektivität zu der vom Auftragnehmer bereit zu stellende Cloudinfrastruktur herstellen kann oder die betroffene Leistung insgesamt nicht oder nicht in allen ihren wesentlichen Grundfunktionalitäten für mehr als einen unwesentlichen Teil der Nutzer zur Verfügung steht.

- Der Auftragnehmer schuldet während der Betriebszeit eine Verfügbarkeit von mindestens der Verfügbarkeitsklasse VK0 im Bezugszeitraum (Mindestverfügbarkeit: 95,0 %; Ausfallzeit pro Monat: < 37h; Ausfallzeit pro Jahr < 438h).
- Bezugszeitraum ist der Kalendermonat.
- Die Zeit von 04:00 Uhr bis 08.00 Uhr ist an Sonntag Zeit geplanter Nichtverfügbarkeit (z.B. für Wartungsarbeiten) und wird bei der Berechnung der Verfügbarkeit nicht berücksichtigt.
- Ausfallzeiten, die auf einem der folgenden Ereignisse beruhen, mindern die Verfügbarkeit nicht:

o Versäumnisse des Auftraggebers, vereinbarte Vorgaben zu erforderlichen Konfigurationen und Architekturen einzuhalten sowie fehlerhafte Eingaben beziehungsweise Anweisungen durch Nutzer des Auftraggebers,

o Handlungen nicht autorisierter Nutzer, soweit die Handlungsmöglichkeit des nicht autorisierten Nutzers dem Auftraggeber zuzurechnen ist (bspw. durch die Nichtbeachtung angemessener Sicherheitsverfahren),

o Aussetzen des Zugangs durch einen Sicherheitsvorfall zum Schutz auch des Auftraggebers,

o Ereignisse, die auf höherer Gewalt beruhen und nicht durch angemessene Maßnahmen des Auftragnehmers kompensiert werden können.

Der Auftragnehmer misst die Verfügbarkeit.

8-Störungsklassifizierung

8.1 Eine **schwerwiegende Störung** liegt vor, wenn für mehr als einen unwesentlichen Teil der vom Auftraggeber vertragsgemäß berechtigten Nutzer die Nutzung der betroffenen Leistung insgesamt oder in wesentlichen Funktionen unmöglich oder schwerwiegend eingeschränkt ist.

8.2 Eine **erhebliche Störung** liegt vor, wenn die Nutzung der betroffenen Leistung erheblich eingeschränkt ist. Eine erhebliche Störung liegt auch vor, wenn die leichten Störungen

insgesamt zu einer nicht unerheblichen Einschränkung der Nutzung der betroffenen Leistung führen.

8.3 Eine **leichte Störung** liegt vor, wenn die Nutzung der betroffenen Leistung ohne oder mit unwesentlichen Einschränkungen möglich ist.

9-Störungsbeseitigung

9.1 Im Störungsfall hat der Auftragnehmer alle zur Wiederherstellung der Betriebsbereitschaft notwendigen Maßnahmen zu ergreifen. Liegt die Ursache der Störung in einem Fehler der Vertragssoftware, wird der Auftragnehmer den Auftraggeber entsprechend informieren.

9.2 Mit der Störungsbeseitigung wird der Auftragnehmer unverzüglich nach Eingang einer entsprechenden Meldung beginnen. Die Störungsbeseitigung ist innerhalb angemessener Frist abzuschließen.

10-Unterauftragnehmer

10.1 Der Auftragnehmer darf zur Leistungserbringung Unterauftragnehmer nur einsetzen oder eingesetzte Unterauftragnehmer nur auswechseln, wenn der Auftragnehmer den bzw. die Unterauftragnehmer und deren jeweiligen Leistungsbereich (Art und Umfang der Auslagerung an den Unterauftragnehmer) benennt. Die Benennung kann entfallen, wenn es sich nur um Zulieferer oder solche Unternehmen handelt, die lediglich Nebenleistungen erbringen.

10.2 Voraussetzung für den Einsatz eines Unterauftragnehmers ist, dass dieser sich, soweit dies seine Leistungen betrifft, zuvor dem Auftragnehmer gegenüber mindestens einem seinem jeweiligen Anteil an der Leistungserbringung entsprechenden Umfang zur Einhaltung der vertraglichen Regelungen verpflichtet hat, wie der Auftragnehmer gegenüber dem Auftraggeber.

Unterauftragnehmer in diesem Sinne sind auch solche, die wiederum von Unterauftragnehmern eingesetzt werden (Unterauftragnehmerkette).

Die Einbindungen von Amazon Web Services EMEA SARL, IONOS SE, Geno Portaltechnologie GmbH, Spacedatists GmbH, onOffice GmbH und twenty.com PBC sind dem Auftraggeber bekannt.

Der Auftragnehmer darf vertrauliche Informationen nur an solche Unterauftragnehmer weitergeben, deren Einsatz der Auftraggeber nicht ausdrücklich widersprochen hat und nur wenn und soweit diese vertraulichen Informationen für die Erbringung der jeweiligen Leistungen durch den Unterauftragnehmer erforderlich sind („Need-to-know“-Prinzip) und der Unterauftragnehmer mindestens im gleichen Maße zur Vertraulichkeit verpflichtet ist wie der Auftragnehmer.