Anhang 1 zur Vereinbarung über die Einhaltung datenschutzrechtlicher Bestimmungen

Sicherheitskonzept des Auftragnehmers: Technische und organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)	
Zutrittskontrolle	- Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen. - Der Zugang zur Agentur ist nur mit Schlüssel möglich. Die Schlüsselvergabe zu den Geschäftsräumen wird kontrolliert und protokolliert. - Der Auftragnehmer gewährt nur befugten Personen Zugang zu den Geschäftsräumen, Unbefugten ist der Zutritt verwehrt. - Es existiert ein Gebäude- und Objektschutz. - Keine weiteren Mieter und Nutzer der Geschäftsräume. - Gesonderter Kundenbereich, Wartezone und Besprechungsräume sind vorhanden, eine Einsicht auf Bildschirme ist nicht möglich. - Schutzbedürftige Räumlichkeiten sind verschlossen und nur befugten Personen zugänglich, der Aufenthalt wird protokolliert: ▪ Serverraum ▪ USV-Anlage (Kaltstrom, im Serverraum) ▪ TK-Anlage (im Serverraum)
Zugangskontrolle	- Keine unbefugte Systemnutzung z.B. durch Kennwortschutz, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern. - Authentifikation von befugten Benutzern durch Benutzername und Passwort. - Für die Vergabe von Passwörtern wird eine nach Empfehlung BSI IT-Grundschutz entwickelte Passwortrichtlinie eingesetzt: ▪ Mindestlänge 8 Zeichen (Administratoren 12 Zeichen) ▪ Ausschluss von Trivialkennworten ▪ Unterbindung der Verwendung von bisherigen Passwörtern (5 Generationen) ▪ Verwendung von Klein-/Großbuchstaben ▪ Verwendung von Zahlen/Ziffern ▪ Verwendung von Sonderzeichen ▪ Gültigkeitsdauer 90 Tage ▪ Mindestgültigkeitsdauer 1 Tag ▪ 60-minütige Sperrung von Benutzer-Kontos nach 3 ungültigen - Schutz der Berechtigungs- und Passworttabellen durch Verschlüsselung - Passwortgeschützter Bildschirmschoner - Anforderung der Benutzerkennung nach 5 Minuten Abwesenheit der angemeldeten Benutzer
Zugriffskontrolle	- Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen - Differenzierte Berechtigungsvergabe nach Lesen, Schreibung und Löschen - Protokollierung von Zugriffen: ▪ An- / Abmeldung

	▪ Shell-Zugriff - Auswertung der Protokollierung - Administration erfolgt durch zentrale Person und deren Vertretung - Rechte zur Selbstadministration nur für Administratoren - Virenschutz mit automatischer Aktualisierung der Signaturdatenbank - Regelmäßige und bedarfsmäßige Aktualisierung der eingesetzten Betriebssysteme und Anwendungen
Trennungskontrolle	- Logische Trennung personenbezogener Daten wird gewährleistet: ▪ Mandantentrennung innerhalb von Anwendungen ▪ Trennung der Anwendungen ▪ Trennung von Datenbanken ▪ Trennung von Heimverzeichnissen - Physikalische Trennung personenbezogener Daten durch: ▪ Trennung der Hostings ▪ Trennung von Entwicklungs-, Test- und Produktivsystemen
Pseudonymisierung	- wenn Pseudonymisierung eingesetzt wird: ▪ gemäß Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO ▪ Trennung von Zuordnungsdaten und Aufbewahrung in separaten Systemen ▪ ggf. Einsatz von Verschlüsselung

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)	
Weitergabekontrolle	- kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur - Verhinderung der Weitergabe personenbezogener Daten bzw. Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträgern: ▪ kein Einsatz, Versand und Transport von mobilen Datenträgern ▪ durch verschlossenen Schrank gesicherte Aufbewahrung von intern verwendeten mobilen Datenträgern ▪ keine automatische Datenübertragung personenbezogener Daten
Eingabekontrolle	- Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement - Protokollierung von: ▪ Datensätzen ▪ Datenfeldern - Aus der Protokollierung ist erkennbar, welche Daten: ▪ eingegeben wurden ▪ verändert wurden ▪ entfernt wurden

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)	
Verfügbarkeitskontrolle	- Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust: ▪ tägliche Voll-Backups ▪ externe Auslagerung der Sicherheitskopien

	▪ Gewährleistung der Aktualität von Sicherheitskopien (Katastrophensicherung) ▪ USV-Anlage vorhanden ▪ keine Brandlasten im Serverraum ▪ Betriebs- und Sicherheitskonzept ist vorhanden
	- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO): ▪ Ständige Spiegelung der Festplatten ▪ Notfallkonzept ist vorhanden
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)	
	- Datenschutz-Management - Incident-Response-Management - Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)
Auftragskontrolle	- ohne entsprechende Weisung des Auftraggebers erfolgt keine Auftragsverarbeitung im Sinne von Art. 28 DSGVO - eindeutige Vertragsgestaltung - formalisiertes Auftragsmanagement - Vorabüberzeugungspflicht - Unterauftragsverhältnisse ausschließlich mit schriftlicher Genehmigung des Auftraggebers - Meldung jeglicher Datenschutzrelevanter Änderungen an den Auftraggeber - Incident-Response-Management

Anhang 2 zur Vereinbarung über die Einhaltung datenschutzrechtlicher Bestimmungen

Verzeichnis zu Standorten der Geschäftsräume des Auftragnehmers

Aus der Übersicht sollen alle Standorte über die Geschäftsräume des Auftragnehmers hervorgehen, welche für die Erhebung, Verarbeitung und Nutzung der Sozialdaten des Auftraggebers im Rahmen des vereinbarten Auftragsverhältnisses genutzt werden.

Standort	**Postalische Anschrift**	**Telefon, Fax, E-Mail**
Geschäftsräume	zone35 GmbH & Co. KG Wilhelmstr. 118 10963 Berlin Aufgang A, 4. OG	Telefon: 030 440136 – 0 Fax: 030 440136 – 13 E-Mail: info@zone35.de

Anhang 3 zur Vereinbarung über die Einhaltung datenschutzrechtlicher Bestimmungen

Verzeichnis zu Unterauftragnehmern

Aus der Übersicht sollen alle Unterauftragnehmer des Auftragnehmers hervorgehen, welche für die Erhebung, Verarbeitung und Nutzung der Sozialdaten des Auftraggebers und der hierzu für die Wartung der eingesetzten automatisierten Verfahren und Datenverarbeitungsanlagen im Rahmen des vereinbarten Auftragsverhältnisses eingesetzt werden.

Unterauftragnehmer:	Michael Krockor ITK-Informations Technologie Krockor
Anschrift:	ITK-Informations Technologie Krockor Inh. Michael Krockor Max-Beckmann-Str. 21 04109 Leipzig
Aufgabenfeld:	Wartung Server
Zeitraum:	seit 01.09.2014

Unterauftragnehmer:	Hetzner Online GmbH
Anschrift:	Industriestr. 25 91710 Gunzenhausen
Aufgabenfeld:	Serverhosting
Zeitraum:	seit 01.10.2020

Unterauftragnehmer:	Strato AG
Anschrift:	Pascalstraße 10 10587 Berlin
Aufgabenfeld:	Serverhosting Hosting Backup-Storage
Zeitraum:	seit 13.07.2010

Anhang 4: Ansprechpartner

1) Ansprechpartner des Auftraggebers ist/sind:

Fachliche Zuständigkeit	
Name, Vorname:	
Funktionsbezeichnung:	
Erreichbarkeit:	

Datenschutzbeauftragter	
Name, Vorname:	
Funktionsbezeichnung:	
Erreichbarkeit:	

2) Ansprechpartner des Auftragnehmers sind:

Fachliche Zuständigkeit	
Name, Vorname:	Ort, Maximilian
Funktionsbezeichnung:	Teamleitung E-Beratung
Erreichbarkeit:	Telefon: 030 440136 – 17 / E-Mail: maximilian.ort@zone35.de

Fachliche Zuständigkeit	
Name, Vorname:	Wimmer, Andreas
Funktionsbezeichnung:	Geschäftsführung

Datenschutzbeauftragter	
Name, Vorname:	DSB Externer Datenschutzbeauftragter Stuttgart / Henkel, Fabian
Funktionsbezeichnung:	Externer Datenschutzbeauftragter
Erreichbarkeit:	Telefon: 0049 7152 564 773 / E-Mail: info@externer-datenschutzbeauftragter-stuttgart.de

Anhang 5: Beschreibung der Betroffenen/Betroffenengruppen und der besonders schutzbedürftigen Daten/Datenkategorien (Standardprodukte)

assisto Web/Messenger	
Personenbezogene Daten	- E-Mail-Adresse - IP-Adresse (anonymisiert) - Pseudonym - Benutzerprofil - Profilbild - Vorname/Name der Beratenden
Betroffene Personen:	- Interessierte/Besucher der Online-Plattformen - Ratsuchende des Auftraggebers - Beratende des Auftraggebers

Löschfristen	- Nutzerdaten und alle weiteren personenbezogene Daten werden anhand der Einstellung des Autolösch-Intervalls behandelt. Alle personenbezogenen Daten werden anhand der durch den Auftraggeber eingestellten Löschfrist unwiderruflich und sofort gelöscht, wenn die verknüpften Nutzerdaten länger als in der Löschfrist definiert inaktiv waren oder durch Beratende oder die Nutzer selbst zur Löschung markiert wurden. - Für die Sicherung der Wiederherstellbarkeit werden regelmäßige Backups erstellt. Die Löschfristen für Backup-Dateien sind mit 7 Tagen definiert. Backups werden nach Erreichen der Löschfrist sofort und unwiderruflich gelöscht. Eine weitere Spiegelung der Daten wird nicht vorgenommen. - Bei Vertragsende oder auf Verlangen des Auftraggebers werden alle Nutzerdaten oder anderweitig verarbeiteten personenbezogene Daten des Auftraggebers an den Auftraggeber übergeben, wenn dieser die Daten zurückverlangt. Nach Ablauf der durch den Auftraggeber definierten Löschfristen werden die Daten anschließend unwiderruflich gelöscht. Backups der Daten werden nach Vertragsende für 7 Tage vorgehalten, bevor diese und alle darin enthaltenen Nutzerdaten unwiderruflich gelöscht werden.

assisto Video	
Personenbezogene Daten	- IP-Adresse (anonymisiert) - keine weiteren Daten
Betroffene Personen:	- Interessierte/Besucher der Online-Plattformen - Ratsuchende des Auftraggebers - Beratende des Auftraggebers
Löschfristen	- Es erfolgt keine Speicherung von Personen-, Nutzungs- oder Videodaten. - System-Backups enthalten ausschließlich Anwendungsdaten. - Protokolldateien werden für 7 Tage vorgehalten (Log-Rotation).