Anlage 1:

Auftragsverarbeitung zum Einzelabruf und technisch-organisatorische Maßnahmen

betreffend die OZG-Verwaltungsleistung:

„App Ehrenamtskarte NRW und des Verwaltungsprogramms EAK NRW“

(OZG-Leistung: Förderung ehrenamtlicher Tätigkeit)

Zwischen dem Auftraggeber (Leistungsbezieher) und dem Auftragnehmer (Leistungserbringer, Kommunalvertreter) wird mit Vertragsschluss des Einzelabrufs die die folgende Einzel-Auftragsverarbeitungsvereinbarung (nachstehend „**Einzel-AV**“) zum Einzelabruf betreffend die OZG-Verwaltungsleistung „Förderung ehrenamtlicher Tätigkeit“ als Anlage 1 (nachstehend „**Einzelabruf**“) geschlossen.

Präambel
Diese Einzel-AV regelt auf Grundlage der zwischen den Vertragsparteien zu Rahmenvereinbarung zur Nachnutzung von OZG-Verwaltungsleistungen über den Kommunalvertreter/öffentlicher IT-Dienstleister geschlossenen Rahmenvereinbarung zur Auftragsverarbeitung (nachstehend „**Rahmen-AV**“) die Einzelheiten der Datenverarbeitung im Zusammenhang mit dem Einzelabruf „„App Ehrenamtskarte NRW und des Verwaltungsprogramms EAK NRW““.

1 OZG-Verwaltungsleistungs-spezifische Zwecke, Betroffene und Datenkategorien
Der Auftragnehmer verarbeitet im Rahmen der OZG-Verwaltungsleistung „Förderung ehrenamtlicher Tätigkeit“ die folgenden personenbezogenen Daten:

- Vor- und Nachname
- Anschrift
- Geburtsdatum
- Telefonnummer
- E-Mailadresse

I. Zwecke

Erhebung und weitere Verarbeitung personenbezogener Daten zur Beantragung einer Ehrenamtskarte NRW, durch die App „Ehrenamtskarte NRW“ und zur Verarbeitung durch das „Verwaltungsprogramm EAK NRW“

II. Betroffene

Antragstellerinnen und Antragsteller, Verfügungsberechtigte oder Nutzungsberechtigte.

III. Datenkategorien

Die erhobenen Daten gehören zu keiner der nach der DSGVO besonders geschützten Datenkategorien.

2 Technische und organisatorische Maßnahmen (TOM)

Für die Bereitstellung der App Ehrenamtskarten NRW und des Verwaltungsprogramms EAK NRW wurde die regio iT durch den Auftragnehmer beauftragt. Die technischen und organisatorischen Maßnahmen gestalten sich wie folgt:

Die TOM der regio iT teilen sich in die Bereiche A und B.

Teil A: Datenschutzspezifische TOM

Umsetzung der Anforderungen der DSGVO durch den Datenverarbeiter; insb. zu Datenschutzprinzipien (Art. 5) und Data protection by design and by default (Art. 25).

Maßnahmen/Anforderung	Umsetzungsdetails
Zweckbindung **Generelle Maßnahmen** − Wahrung der zweckgebundenen Verarbeitung (Festlegungen, Verpflichtungen, etc.) **Produktspezifischen Maßnahmen**[1] − Möglichkeit zur Deaktivierung nicht-benötigter / nicht-relevanter Datenfelder und Bearbeitungsfunktionen. − Übersicht von Tabellen und Datumsfelder auf Anfrage	− Verpflichtung der Mitarbeiter zur „Arbeit auf Weisung“ und zur Vertraulichkeit − Vereinbarung zur (ausschließlichen dienstlichen) Nutzung dienstlicher Daten und Assets
Rechtmäßigkeit der Verarbeitung **Generelle Maßnahmen** − Führung von Nachweisen zur weisungsgebundenen Arbeit − Abschluss von Verträgen mit Kunden und Verpflichtungen von Externen **Produktspezifischen Maßnahmen** − Umsetzung des Option Grundsatzes (explizite Zustimmung zur Verarbeitung durch Betroffenen) − Datenschutzkonforme Umsetzung der Einwilligungsregelung sowie Widerspruch	− Ticketsystem; Jira-Aufgabensteuerung − Vertrags- und Verpflichtungsdokumentation in SAP VMS
Datenminimierung **Generelle Maßnahmen** − Sicherstellung der Datenminimierung **Produktspezifischen Maßnahmen** − Möglichkeit der Deklaration von Pflicht- und Bedarfseingaben für alle Datenfelder − Übersicht von Tabellen und Datumsfelder auf Anfrage − Möglichkeit zur Deaktivierung nicht-benö-tigter / nicht-relevanter Datenfelder und Bearbeitungsfunktionen	- Festlegungen zum Umfang der Datenerhebung in Kundenprozessen

Speicherbegrenzung **Generelle Maßnahmen** - Umsetzung des datenschutzkonformen Löschens und Entsorgen von Datenträgern, Medien und Dokumenten auf Basis des Löschkonzepts des Verantwortlichen **Produktspezifischen Maßnahmen** − Bereitstellung der Möglichkeit zur Konfiguration von Sperr-, Lösch-, Pseudonymisierungs und Anonymisierungskennzeichnung, -dauern und -fristen pro Datum	− Papiershredder an zentralen Abteilungsstellen − Löschung mittels BSI konformen Löschprogrammen − Entsorgung von Datenträgern gem. DIN 66399 durch zertifiziertes Unternehmen
Integrität **Generelle Maßnahmen** − Berücksichtigung der Anforderungen an Mandantenfähigkeit − Möglichkeit zur Konfiguration des Logging auf externen Systemen − Revisionssichere Archivierung je nach Weisung des Auftraggebers − Geregelte Transportwege von Datensicherungsbändern **Produktspezifischen Maßnahmen** − Regelmäßige und ad-hoc-Tests bei Programmänderungen − Tests bei Programmänderungen auf Basis von "Standard-Prozeduren" − Konfigurationsmöglichkeit unterschiedlicher "Protokolltiefen" sowie Kopplung der Protokollierung an das Rechte/Rollenkonzept	− Berücksichtigung OH zu Mandantenfähigkeit − Abgestufte Berechtigungs-konzepte − Externes Syslogsystem − Archivierung gem. vertraglicher Vereinbarung − Mit den Kunden vereinbarte Transportwege von Datensicherungsbändern
Vertraulichkeit **Generelle Maßnahmen** − Möglichkeit zur Rechtesteuerung auf Nutzer/Administrationsebene bzw. auf Ebene von (kritischen) Funktionen oder Konfigurationseinstellungen − Verwendung gesicherter Kommunikationsschnittstellen − Verpflichtung aller MA und Externer auf Vertraulichkeit und Weisungsgebundenheit der Tätigkeiten − Schulung und Sensibilisierung aller Mitarbeiter − Methoden und organisatorische Regelungen zur Sicherung der Arbeitsplätze wie Clear-Desk etc. **Produktspezifischen Maßnahmen** − Konfigurationsmöglichkeit unterschiedlicher "Protokolltiefen" sowie Kopplung der Protokollierung an das Rechte/Rollenkonzept	- Details gem. TOM Liste
Rechenschaftspflicht **Generelle Maßnahmen**	− Definition und Betrieb eines DSMS (policies und Daten-schutzhandbuch)

- Nachweis zur Umsetzung eines Daten-schutz-Managementsystems - Ggf. Zertifizierung nach ISO 27001, BSI Grundschutz oder vergleichbar - Vertragliche Festlegungen zu Art, Umfang und Umsetzung der Auftragsverarbeitung mit Unterauftragnehmern - Generelle Übersicht über die technischen und organisatorischen Maßnahmen Produktspezifischen Maßnahmen1 - Integrative Beschreibung der Datenschutzmaßnahmen als Bestandteil der Programmdokumentation - Möglichkeit zur online-Beantragung von Betroffenenrechten	Integration des Datenschutzmanagementsystems im zertifizierten IMS (Integrierten Managementsystem) − Dokumentation von Prozessen, Richtlinien und Vorgaben zum Datenschutz sowie Berücksichtigung DS-relevanter Aspekte in allen Prozessen (im IMS) − Prüfung DS Wirksamkeit durch interne Audits − Nachweisbare regelmäßige Schulung aller Mitarbeiter − Prüfung und Abschluss vertraglicher Festlegungen/Re-gelungen mit Unterauftragsverarbeitern − Vertrags- und Verpflichtungsdokumentation in SAP VMS
<u>Transparenz</u> **Generelle Maßnahmen** - Definition von Verarbeitungskategorien - Führung von Verzeichnissen der Verarbeitungskategorien **Produktspezifischen Maßnahmen** - Möglichkeit zur Information	- Umsetzung als Ergänzung zu SLA und Leistungsscheinen - Führen des VVT-AV (Verzeichnis der Verarbeitungs-kategorien)
<u>Betroffenenrechte</u> **Generelle Maßnahmen** - Unterstützung des Verantwortlichen zur Umsetzung der Betroffenenrechte gem. vertraglicher Festlegungen **Produktspezifischen Maßnahmen** - Möglichkeit zur Bereitstellung von Formularen, links oder sonstigen strukturierten Erfassungen der Betroffenenanfragen	- Prozess zur Erfassung, Steuerung und Dokumentation von Anfragen
<u>Data protection by design and by default</u> **Generelle Maßnahmen** - Umsetzung der Datenschutzprinzipien - Sicherstellung der Prüfmöglichkeit zu DS Maßnahmen durch Audits - Bereitstellung TOM Liste **Produktspezifischen Maßnahmen** - siehe Datenschutzprinzipien	- Integration Datenschutz(DS) in die Informationssicherheits-Prozesse auf Basis nationaler und internationaler Standards und Empfeh-lungen2 - Prüfung und Beachtung des DS in Projekten - Prüfungsmöglichkeit DS Konformität zu SW-Produkten in Beschaffungen / Projekten - Erfassung und Prüfung spezifischer Datenschutzanforderungen und -Maßnahmen in Kundenprozessen
<u>Verarbeitung unter Aufsicht</u> **Generelle Maßnahmen** - Nachweisliche Verpflichtung von Mitarbeitern und Externen - Nachweisliche Schulung der Mitarbeiter **Produktspezifischen Maßnahmen**	- Siehe Datenschutzprinzipien

keine	
Sicherheit der Verarbeitung **Generelle Maßnahmen** - Definition von Maßnahmen in strukturierten und dokumentierten Prozessen - Regelmäßige Kontrolle der Wirksamkeit und Angemessenheit von Maßnahmen **Produktspezifischen Maßnahmen** keine	- Zertifizierung nach ISO 27001 - Regelmäßige Prüfung in in-ternen und externen Audits - Details in „sicherheitsspezifischen TOM“
Meldung von Datenschutzverletzungen **Generelle Maßnahmen** - Nachweis zur Erfassung von Datenschutz-verletzungen - Meldung von DS Verletzungen an kunden-definierte Kontaktstellen - Ggf. Umsetzung von Sofortmaßnahmen Unterstützung der Verantwortlichen zur Dokumentation von DS-Verletzungen gem. vertraglicher Regelungen **Produktspezifischen Maßnahmen** keine	- Integration Prozess zu DS-Verletzungen in Sicherheitsereignisprozess - Merkblatt für MA zum Ver-halten bei DS Verletzungen - Entwicklung von DS-Responseplänen (Sofortmaßnahmen)
Datenschutzbeauftragter **Generelle Maßnahmen** - Ernennung einer/s Datenschutzbeauftragten **Produktspezifischen Maßnahmen** Keine	- Rollendefinition und -besetzung zu Datenschutzbeauftragten in Stabsstelle

Teil B: TOM zur (Informations-) Sicherheit

u. a. Sicherheit der Verarbeitung (Art. 32)

Grundlage	Maßnahmen/Anforderungen
Verschlüsselung von Daten	**Generelle Maßnahmen** − Verschlüsselung • Verschlüsselungen von Daten auf Datenhaltungssystemen erfolgen gemäß als sicher anerkannter Verfahren und Schlüssellängen, entsprechend den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnologie (BSI)

Vertraulichkeit	**Generelle Maßnahmen** − Zutrittskontrolle • Technische Maßnahmen wie Einfriedung, Video-Überwachung, Einbruchmeldeanlage • Organisatorische Maßnahmen wie Pfortenfunktion, Wachdienst, Begleitung Externer, etc. • Elektronische und mechanische Zutrittskontrollsysteme in Verbindung mit Berechtigungskonzepten (RBAC-Rule based access control), Registrierungen, Protokollierungen, Auditierungen, Verpflichtungen und Begleitung Externer, etc. − Zugangskontrolle • Prozessorientierte Identity und Access Management Methoden mittels Verzeichnisdienste in Verbindung mit Passwortkonvention • Einsatz unterschiedlicher Authentisierungs- und Autorisierungsmethoden bei Netzzugängen • Multifaktor-Authentisierung bei kritischen / sensiblen Systemen • Technische Methoden zur Erkennung, Vermeidung und Protokollierung unberechtigter Zugangsversuche mittels sog. Intrusion Detection /- Prevention Systeme − Zugriffskontrolle • Organisatorische/personelle Methoden wie Verpflichtungen (Daten-schutz, Fernmeldegeheimnis, etc.), Unterweisungen, Protokollierungen, etc. • Technische Methoden zur Detektion und Vermeidung unberechtigter Zugriffsversuche, Malware-Erkennung • Berechtigungs- und Rollenkonzept • Sichere Löschung / Entsorgung von Datenträgern − Weiteres • regelmäßige Schulung u. Sensibilisierung der Mitarbeiter • physikalische u. logische Trennung von Systemen und Netzes • Betriebsprozesse nach best-practice Empfehlungen und Standards (ISO 20000) • Einsatz aktueller Schadware-Schutzsysteme • Sichere Netzzugangs- und Kommunikationstechnologien wie VPN (mittels IPsec oder SSL/TLS), verschlüsselte Datenübertragungen, remote access, • Begrüßung, Registrierung, Begleitung und Verabschiedung von Externen
Integrität	**Generelle Maßnahmen** − Protokollierung benutzer- und systembezogener Aktivitäten sofern erforderlich − Einheitlicher Systemzeitabgleich − Schutz von Web-Systemen (z.B: Einhaltung OWASP, Web-Appliction Firewall u.ä.) − System Monitoring inkl. Alarmierungen − Automatisierte Schwachstellenscans sowie regelmäßige Patchzyklen − Einsatz von Zertifikaten (Web-Server)
Verfügbarkeit	**Generelle Maßnahmen** − Regelungen zum Störfall- und Notfallmanagement − Redundanzkonzepte, Lastverteilungsmethoden, Monitoringsysteme, Wartungskonzepte, etc. − Backup und Recovery − Prozessorientiertes Vorgehen inkl. Incident-, Problem und Change-Management. − Physikalische und logische Trennung von Diensten, Systemen, Netzen, . − Trennung von Test-, Entwicklungs- und Produktivsystemen − Verteilung der Datensicherung in unterschiedliche Brandabschnitte

	− Redundante RZ Infrastruktur − Einsatz eines BSI-zertifizierten DDoS-Mitigationsanbieters
Belastbarkeit	**Generelle Maßnahmen** − Härtung von Web-Systemen − Durchführung von automatisierten Schwachstellenscans sowie regemäßige Patchzyklen − Bedarfsorientierte Durchführung von Penetrationstests
Wiederherstellung bei physischen / technischen Zwischenfällen	**Generelle Maßnahmen** − Störfall- und Notfallmanagement − Durchführung von Notfall- und Wiederherstellungstests
Sicherstellung der Wirksamkeit	**Generelle Maßnahmen** − Regelmäßige interne und externe Auditierung im Rahmen der Zertifizierungen der regio iT − Anpassungen und Verbesserungen von Maßnahmen und Prozessen anhand des definierten kontinuierlichen Verbesserungsprozesses (KVP)

3 Liste der genehmigten Subunternehmer

	Name des Subunternehmers	Kontaktperson	Anschrift	Leistung
1	Regio iT gesellschaft für informations-technologie mbh	Claudia Husz	Lombardenstr. 24, 52070 Aachen	Datenschutz-beauftragte