Anlage 1:

Vereinbarung zur Auftragsverarbeitung zum Einzelabruf und technisch-organisatorische Maßnahmen

betreffend der digitalen Leistung:

„Engagementdirekt“

in Form des gleichnamigen Onlineportals

Zwischen dem Leistungsbezieher (Auftraggeber/Kommune) und dem Leistungserbringer (Auftragnehmer/Kommunalvertreter NRW) wird mit Vertragsschluss des Einzelabrufs die folgende Einzel-Auftragsvereinbarung (nachstehend „Einzel-AV“) zum Einzelabruf betreffend des Onlineportals „Engagementdirekt“ als Anlage 1 geschlossen.

Präambel
Diese Einzel-AV regelt auf Grundlage der zwischen den Vertragsparteien geschlossenen Rahmenvereinbarung zur Auftragsverarbeitung (nachstehend „**Rahmen-AV**“) die Einzelheiten der Datenverarbeitung im Zusammenhang mit dem Einzelabruf „Engagementdirekt“.

1 OZG-Verwaltungsleistungs-spezifische Datenkategorien, Zwecke, Betroffene

Der Auftragnehmer verarbeitet im Rahmen der OZG-Verwaltungsleistung „Engagementdirekt“ die folgenden personenbezogenen Daten:

Privatperson
- Daten nur intern für die Redakteure sichtbar
  - Vor- und Familienname
  - Adresse
  - Geburtsdatum
  - E-Mail-Adresse
  - Telefonnummer
- Daten öffentlich sichtbar
  - Einsatzort

Unternehmen, Verein & freie Initiative, Bildungseinrichtung
- Alle Daten sind öffentlich sichtbar
  - Name des Unternehmens
  - Name des Vereins & der freien Initiative
  - Name der Bildungseinrichtung
  - Kontakt
  - Ansprechpartner
  - Einsatzort

I. Zwecke

Die Daten werden zum Zweck der Registrierung und Anzeigenschaltung auf dem Onlineportal erhoben.

II. Betroffene

Nutzer des Onlineportals, dies können sowohl Privatpersonen oder auch Organisationen sein.

III. Datenkategorien

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

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere die Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

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)

Prinzip/Grundlage	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[1]** – Umsetzung des Opt-in Grundsatzes (explizite Zustimmung zur Verarbeitung durch Betroffenen) – Datenschutzkonforme Umsetzung der Einwilligungsregelung sowie Widerspruch	– Zentrales Ticketsystem – Aufgabensteuerung – Vertrags- und Verpflichtungsdokumentation in Vertragsmanagementsystem – Schulung und Sensibilisierung der Mitarbeiter zu Rechtmäßigkeit der Verarbeitung (z.B. Hinweispflicht)
Datenminimierung	**Generelle Maßnahmen** – Sicherstellung der Datenminimierung **Produktspezifischen Maßnahmen[1]** – Möglichkeit der Deklaration von Pflicht- und Bedarfseingaben für alle Datenfelder	- Festlegungen zum Umfang der Datenerhebung in Kundenprozessen - Beratung und Empfehlung bezüglich der Datenminimierung in Entwicklungen und Projekten

[1] Maßnahmen zu Produkten externer Lieferanten können durch regio iT nur geprüft werden; eine Umsetzung muss durch die verantwortliche Stelle festgelegt werden.

Prinzip/Grundlage	Maßnahmen/Anforderung	Umsetzungsdetails
	– Übersicht von Tabellen und Datumsfelder auf Anfrage – Möglichkeit zur Deaktivierung nicht-benötigter / nicht-relevanter Datenfelder und Bearbeitungsfunktionen	
Speicherbegrenzung	**Generelle Maßnahmen** - Umsetzung des datenschutzkonformen Löschen und Entsorgen von Datenträgern, Medien und Dokumenten auf Basis des Löschkonzepts des Verantwortlichen **Produktspezifischen Maßnahmen[1]** – 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[1]** – 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 Berechtigungskonzepte – Externes Syslogsystem – Archivierung gem. vertraglicher Vereinbarung – Mit den Kunden vereinbarte Transportwege von Datensicherungsträger – Gesicherte Datenaustauschverfahren
Vertraulichkeit	**Generelle Maßnahmen** – Möglichkeit zur Rechtesteuerung auf Nutzer/Administrationsebene bzw. auf Ebene von (kritischen)	- Details gem. TOM Liste Teil B

Prinzip/Grundlage	Maßnahmen/Anforderung	Umsetzungsdetails
	Funktionen oder Konfigurations-einstellungen – 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[1]** – Konfigurationsmöglichkeit unterschiedlicher "Protokolltiefen" sowie Kopplung der Protokollierung an das Rechte/Rollenkonzept	
Rechenschaftspflicht	**Generelle Maßnahmen** - Nachweis zur Umsetzung eines Datenschutz-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 Maßnahmen[1]** - Integrative Beschreibung der Datenschutzmaßnahmen als Bestandteil der Programmdokumentation - Möglichkeit zur online-Beantragung von Betroffenenrechten	– Definition und Betrieb eines DSMS (policies und Datenschutzhandbuch) – 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/Regelungen mit Unterauftragsverarbeitern – Vertrags- und Verpflichtungsdokumentation in SAP VMS
Transparenz	**Generelle Maßnahmen** - Definition von Verarbeitungskategorien - Führung von Verzeichnissen der Verarbeitungskategorien **Produktspezifischen Maßnahmen[1]**	- Umsetzung als Ergänzung zu SLA und Leistungsscheinen - Führen des VVT-AV (Verzeichnis der Verarbeitungskategorien)

Prinzip/Grundlage	Maßnahmen/Anforderung	Umsetzungsdetails
	- Möglichkeit zur Information	
Betroffenenrechte	**Generelle Maßnahmen** - Unterstützung des Verantwortlichen zur Umsetzung der Betroffenenrechte gem. vertraglicher Festlegungen **Produktspezifischen Maßnahmen[1]** - Möglichkeit zur Bereitstellung von Formularen, links oder sonstigen strukturierten Erfassungen der Betroffenenanfragen	- Prozess zur Erfassung, Steuerung und Dokumentation von Anfragen
Data protection by design and by default	**Generelle Maßnahmen** - Umsetzung der Datenschutzprinzipien - Sicherstellung der Prüfmöglichkeit zu DS-Maßnahmen durch Audits - Bereitstellung TOM-Liste **Produktspezifischen Maßnahmen[1]** - siehe Datenschutzprinzipien - Pseudonymisierung und Anonymisierung nach produktspezifischer Vereinbarung	- Integration Datenschutz (DS) in die Informationssicherheits-Prozesse auf Basis nationaler und internationaler Standards und Empfehlungen[2] - 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
Verarbeitung unter Aufsicht	**Generelle Maßnahmen** - Nachweisliche Verpflichtung von Mitarbeitern und Externen - Nachweisliche Schulung der Mitarbeiter **Produktspezifischen Maßnahmen[1]** keine	- Siehe Datenschutzprinzipien
Sicherheit der Verarbeitung	**Generelle Maßnahmen** - Definition von Maßnahmen in strukturierten und dokumentierten Prozessen - Regelmäßige Kontrolle der Wirksamkeit und Angemessenheit von Maßnahmen	- Zertifizierung nach ISO 27001 - Regelmäßige Prüfung in internen und externen Audits - Details in „sicherheitsspezifischen TOM“

[2] Bspw. SDM – Standard Datenschutz Modell; ISO 29151; BS 10012:2017

Prinzip/Grundlage	Maßnahmen/Anforderung	Umsetzungsdetails
	Produktspezifischen Maßnahmen[1] keine	
Meldung von Datenschutzverletzungen	**Generelle Maßnahmen** - Nachweis zur Erfassung von Datenschutzverletzungen - Meldung von DS-Verletzungen an kundendefinierte Kontaktstellen - Ggf. Umsetzung von Sofortmaßnahmen Unterstützung der Verantwortlichen zur Dokumentation von DS-Verletzungen gem. vertraglicher Regelungen **Produktspezifischen Maßnahmen[1]** keine	- Integration Prozess zu DS-Verletzungen in Sicherheitsereignisprozess - Absprache, Bewertung, Dokumentation und ggf. Meldung der Datenschutzverletzung nach geregeltem Prozess - Merkblatt für MA zum Verhalten bei DS-Verletzungen - Entwicklung von DS-Responseplänen (Sofortmaßnahmen)
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung	**Generelle Maßnahmen** - Nachweis der Verarbeitung im Rahmen der Auftragsverarbeitung nur auf Weisung des Auftraggebers - Überprüfung der Angemessenheit und Wirksamkeit der technisch-organisatorischen Maßnahmen - Sicherstellung der Aktualität und der Wirksamkeit der Datenschutzprozesse	- Auftragskontrolle - Formale Auftragserteilung (Ticketsystem) - Verpflichtung von Mitarbeitern auf Weisungsgebundenheit und Vertraulichkeit - Review von Verpflichtungserklärungen und AV-Verträge (Dienstleistern) - Jährliches Review der TOM - Datenschutzmanagement - Etablierte Prozesse nach DSGVO - Jährliches Prozessreview und Überprüfung durch interne Audits
Datenschutzbeauftragter	**Generelle Maßnahmen** - Ernennung einer/s Datenschutzbeauftragten **Produktspezifischen Maßnahmen[1]** - Keine	- Rollendefinition und -besetzung zu Datenschutzbeauftragten in Stabsstelle

Teil B: TOM zur (Informations-) Sicherheit

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

Prinzip/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 • Elektronische und mechanische Zutrittskontrollsysteme in Verbindung mit Berechtigungskonzepten (RBAC-Rule based access control), Registrierungen, Protokollierungen, Auditierungen, Verpflichtungen und Begleitung Externer – 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 (Datenschutz, Fernmeldegeheimnis, etc.), Unterweisungen, Protokollierungen • 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

3 Liste der genehmigten Subunternehmer

	Name des Subunternehmers	Kontaktperson	Anschrift	Leistung
1	Informatik Consulting Systems GmbH	Tobias Pankrath	Sonnenbergstraße 13 70184 Stuttgart	Unterstützung Entwicklung
2				
3				