Projektreferenz

Ausschreibung: “Weiterentwicklung und Betrieb der Software für die Datentreuhänder-Plattform EuroDaT sowie des AML-Anwendungsfalls safeAML”

**Ausfüllhinweise:**

1. Füllen Sie das Formular für jede Referenz getrennt aus und benennen Sie die Dateien wie in den Angebots- und Verfahrensbedingungen beschrieben.
2. Änderungen am Format der Projektreferenz sind nicht zulässig. Ebenso wenig dürfen vorgegebene Texte oder Abstände verändert, ersetzt oder entfernt werden.
3. Der Gesamtumfang jeder einzelnen Referenz darf die folgende Seitenzahl nicht überschreiten: Nicht mehr als 20 Seiten, falls die Referenz für beide Lose gilt. Nicht mehr als 15 Seiten, falls sie nur für Los 1 gilt. Nicht mehr als 8 Seiten, falls sie nur für Los 2 gilt.

| Name der Bewerberin/Bewerberinnengemeinschaft |  |
| --- | --- |
| Laufende Nr. der Referenz (1-3) |  |
| Referenz für welche Lose (Los 1 / Los 2 / Los 1 und Los 2) |  |

| **A** | Projektbezeichnung |  |
| --- | --- | --- |
| **B** | Auftraggeberin (Name, Anschrift) |  |
| **C** | Aktuelle Ansprechperson bei der Auftraggeberin (Name, Rolle, Tel.-Nr., E-Mail-Adresse) |  |
| **D** | Branche |  |
| **E** | Projektlaufzeit von bis  (von MM/JJ bis MM/JJ) |  |
| **F** | Anzahl eingesetzter VZÄ (des Unternehmens) |  |

| **Beschreibung des Projekts**  Bitte beschreiben Sie Ihr Projekt (max. 1 Seite). |
| --- |
|  |

**Angaben zu Bewertungskriterien in der Matrix**

| **Kriterium 1 (erforderlich für Los 1 und Los 2)** | | |
| --- | --- | --- |
| **Ausgewiesene Erfahrungen bei der Implementierung von Individualsoftware im Finanzsektor sowie Kenntnisse über die dort geltenden rechtlichen Rahmenbedingungen** | | |
| Welche Art von Individualsoftware wurde implementiert und wie ist der Rechtsrahmen des Finanzsektor dabei berücksichtigt worden? |  | |
| Zeitraum (Monate/Jahre) |  | |
| Umfang der Tätigkeit (PT) |  | |

| **Kriterium 2 (erforderlich für Los 1 und Los 2)** | | |
| --- | --- | --- |
| **Einschlägige Erfahrungen beim Einsatz von Sicherheitstechnologien und -praktiken zur Absicherung sensibler Daten bei der Implementierung und dem Betrieb von Individualsoftware. Anwendung und Implementierung von Verfahren zur Anonymisierung oder Pseudo-Anonymisierung.** | | |
| Wie und welche Sicherheitstechnologien und -praktiken wurden bei der Implementierung und dem Betrieb der Individualsoftware angewandt? Wurden Verfahren zur Pseudonymisierung / Anonymisierung angewandt und / oder entwickelt? Wie, welche und wofür? |  | |
| Zeitraum (Monate/Jahre) |  | |
| Umfang der Tätigkeit (PT) |  | |

| **Kriterium 3 (erforderlich für Los 1)** | | |
| --- | --- | --- |
| **Einschlägige Erfahrungen bei der Entwicklung und dem Betrieb von Dataspace- oder Datentreuhänder-Software als Free and Open Source Software (FOSS). Dies im Kontext von (Public-) Cloud und/oder On-Premises Infrastrukturen.** | | |
| Welche Dataspace- oder Datenraum-Software haben Sie im Projekt als Open Source entwickelt? Welche? Wo und unter welcher Lizenz ist sie veröffentlicht? |  | |
| Auf welcher Infrastruktur wird sie betrieben? |  | |
| Umfang der Tätigkeit (PT) |  | |

| **Kriterium 4 (erforderlich für Los 1)** | | |
| --- | --- | --- |
| **Einschlägige Erfahrungen bei der Entwicklung Kubernetes-nativer Applikationen unter Einsatz z.B. der folgenden oder vergleichbarer Technologien: 1. Kotlin/Quarkus, 2. Typescript/Angular, 3. PostgreSQL, 4. Gradle** | | |
| Haben Sie im Kontext des Projekts Kubernetes-native Applikationen entwickelt? Welche und nach welchen Prinzipien? |  | |
| Welche der folgenden oder vergleichbaren Technologien wurden dabei eingesetzt: 1. Kotlin/Quarkus, 2. Typescript/Angular, 3. PostgreSQL, 4. Gradle? |  | |
| Umfang der Tätigkeit (PT) |  | |

| **Kriterium 5 (erforderlich für Los 1)** | | |
| --- | --- | --- |
| **Einschlägige Erfahrungen bei der Umsetzung und Pflege von CI/CD-Pipelines z.B. mit den folgenden oder vergleichbaren Technologie: 1. Argo CD, 2. Docker, 3. GitLab, 4. SonarCloud, 5. Terraform/OpenTofu** | | |
| Haben Sie im Kontext des Projekts CI/CD-Pipelines umgesetzt und/oder gepflegt? Nach welcher Vorgehensweise? |  | |
| Welche der folgenden oder vergleichbaren Technologien wurden dabei eingesetzt: 1. Argo CD, 2. Docker, 3. GitLab, 4. SonarCloud, 5. Terraform/OpenTofu? |  | |
| Umfang der Tätigkeit (PT) |  | |

| **Kriterium 6 (erforderlich für Los 1)** | | |
| --- | --- | --- |
| **Einschlägige Erfahrungen beim Deployment und der Wartung Kubernetes-nativer Applikationen z.B. mit den folgenden oder vergleichbaren Technologien: 1. Kubernetes, 2. Docker, 3. Helm, 4. Argo CD** | | |
| Haben Sie im Kontext des Projekts Kubernetes-native Applikationen deployt und gewartet? Welche? Wie sind Sie vorgegangen? |  | |
| Welche der folgenden oder vergleichbaren Technologien wurden dabei eingesetzt: 1. Kubernetes, 2. Docker, 3. Helm, 4. Argo CD? |  | |
| Umfang der Tätigkeit (PT) |  | |

| **Kriterium 7 (erforderlich für Los 1)** | | |
| --- | --- | --- |
| **Einschlägige Erfahrungen beim Aufbau und der Wartung von (Public-) Cloud-Organisationen für sicherheitskritische Anwendungen in der Google Cloud (oder vergleichbar) z.B. mit folgenden oder vergleichbaren Technologie: 1. GitLab, 2. Terraform/OpenTofu** | | |
| Haben Sie im Kontext des Projekts eine Cloud-Organisation für eine sicherheitskritische Anwendung aufgebaut und gewartet? Welche? Mit welchen sicherheitskritischen Anforderungen? In welcher Cloud? |  | |
| Welche der folgenden oder vergleichbaren Technologien wurden dabei eingesetzt: 1. GitLab, 2. Terraform/OpenTofu? |  | |
| Umfang der Tätigkeit (PT) |  | |

| **Kriterium 8 (erforderlich für Los 1)** | | |
| --- | --- | --- |
| **Einschlägige Erfahrungen bei der Umsetzung von Authentifizierung/Autorisierung in der Google-Cloud (oder vergleichbar) und in Kubernetes z.B. mit den folgenden oder vergleichbaren Technologien: 1. OIDC, 2. OAuth2, 3. Keycloak, 4. Google IAM, 5. Hashicorp Vault** | | |
| Haben Sie im Kontext des Projekts eine Authentifizierung und Autorisierung in der Cloud umgesetzt? Wofür und auf welche Weise? In welcher Cloud? |  | |
| Welche der folgenden oder vergleichbaren Technologien wurden dabei eingesetzt: 1. OIDC, 2. OAuth2, 3. Keycloak, 4. Google IAM, 5. Hashicorp Vault? |  | |
| Umfang der Tätigkeit (PT) |  | |

| **Kriterium 9 (erforderlich für Los 2)** | | |
| --- | --- | --- |
| **Erfahrungen bei der Entwicklung von Individualsoftware im Bereich Geldwäsche und Terrorismusfinanzierung (AML/CFT)** | | |
| Haben Sie im Kontext des Projekts Individualsoftware im Bereich AML/CFT entwickelt? Welche? In welchen dieser Bereiche? |  | |
| Umfang der Tätigkeit (PT) |  | |

| **Kriterium 10 (erforderlich für Los 2)** | | |
| --- | --- | --- |
| **Einschlägige Erfahrungen bei der cloud-nativen Applikationsentwicklung z.B. mit den folgenden oder vergleichbaren Technologien: 1. Java/Spring Boot, 2. Typescript/Vue, 3. Python, 4. PostgreSQL, 5. Gradle** | | |
| Haben Sie im Kontext des Projekts cloud-native Applikationen entwickelt? Welche? Nach welche Prinzipien? |  | |
| Welche der folgenden oder vergleichbaren Technologien wurden dabei eingesetzt: 1. Java/Spring Boot, 2. Typescript/Vue, 3. Python, 4. PostgreSQL, 5. Gradle? |  | |
| Umfang der Tätigkeit (PT) |  | |

| **Kriterium 11 (erforderlich für Los 2)** | | |
| --- | --- | --- |
| **Einschlägige Erfahrungen beim Serverless-Deployment Cloud-nativer Applikationen z.B. mit den folgenden oder vergleichbaren Technologien: 1. Cloud Run, 2. Docker, 3. Gitlab, 4. Argo CD** | | |
| Haben Sie im Kontext des Projekts cloud-native Applikationen serverless deployt? Welche? Wie sind Sie vorgegangen? |  | |
| Welche der folgenden oder vergleichbaren Technologien wurden dabei eingesetzt: 1. Cloud Run, 2. Docker, 3. Gitlab, 4. Argo CD? |  | |
| Umfang der Tätigkeit (PT) |  | |

EuroDaT behält sich vor, die Richtigkeit der hier gemachten Angaben u.a. durch Rückfrage bei der genannten Ansprechperson zu prüfen.

| **Name und Rechtsform der Bewerberin/Bieterin** |
| --- |
|  |
| **Name, Vorname und Funktion der:des Vertreters:in der Bewerberin/Bieterin** |
|  |
| **Datum** |
|  |