FORSCHUNGSFÖRDERUNG CYBERSICHERHEIT HESSEN

Hessisches Ministerium des Innern und für Sport

Aufruf zur Einreichung von Anträgen (2022-01)

gemäß der „Förderrichtlinie Cybersicherheitsforschung in Hessen“ des Hessischen Ministeriums des Innern und für Sport

1. **Allgemeines**

   Eine Zuwendung auf Basis der o. g. Richtlinie ist im Rahmen dieses Aufrufs nur möglich für Forschungsvorhaben, die Fragestellungen innerhalb eines der unter Nr. 5 genannten Themengebiete behandeln.

   Dieser Aufruf wurde am 02.02.2022 veröffentlicht. Ab diesem Zeitpunkt können auf Basis der Richtlinie Antragsskizzen eingereicht werden.

2. **Ablauf des Verfahrens**

   Die Antragstellung erfolgt gemäß Nr. 7 der Förderrichtlinie. In einem ersten Schritt wird eine Antragsskizze eingereicht. Sofern dem Zuwendungsgeber bereits diesbezügliche Skizzen vorliegen, kann dieser Schritt entfallen. In einem zweiten Schritt erfolgt nach Aufforderung durch den Zuwendungsgeber die Einreichung des Projektantrags.
   Es wird empfohlen, vor Einreichung einer Antragsskizze mit dem Zuwendungsgeber Kontakt aufzunehmen, um die Eignung des geplanten Forschungsvorhabens zu beraten.

3. **Fristen zur Einreichung von Antragskizzen und zur Antragsstellung**

   Die Antragsskizze muss spätestens drei Wochen nach Veröffentlichung dieses Aufrufs beim Zuwendungsgeber eingegangen sein. Der Zuwendungsgeber ist bestrebt, den Antragsteller innerhalb von vier Wochen nach Ende dieser Frist zur Abgabe eines Projektantrags aufzufordern. Sollte das Projekt nicht förderungsfähig sein, so informiert der Zuwendungsgeber den Antragsteller darüber.

   Der Projektantrag muss nach erfolgter Aufforderung innerhalb von sechs Wochen eingereicht werden.

   Sowohl Antragsskizze als auch Projektantrag müssen von einer vertretungsberechtigten Person des Antragstellers unterschrieben und schriftlich an folgende Stelle gerichtet sein:

Hessisches Ministerium des Innern und für Sport
Referat VII 4 Innovationsmanagement Cybersicherheit
Friedrich-Ebert-Allee 12
65185 Wiesbaden

Beide Dokumente sind zusätzlich elektronisch an den Zuwendungsgeber (E-Mail-Funktionspostfach: RefLtgVII4@hmdis.hessen.de) zu senden. Das Datum des Poststempels gilt als fristwahrend.

4. Maximale Fördersumme

Für das Forschungsvorhaben dieses Aufrufs werden maximal 350.000€ als Zuwendung bewilligt. In begründeten Ausnahmefällen (bspw. bei Gemeinschaftsanträgen) kann davon abgewichen werden.

5. Thematischer Rahmen (Themengebiet)

Die Zuwendung zielt stets auf die wissenschaftliche Erforschung von Fragen der Cybersicherheit im Kontext der öffentlichen Verwaltung in Hessen in definierten Themengebieten. Das Forschungsvorhaben muss Teile des skizzierten Forschungsbedarfs abdecken und in seiner Zielstellung den Stand der Forschung übertreffen.

Eine Zuwendung im Rahmen dieses Aufrufs ist nur möglich für ein Forschungsvorhaben, das Fragestellungen innerhalb des folgenden Themengebiets behandelt:

Hessisches „Federated Learning Framework“ für Sicherheitsbehörden (HFL)

Mit der zunehmenden digitalen Transformation werden immer mehr Daten erzeugt, die übertragen, gespeichert und verarbeitet werden müssen. Besonders die Analyse von Big Data zur Bekämpfung von Cyberangriffen und Cyberkriminalität stellt Strafverfolgungsbehörden vor Herausforderungen. In diesem Zusammenhang zeigen die aktuellen Entwicklungen auf dem Gebiet des so genannten „Federated Learning“ (FL) vielversprechende Resultate. Diese Algorithmen ermöglichen es mehreren Parteien, gemeinsam Machine-Learning-Modelle (bspw. Deep Neural Networks) zu trainieren, ohne die auszuwertenden Ursprungsdaten herausgeben, bzw. teilen zu müssen. Stattdessen erlauben diese Algorithmen den beteiligten Parteien gemeinsam Machine-Learning einzusetzen, um große Datenmengen zu analysieren.

Ziel des Forschungsprojektes soll die wissenschaftliche Entwicklung und Implementierung eines sicheren und effizienten „Federated Learning Framework“ zur KI-unterstützten, gemeinsamen Big Data-Analyse der hessischen Sicherheitsbehörden unter Bezugnahme des Bereichs Rechtsextremismus sein.

Innerhalb des hier aufgerufenen Forschungsprojekts sollen dynamische Rahmenbedingungen für ein Federated Learning Framework entworfen und implementiert werden, welche die Sicherheitsbedrohungen, bspw. Daten- und Modellverfälschungen, Evasion-Angriffe und Datenschutzbedrohungen, bspw. Member-Inference- und Datenrekonstruktionsangriffe, im konkreten Anwendungskontext berücksichtigt.

6. Maximale Projektlaufzeit

Die Forschungsvorhaben sollen eine dem Forschungsgegenstand (Bedarf, Methodik und Ziel) angemessene Laufzeit haben. Dabei soll eine Laufzeit von 12 Monaten als Richtwert dienen; 24 Monate dürfen nicht überschritten werden.