Antrag auf Bereitstellung eines (virtuellen) Servers im Studiengang Informatik

(Abgabe: netz@dhbw-karlsruhe.de / Raum E311, E312 oder E314)

DHBW
Duale Hochschule
Baden-Württemberg
Karlsruhe

Bezeichnung	studienarbeit-mischmaschine			
Zweck/Funktion	Studienarbeit - Trainieren eines KI-Modells			
Betreiber*In (verantwortlich)	Felix Gervasi	Kurs	TINF20B4	
E-Mail Adresse	fgervasi@web.de			
Betreuer*In (DHBW)	Prof. Dr. Jörn Eisenbiegler			
Nutzungsdauer	Startdatum	19.12.2022	Enddatum	31.05.2023

Erreichbarkeit

- (●) Intern (nur vom Lehre-Netz, WLAN und VPN aus)
- ( ) Öffentlich (Genehmigung durch Leitungsgremien erforderlich)

DNS-Eintrag (optional)

( ) .inf ( ) .wi ( ) .el ( ) .mb ( ) .mt .dh-karlsruhe.de

CPU (Kerne)	8	RAM (GB)	32	Storage (GB)	100		
Betriebssystem	Linux	Ubuntu					
Ports ankommend	TCP	22	UDP				
Ports abgehend (SMTP / TCP 25 ist gesperrt)	TCP	22	UDP				
Anmerkungen:							

Sie sind während des Betriebs für die Einhaltung der geltenden, gesetzlichen Bestimmungen (u.a. Urheberrecht, Datenschutzgrundverordnung (DSGVO), Paragraphen §202 und §303 StGB) verantwortlich. Die regelmäßige Datensicherung liegt in der Verantwortung des Betreibers/der Betreiberin.

Datum 12.12.2022 Unterschrift F. Gervasi

Vermerke (werden vom Fachbereich Netz ergänzt)

IPv4-Adresse:		Subnetz:		Gateway:	
IPv6-Adresse:					

Bearbeiter*In: _____ Unterschrift: _____

Anhang

Urheberrecht:

Die durch den/die Betreiber*In erstellten Inhalte und Werke auf dem zur Verfügung gestellten Server unterliegen dem deutschen Urheberrecht. Für Inhalte haftet der/die Studierende selbst.

Datenschutzgrundverordnung (DSGVO)

Die Datenschutzgrundverordnung (DSGVO) der Europäischen Union verfolgt das Ziel den Schutz personenbezogene Daten in der Europäischen Union sicherzustellen. Ebenfalls soll der Datenverkehr innerhalb des Europäischen Binnenmarktes gewährleistet werden. Seit dem 25. Mai 2018 ist die DSGVO anzuwenden.

Die DSGVO enthält eine Vielzahl an Regelungen zum Schutz personenbezogener Daten und eine erhebliche Anzahl an Informationspflichten. Teilweise sind die Regelungen nur mit erheblichem Aufwand umsetzbar. Generell verbietet die DSGVO die Verarbeitung personenbezogener Daten aller Art. Erlaubt ist eine Datenverarbeitung seit dem 25. Mai 2018 nur noch dann, wenn dafür eine gesetzliche Grundlage besteht.

Die DSGVO stellt nicht nur für viele Unternehmen, Vereine, Verbände, Kommunen und öffentliche Einrichtungen eine Herausforderung dar. Auch viele private Webseitenbetreiber sind betroffen. Erschwerend kommt hinzu, dass IP-Adressen als personenbezogene Daten gelten. Daraus ergeben sich in der Praxis teils erhebliche Probleme.

Grundsätzlich gilt:

- eine Verarbeitung personenbezogener Daten ist nur noch auf Grundlage einer gesetzlichen Regelung zulässig
- unter personenbezogene Daten fallen auch IP-Adressen
- personenbezogene Daten dürfen nur zu einem bestimmten Zweck erhoben und verarbeitet werden
- es dürfen nur so viele Daten erhoben werden, wie für einen bestimmten Zweck unbedingt notwendig sind
- erhobene Daten müssen sachlich richtig sein
- personenbezogene Daten müssen so sicher wie möglich verarbeitet werden
- grundsätzlich benötigt jede Website eine Datenschutzerklärung
- Tools, Module und Plugins auf Websites sind auf das notwendige Maß zu beschränken
- Tools, Module und Plugins mit unbekannter Herkunft oder auffälliger Verhaltensweise sind zu ersetzen oder zu entfernen
- die meisten Websites müssen über HTTPS erreichbar sein
- Formulare und E-Mails sind verschlüsselt zu übertragen

Eine rechtskonforme Umsetzung der DSGVO ist damit noch nicht abgeschlossen. Sie müssen darüber hinaus prüfen, ob Sie einen Datenschutzbeauftragten bestellen müssen, nach Artikel 37 DSGVO und § 38 Bundesdatenschutzgesetz (BDSG). Außerdem ist nach Artikel 30 DSGVO ein Verzeichnis mit Verarbeitungstätigkeiten zu führen. Unter Umständen müssen Sie eine Datenschutz-Folgenabschätzung nach Artikel 35 DSGVO durchführen. Es sind außerdem technische und organisatorische Maßnahmen zur Gewährleistung des Datenschutzes zu ergreifen. Insgesamt obliegen Ihnen nach der DSGVO diverse, teils umfangreiche Dokumentationspflichten.

Die Deutsche Gesellschaft für Datenschutz bietet für die Erstellung einer Datenschutzerklärung ein Tool an unter: https://dsgvo-muster-datenschutzerklaerung.dg-datenschutz.de/.

Paragraph §202 Strafgesetzbuch (StGB)

§202a StGB: Ausspähen von Daten
(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind,unter Überwindung der Zugangssicherungverschafft,wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
(2)Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch,magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

§202b StGB: Abfangen von Daten
Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

§202c StGB: Vorbereitung des Abfangens
(1) Wer eine Straftat nach §202a oder §202b vorbereitet, indem er 1) Passwörter oder sonstige Sicherungscodes, die den Zugang zuDaten (§202a Abs. 2) ermöglichen, oder 2) Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

Paragraph §303 Strafgesetzbuch (StGB)

§303a StGB: Datenveränderung
(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
(2) Der Versuch ist strafbar.
(3) Für die Vorbereitung einer Straftat nach Absatz 1 gilt §202 centsprechend.

§303b StGB: Computersabotage
(1) Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er 1) eine Tat nach §303a Abs. 1 begeht, 2) Daten(§202a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder 3) eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
(2) Handelt es sich um eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behördevon wesentlicher Bedeutung ist, ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.
(3) Der Versuch ist strafbar.
(4) Insbesonders schweren Fällen des Absatzes 2 ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter 1) einen Vermögensverlust großen Ausmaßes herbeiführt, 2) gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Computersabotage verbunden hat 3) durch die Tat die Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder die Sicherheit der Bundesrepublik Deutschland beeinträchtigt.
(5) Für die Vorbereitung einer Straftat nach Absatz 1 gilt §202 centsprechend.