OSTBAYERISCHE TECHNISCHE HOCHSCHULE REGENSBURG

FAKULTÄT
INFORMATIK UND MATHEMATIK

Antrag auf Einrichtung einer Internetpräsenz an der Fakultät IM

(Stand 10.07.2018 LUF)

Antragsbedingungen:

- Bedienstete der Fakultät IM können auf Wunsch eine dienstliche Homepage auf dem Server FBIM unter ihrem RZ-Account oder für ein "Projekt" erhalten.
  - Dort wird lediglich Webspace mit PHP und MySQL-Datenbank angeboten.
  - Der administrative Zugang zu Homepage bzw. Datenbank erfolgt per SSH/SFTP und phpMyAdmin.
  - Adresse der Homepage: https://fbim.oth-regensburg.de/~*kennung*
- Mit Zustimmung des Dekans kann auch ein System in der DMZ realisiert werden, dessen technische Auslegung mit dem Pool-Management abgestimmt wird.
- Für Erstellung, Inhalte, Pflege und Missbrauchsschutz der Internetpräsenz (FBIM-Homepage oder DMZ-System) ist allein der Antragsteller verantwortlich.

Sicherheit:

- Die eingerichtete Internetpräsenz ist öffentlich und frei im Internet erreichbar!
- Falls notwendig kann für eine FBIM-Homepage ein Zugriffsschutz eingerichtet werden. Die Mitarbeiter im Pool-Management können dabei behilflich sein.
- Ein DMZ-System wird grundsätzlich von der RZ-Firewall geschützt. Ausgenommen sind die für den Betrieb notwendigen geöffneten Ports (z.B. 22, 80, 443, etc.) für deren Verwendung und Schutz der Antragsteller verantwortlich ist.
- Der Antragsteller sorgt für Wartung und Sicherheitsupdates seines DMZ-Systems.

Rechtslage:

- Es handelt sich hier an der Hochschule um eine dienstliche Internetpräsenz!
- Die gültige Rechtslage für dienstliche Internetpräsenzen ist vom Antragsteller jederzeit zu beachten und umzusetzen (Bayrisches Datenschutzgesetz BayDSG, Europäische Datenschutzgrundverordnung EU-DSGVO).
- Dazu müssen Impressum und Datenschutzerklärung der OTH-Regensburg (https://www.oth-regensburg.de/) vom Antragsteller bereitgestellt (und ggf. angepasst) werden, und von jeder (Unter)-Webseite aus erreichbar sein.

Hiermit beantrage ich die Einrichtung einer Internetpräsenz (DMZ-System, vorbehaltlich der Zustimmung des Dekans, oder FBIM-Homepage) zu dienstlichen Zwecken, und versichere die Einhaltung aller rechtlichen und hausinternen Vorgaben dafür.

_____ ☐ FBIM-Homepage ☐ DMZ-System

RZ-Account oder Projektname:

_____ _____

Ort, Datum Unterschrift

Abgabe des unterschrieben Antrags beim Pool-Management in Raum K102 Hilfe zur Umsetzung siehe Rückseite

Antrag auf Einrichtung einer Internetpräsenz an der Fakultät IM – Anhang

Begriffsklärungen:

- Internetpräsenz: jeder im Internet öffentlich erreichbare (Web)-Server oder gehostete Webseite, die von beliebigen, im Vorfeld unbekannten Personen abgerufen werden kann.
- FBIM: historisch bedingter Name des Fakultätswebservers, https://fbim.oth-regensburg.de/
- PHP: PHP Hypertext Processor. Verbreitete Scriptsprache zur Erstellung von dynamischen Webseiten.
- DMZ: Demilitarisierte Zone. Fachbegriff für einen Netzwerkbereich, der vom Internet her soweit wie technisch notwendig zugänglich, ansonsten aber durch eine Firewall geschützt ist, und auch das interne Netzwerk einer Organisation (Campus-LAN) abtrennt.
- RZ: Rechenzentrum (der OTH Regensburg)
- DSGVO, EU-DSGVO: europäische Datenschutzgrundverordnung
- TMG: Telemediengesetz
- BDSG: Bundesdatenschutzgesetz
- BayDSG: Bayrisches Datenschutzgesetz
- DSE: Datenschutzerklärung nach den Vorgaben der zutreffenden Datenschutzgesetze
- VM: virtuelle Maschine. Ein System, bei dem sich viele Systeme/Server eine gemeinsame Hardware teilen.

Handreichung zur DSGVO (vom Uni-RZ übernommen und angepasst):

- Social-Media-Angebote: Wenn Sie ein Angebot auf Facebook, Twitter oder Youtube pflegen, verlinken Sie dort auf Datenschutzerklärung und Impressum der Hochschule. Setzen Sie statt Social-Media-Buttons auf ihren Webseiten das entsprechende Logo mit einem "normalen" Link zum externen Anbieter ein (anstatt mit JavaScript), da dadurch keine versteckte Datenweitergabe stattfindet (siehe unten).

- Eigene Webangebote auf zentralen Webservern: Wenn Sie Webangebote bereitstellen, die nicht mit dem zentralen CMS (= Typo3) erstellt wurden, die aber auf einem zentralen Webserver (= FBIM-Homepage) liegen, ist folgendes zu tun: Stellen Sie sicher, dass jede Seite einen Link auf die Datenschutzerklärung und das Impressum der Hochschule enthält. Prüfen Sie, ob die dort genannten Informationen für Ihr Angebot zutreffen und ausreichen. Falls Ihr Angebot nicht im Verantwortungsbereich der Hochschule liegt, z.B. evtl. bei Aninstituten, Vereinen, überwiegend externen Projekten etc., müssen sie ein eigenes Impressum und eine eigene DSE erstellen und verlinken. Sie können dabei auf zutreffende Passagen der DSE der Hochschule verweisen oder diese kopieren, z.B. ist die Passage Web-Logs für die zentralen Webserver immer identisch. Beachten Sie den Punkt Datenweitergabe und "versteckte Datenweitergabe". Falls Ihr Angebot zusätzliche Daten erhebt und/oder Daten an Dritte weitergegeben werden, müssen Sie darüber zwingend in einer eigenen Datenschutzerklärung informieren und Sie benötigen zwingend entweder eine Rechtsgrundlage oder eine Einverständniserklärung des Nutzers (siehe unten). Praktisch können Sie dann auf die DSE der Hochschule als Grundlage verweisen und diese ergänzen, z.B. "Ergänzend (abweichend) zur Datenschutzerklärung (Link) der Hochschule gilt Folgendes:... ".

- Webangebote auf eigenen Servern: Wenn Sie eigene Server oder VMs betreiben (= DMZ-System), sind die gleichen Punkte wie bei den zentralen Webservern zu beachten. Zusätzlich müssen Sie sicherstellen, dass Sie für Ihre Protokolldaten (z.B.: Web-Logs) passende Zweckmäßigkeit und Löschfristen haben. Wenn Sie die gleichen Einstellungen wie die zentralen Webserver verwenden (z.B. 14 Tage Löschfrist bei Web-Logs), können Sie auch hier auf die zentrale DSE verweisen. (Ferner müssen Sie mit geeigneten technischen und organisatorischen Maßnahmen die Datensicherheit und den Datenschutz Ihres Servers sicherstellen und dokumentieren. Diese Dokumentation muss aber nicht öffentlich publiziert werden.)

- Datenweitergabe, Achtung vor "versteckter Datenweitergabe": Beachten Sie, dass in vielen Konstellationen Daten von Dritten nachgeladen werden können und dabei werden i.d.R. mindestens Aufrufdaten weitergereicht, u.U. sogar Cookies gesetzt. Insbesondere beim Einsatz von Frameworks, PlugIns, Templates etc. werden häufig Elemente (Schriften, CSS, Karten, Bilder, Videos etc.) von fremden Servern (z.b. Google) nachgeladen. Prüfen Sie mit einer Analyse der Netzwerkaktivitäten Ihres Browsers (z.B. Entwicklertools im Firefox, siehe https://developer.mozilla.org/de/docs/Tools/netzwerkanalyse) von welchen Servern Daten geladen werden, wenn Sie Ihr Webangebot aufrufen und ob Cookies gesetzt werden. Wenn in der Liste ein Server, der nicht von der Hochschule betrieben wird, auftaucht, besteht Handlungsbedarf. Prüfen Sie, ob Sie die nachgeladenen Elemente auf Ihrem eigenen Webspace ablegen können, so dass sie nicht mehr bei Dritten nachgeladen werden. Verzichten Sie ggf. auf den Einsatz von Kartendiensten (z.B. Google-Maps), Suchdiensten (Google Custom Search), Tracking-Diensten (Google-Analytics), Werbung und ähnlichen Einbettungen, wenn Sie die Zweckmäßigkeit nicht begründen können, Sie keinen Vertrag zur Auftragsverarbeitung mit dem jeweiligen Anbieter geschlossen haben und Sie keine entsprechenden Informationen in Ihrer eigenen Datenschutzerklärung bereitstellen.

- Was ist zu beachten bei der Datenerhebung: Wenn Sie Daten bei oder über Personen erheben, gehen Sie davon aus, dass diese i.d.R. personenbeziehbar sind und Sie eine rechtliche Grundlage oder eine Einwilligung des Betroffenen benötigen. Nach §13 DSGVO müssen Sie darüber informieren und im Falle einer einwilligungsbasierten Erhebung sicherstellen, dass Sie die Einwilligung dokumentieren und ggf. nachweisen können. Prüfen Sie, dass sie keine Daten erheben, die Sie nicht direkt zur Erfüllung des vorgesehenen Zweckes benötigen. Informieren Sie zu sämtlichen erhobenen Daten in einem Beiblatt zu Ihrer Datenschutzerklärung, das ständig an die Gegebenheiten Ihrer Datenerhebung angepasst wird, benennen Sie eine zweckentsprechende Löschfrist und stellen Sie sicher, dass die Daten nach Fristablauf gelöscht werden.

- Der Datenschutzbeauftragte der Hochschule kann Ihnen bei datenschutzspezifischen Fragen weiterhelfen.