IMZ – Newsletter Sommersemester 2021

des Informationssicherheitsbeauftragten

und des Datenschutzbeauftragten an der HTWG im Mai 2021

Liebe Professorinnen und Professoren, liebe Mitglieder der Hochschule,

wir freuen uns, Ihnen zum Sommersemesterstart 2021 die aktuelle Ausgabe des gemeinsamen Newsletters des Datenschutzbeauftragten und des Informationssicherheitsbeauftragten vorzustellen.

In diesem Newsletter möchten wir Sie auf die Notwendigkeit eines **Datenschutzhinweises** in der **Signatur Ihrer HTWG-E-Mail-Adresse** und auf das Angebot eines **eLearning zum Datenschutz** aufmerksam machen, wodurch Sie den kleinen „Datenschutzführerschein“ an der HTWG erwerben können.
Wir bieten im Sommersemester wieder Online-**Schulungen** zum Thema **Datenschutz** an – nehmen Sie teil und werden Sie ihr eigener Datenschutzexperte!

Aus dem Bereich Informationssicherheit haben wir wichtige Tipps für Sie zum **sicheren IT-Einsatz bei der Telearbeit** und wir möchten Sie auf **Trainingsmodule rund um die IT-Sicherheit** auf Moodle aufmerksam machen.

Wir wünschen Ihnen viel Spaß beim Lesen und weiterhin ein gutes und erfolgreiches Sommersemester.

Beste Grüße, Ihre Marc Strittmatter (DSB), Hanno Langweg (ISB) und Frau jur. Ass. Inna Feldmann (Stabsstelle Datenschutz)

Die Themen:

- Datenschutzhinweis in der E-Mail-Signatur
- E-Learning Datenschutz
- Tipps zur Informationssicherheit
- Schulungstermine

A. Datenschutzhinweis in der E-Mail-Signatur

Seit Inkrafttreten der EU Datenschutz-Grundverordnung (DSGVO) ist auch die E-Mail-Kommunikation besonderen Anforderungen unterworfen: Artikel 13 DSGVO verlangt einen Datenschutzhinweis beim E-Mail-Versand. Falls Sie nicht die Zeit haben, sich über die Gründe und Details im Einzelnen zu informieren, scrollen Sie bitte einfach nach unten und **fügen Sie** den **Link** in Ihre **E-Mail-Signatur** ein (siehe A. 3., Seite 4 oben), dann haben Sie schon alles getan, was zu tun war.

Bild: iStockphoto.com

1. Informationspflicht bei E-Mail-Empfang

Durch eine E-Mail, die Sie erhalten oder eine dienstliche E-Mail, die Sie an Externe schreiben und auf die Sie Antwort erhalten, kann es sein, dass Sie personenbezogene Daten anfordern („erheben“) und diese anschließend abspeichern.

E-Mail-Adressen sind Informationen, die sich auf „identifizierte oder identifizierbare natürliche Personen“ beziehen und damit personenbezogene Daten. Sie unterliegen dem Datenschutz, es ist unerheblich, ob sie den vollen Namen des Adressaten beinhalten oder ob es sich um eine E-Mail-Adresse ohne weitere persönliche Daten handelt. Auch enthalten E-Mails fast immer weitere Informationen wie z.B. den Vor- und Zunamen, die Adresse und die Telefonnummer etc.

Die DSGVO sieht vor, dass betroffene Personen über eine etwaige Datenverarbeitung zu informieren sind. Die HTWG ist als Behörde

„Verantwortliche“ nach Artikel 4 Nr. 7 DSGVO und damit Adressat der DSGVO-Pflichten.

Da eine Datenerhebung nicht mit jeder E-Mail erfolgt, es aber andererseits nicht möglich ist, sich für jede Mail zu überlegen, ob nun ein erlaubnispflichtiger Vorgang vorliegt, ist der pragmatische Vorschlag, dass wir den Hinweis in unsere E-Mail-Signatur aufnehmen. Durch den Verweis per Link können wir Änderungen dynamisch nachpflegen und müssen Sie nur den weiter unten genannten, einfachen Hinweis aufnehmen.

Zur Nutzung von Zertifikaten möchten wir Sie gerne einladen (https://www.htwg-konstanz.de/rz/dienste/zertifikate/).

2. Inhalt der E-Mail mit den Informationen

Die Informationen, die dem E-Mail-Absender zur Verfügung gestellt werden müssen, sind recht umfangreich, der E-Mail-Absender ist unter anderem zu informieren über:

- den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters
- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen sowie die Rechtsgrundlage für die Verarbeitung
- die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer
- gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten
- gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten
- das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten inklusive des Rechts auf Beschwerde bei einer Aufsichtsbehörde

Hinzu kommt, dass der Aufwand sehr hoch wäre, nachzuvollziehen, ob bereits zu einem früheren Zeitpunkt eine E-Mail mit Informationen darüber an den E-Mail-Absender versendet wurde, welche Daten gesammelt werden und wie diese Daten verarbeitet werden.

3. Link-Lösung

Um die Informationspflicht auf einfache Weise zu automatisieren und nicht jedem E-Mail-Absender umgehend eine E-Mail zurücksenden zu müssen,

welche die geforderten Informationen enthält, bietet es sich an, den Datenschutzhinweis der HTWG mit Link in Ihre E-Mail-Signatur aufzunehmen. Sie können hierzu folgende Formulierung (mit Link) verwenden:

„Unsere Hinweise zum Datenschutz finden Sie hier: https://www.htwg-konstanz.de/info/datenschutzerklaerung/“.

Es ist nicht erforderlich, dass Sie den ganzen Text der schriftlichen Datenschutzhinweise in die E-Mail-Signatur selbst aufnehmen.

Es reicht jedoch nicht aus, wenn Sie in Ihrer E-Mail auf die Datenschutzerklärung der HTWG verweisen. Die Beifügung des Links ist erforderlich.

B. Stärken Sie Ihre Datenschutz-Awareness durch unser E-Learning Datenschutz!

- *Was ist überhaupt die Verarbeitung personenbezogener Daten?*
- *Ab wann muss ich an das Thema Datenschutz denken?*
- *Inwiefern betrifft mich der Datenschutz?*
- *Welche Pflichten muss ich als HTWG-MitarbeiterIn beachten?*
- *Wie verhindere ich Datenschutzverstöße?*
- *Verhalte ich mich datenschutzrechtlich konform?*

Datenschutz gelingt nur, wenn er von allen Beteiligten an der HTWG verstanden und unterstützt wird.

Wir möchten Ihnen dabei helfen, sich einen ersten Überblick zu verschaffen und wichtige Schritte im Umgang mit der Verarbeitung von personenbezogenen Daten zu lernen. Nutzen Sie hierfür gerne unser webbasiertes E-Learning mit Testfragen zum Datenschutz und bauen Sie Ihr Knowhow digital auf! Wir informieren Sie, welche Datenschutzgrundsätze Sie kennen müssen und wie Sie richtig mit Datenpannen und Meldepflichten umgehen.

Qualifizieren Sie sich für den **„kleinen Datenschutzführerschein“** auf

https://moodle.htwg-konstanz.de/moodle/course/view.php?id=4222

C. Tipps zur Informationssicherheit

Viele Beschäftigte nutzen seit dem vergangenen Jahr das mobile Arbeiten intensiver als vorher, manche zum ersten Mal. Während die IT-Infrastruktur der Hochschule auf dem Campus durch IuK und RZ intensiv betreut wird, ist zu Hause nicht immer der gleiche Servicelevel erreichbar. Auch lässt es sich nicht immer vermeiden, dass private Geräte genutzt werden. Für den **sicheren IT-Einsatz bei der Telearbeit** gibt es Empfehlungen des BSI (Bundesamt für Sicherheit in der Informationstechnik):

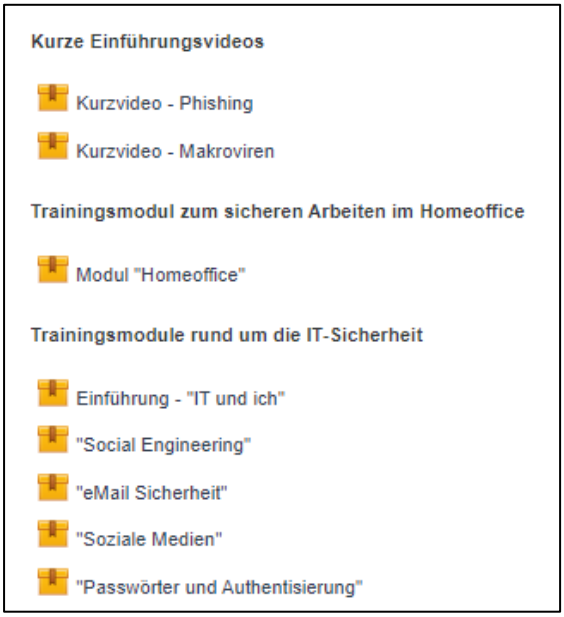
- Sorgen Sie dafür, dass **dienstliche Unterlagen sicher verwahrt** sind, wenn Sie den häuslichen Arbeitsplatz verlassen.
- Sorgen Sie für das Einspielen von Software-**Updates**, damit die von Ihnen genutzte Software stets aktuell und frei von bekannten Fehlern und Sicherheitslücken ist. Das gilt auch für private Geräte.
- **Vermeiden Sie den Transport dienstlicher Daten auf** unverschlüsselten **Wechseldatenträgern**. Nutzen Sie Speichermöglichkeiten wie das Z-Laufwerk, Alfresco, bwSyncAndShare und greifen Sie vom häuslichen Arbeitsplatz auf die gleichen Netzwerkspeicherorte zu wie im Büro. Datenträger, die Sie gar nicht erst transportieren, können Sie auch nicht verlieren.
- **Vermeiden Sie eine ausschließlich lokale Speicherung von Daten**. Datenverlust z.B. durch herunterfallende Geräte oder spielende Kinder ist vermeidbar, wenn Sie Daten auf zentral gewarteten Systemen der Hochschule speichern. Was nicht bei Ihnen lokal gespeichert ist, kann auch nicht lokal beschädigt werden.
- Wenn doch einmal etwas schiefgehen sollte, **melden Sie sich bei Ihrer EDV-Betreuung**. Dort wird Ihnen geholfen, bevor ein Schaden größer wird.

Sie können die Empfehlungen in längerer Fassung auch hier nachlesen: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/empfehlung_home_office.pdf?__blob=publicationFile

Im vergangenen Herbst haben wir unsere **Sensibilisierungsmaßnahme zu Phishing-Mails** fortgesetzt. Im Vergleich 2019 zu 2020 hat es Verbesserungen gegeben. Der Anteil derjenigen, die nicht auf zweifelhafte Links in E-Mails geklickt haben, ist von 83% auf 87% gestiegen. Allerdings hat sich gleichzeitig der Anteil geöffneter zweifelhafter Dateien auf niedrigem Niveau verdoppelt. Ebenfalls gestiegen ist der Anteil ausgeführter sogenannter Makros zweifelhafter Herkunft.

- Tipp 1: Die meisten Makro-Viren können Sie gut erkennen, wenn Sie auf die **Dateiendung** schauen. Endet die Dateinamenerweiterung – das ist die Buchstabenfolge nach dem letzten Punkt – auf ein "m", so kann die Datei ausführbare Makros enthalten. Für Microsoft Office sind das .docm, .xlsm, .pptm. Öffnen Sie solche Dateien nur, wenn Sie sie aus vertrauenswürdiger Quelle erhalten. Fragen Sie im Zweifel bei der Person nach, von der Sie vermuten, die Datei erhalten zu haben. Haben Sie eine Datei mit Makros geöffnet und sind Sie unsicher, ob diese Makro-Viren enthalten haben könnte, wenden Sie sich an IuK bzw. RZ.

- Tipp 2: Vermeiden Sie die veralteten Dateiformate doc, xls, ppt und speichern Sie Ihre Inhalte in den aktuellen Dateiformaten docx, xlsx, pptx. Die Dateiformate mit den Endungen auf x können keine ausführbaren Makros enthalten und sind damit sicherer als die alten Dateiformate ohne das x am Ende.



Für einen noch besseren Umgang mit E-Mails, Dateien und Makros stellen wir Ihnen eLearning-Module bereit, die Sie bequem in Moodle nutzen können:
Moodle → Rechenzentrum → Datenschutz und Informationssicherheit.

In kurzen Videos erhalten Sie umsetzbare Tipps für Ihren Arbeitsalltag im Büro und beim mobilen Arbeiten.
Die Videos stehen Ihnen **bis Ende Juni 2021** zur Verfügung.

https://moodle.htwg-konstanz.de/moodle/course/view.php?id=3737

D. Individuelle Schulungen zum Datenschutz

Um Ihnen den Einstieg zu erleichtern, bieten wir auch dieses Sommersemester ergänzend zum eLearning auch wieder ein Schulungsprogramm an.

Unsere Datenschutz-Expertin Frau jur. Ass. Inna Feldmann von der Stabsstelle Datenschutz wird Sie auf den aktuellsten Stand bringen.

Die Schulung ist aktuell als Online-Seminar geplant und findet an folgenden Terminen statt:

- Donnerstag, **27. Mai 2021**, 10.00 Uhr bis 11.30 Uhr

  https://htwg-konstanz.webex.com/htwg-konstanz/j.php?MTID=m3124686d95dfa0d8e3e35d96b868288e

  Meeting-Kennnummer (Zugriffscode): 121 869 7698

  Meeting Passwort: R54yivtbJW7

  Über Telefon beitreten
  +49-619-6781-9736

- Donnerstag, **24. Juni 2021**, 10.00 Uhr bis 11.30 Uhr

  https://htwg-konstanz.webex.com/htwg-konstanz/j.php?MTID=m8b4dc504d4cbb927e489a0bf321255ec

  Meeting-Kennnummer (Zugriffscode): 121 270 4884

  Meeting Passwort: WyTVsStf686

  Über Telefon beitreten
  +49-619-6781-9736

Wir freuen uns auf Ihre rege Teilnahme!

Beste Grüße und bis zum nächsten Newsletter.

Ihre Prof. Dr. Marc Strittmatter und Prof. Dr. Hanno Langweg