Hochschule Konstanz
Technik, Wirtschaft und Gestaltung

Prof. Dr. Marc Strittmatter
Datenschutzbeauftragter

Prof. Dr. Jürgen Freudenberger
Informationssicherheitsbeauftragter

2. Newsletter

des Informationssicherheitsbeauftragten

und

des Datenschutzbeauftragten an der HTWG

vom 21.03.2019

Die Themen:

- Umgang mit Auskunftsersuchen nach Datenschutzgrundverordnung
- Grundsätze des Datenschutzrechts
- Handreichung Bilder, Fotos, Social Media
- Sensibilisierungsmaßnahmen
- Termine

Liebe Professorinnen und Professoren, liebe Mitarbeiterinnen und Mitarbeiter,

wir freuen uns, Ihnen unseren zweiten Newsletter mit Beiträgen zu einem sicheren und rechtmäßigen Umgang mit personenbezogenen Daten an der HTWG übermitteln zu können.

Möchten Sie gern wissen, wie Sie vorgehen sollen, wenn ein Studierender Auskunft zu seinen an der HTWG gespeicherten Daten verlangt?

Oder haben Sie sich in Ihrem Arbeitsalltag schon einmal gefragt, ob und unter welchen Voraussetzungen es zulässig ist, Fotos von z.B. Studierenden auf Ihrer Internetseite zu veröffentlichen?

Auf diese und weitere Fragen zum Datenschutz finden Sie Antwort in unserem Newsletter.

Die Themen:

- Umgang mit Auskunftsersuchen nach Datenschutzgrundverordnung
- Grundsätze des Datenschutzrechts (Teil 2)
- Handreichung Bilder, Fotos, Social Media
- Datenschutz bei Anfragen zu Studierenden von Behörden, Privatpersonen (z.B. Eltern) usw.
- Schulungen
- Sensibilisierungsmaßnahme zu Phishingmails und aktuelle Warnhinweise des Innenministeriums
- Änderungen für die Nutzung von eduroam ab dem Sommersemester 2019
- Links zu weiteren Informationen im Intranet

Wir wünschen Ihnen eine interessante Lektüre!

A. Umgang mit Auskunftsersuchen nach Datenschutzgrundverordnung

Wie muss reagiert werden, wenn eine Person ein Auskunftsersuchen zu ihren an der HTWG verarbeiteten Daten einreicht?

Die DSGVO hat den Betroffenenrechten einen sichtbareren Platz gegeben. Dazu gehört auch, dass wir als Hochschule in der Lage sein müssen, Auskunftsansprüche zeitnah zu erfüllen.

1. Da eine Antwort an den Betroffenen innerhalb eines Monats erfolgen muss, sollten solche Anfragen sofort nach Eingang zügig bearbeitet werden.

2. Zunächst sollte geprüft werden, ob von der Person überhaupt personenbezogene Daten an der HTWG gespeichert werden. Welchen Status hat die Person an der HTWG? An welchen Stellen an der HTWG könnten Daten zu dieser Person gespeichert sein?

3. Sodann sollen folgende Informationen an den Datenschutzbeauftragten der HTWG, E-Mail-Adresse dsb@htwg-konstanz.de, weitergeleitet bzw. geschickt werden:

    - ursprüngliche Anfrage inkl. Kontaktangaben
    - Angabe wann und in welcher Form die Anfrage einging
    - Status der anfragenden Person an der HTWG
    - Stellen an der HTWG, an denen Daten der Person gespeichert sein könnten, idealerweise auch die zugehörigen Verarbeitungsvorgänge.
    - Ein vollständiger Auszug aus den ggf. vorhandenen Akten muss noch nicht mitgeschickt werden.

4. Der Datenschutzbeauftragte wird sich ggf. mit weiteren Fragen an Sie wenden.

B. Grundsätze des Datenschutzrechts (Teil 2)

1. Datensicherheit

Nach der DSGVO müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet, einschließlich dem Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung. Dies erfolgt durch geeignete Technische und Organisatorische Maßnahmen.

Zu den technischen Maßnahmen gehören z.B. der Einsatz einer Firewall, regelmäßige Software-Updates, das Verschlüsseln von Festplatten, USB-Sticks oder E-Mail-Inhalten gegen den unbefugten Zugriff. Diese sind zum Teil bereits bei Bereitstellung der technischen Infrastruktur in der Hardware enthalten oder werden im Rahmen des Server- und Netzbetriebs zentral gesteuert und eingesetzt.

Ebenso wichtig sind organisatorische Maßnahmen, die jeder Mitarbeitende umsetzen sollte. Hierzu zählen z.B. die Vergabe ausreichender Passwörter, das Sperren des PCs und Abschließen des Raumes gegen unbefugten Zugriff auf Daten oder daran zu denken, einen Laptop nicht im heißen Pkw liegen zu lassen, gegen unbeabsichtigten Datenverlust.

Insbesondere bei den organisatorischen Maßnahmen ist jeder Mitarbeitende täglich gefragt!

2. Rechenschaftspflicht

Jeder Verantwortliche muss die Einhaltung aller Datenverarbeitungsgrundsätze nachweisen können. Das bedeutete, dass eine lückenlose Dokumentation über alle Verarbeitungsvorgänge an der HTWG geführt werden sollte.

Hierzu gehört zum Beispiel das Anlegen einer Beschreibung für eine Verarbeitungstätigkeit, aber auch das Dokumentieren einer abgegebenen Einwilligung, oder dass dem Betroffenen eine Datenschutzinformation zur Verfügung gestellt wurde. Ebenfalls muss das datenschutzgerechte Löschen von Daten anhand von Aufzeichnungen nachvollzogen werden können.

Die Umsetzung der Rechenschaftspflicht erfolgt im Wesentlichen in den einzelnen Bereichen der HTWG bei den Mitarbeitenden, die personenbezogene Daten verarbeiten. Hierfür kann es helfen, eine geeignete Dokumentationsstruktur zu erarbeiten.

3. Datenschutzgerecht Löschen

Sollen oder müssen personenbezogene Daten gelöscht werden, muss dies datenschutzgerecht, das heißt permanent erfolgen. Es genügt z.B. nicht, eine Datei in den „Papierkorb“ zu verschieben. Eine Datei ist i.d.R. erst dann von einem Datenträger dauerhaft gelöscht, wenn dieser mechanisch zerstört wurde oder die Datei z.B. mit einem speziellen Löschprogramm wie „Eraser“ mehrfach überschrieben wurde, so dass sie nicht mehr wiederhergestellt werden kann.

Achten Sie auch beim Vernichten von Papierakten darauf, dass dies auf geeignetem Weg erfolgt. Nutzen Sie spezielle Papiercontainer an der HTWG, die gegen Entnahme gesichert sind und deren Inhalt professionell entsorgt wird. Möchten Sie Unterlagen selbst schreddern, achten Sie auf eine kleine Teilchengröße, bei der ein späteres Zusammenfügen ausgeschlossen werden kann.

C. Handreichung Bilder, Fotos, Social Media

Berichte über Veranstaltungen, Exkursionen oder Studierende an der HTWG leben häufig von der Illustration durch Fotos. Damit die Aufnahme und Veröffentlichung der Bilder dem geltenden Datenschutzrecht entspricht, müssen verschiedene Aspekte beachtet werden.

Welche das sind, sowie Muster für eine Einwilligung und Datenschutzinformation, erfahren Sie in der Handreichung zu diesem Thema.

Die Handreichung finden Sie unter https://www.htwg-konstanz.de/datenschutz/newsletter-handreichungen-und-links/

D. Datenschutz bei Anfragen zu Studierenden von Behörden, Privatpersonen (z.B. Eltern) usw.

Wie verhalte ich mich, wenn mich eine Anfrage zu Studierendendaten von Dritten, z.B. einer Behörde erreicht? Muss ich Eltern Auskunft geben? Wann darf ich eine Auskunft erteilen und was muss ich hierbei beachten?

Diese Fragen beantwortet eine Handreichung zum Thema „Anfragen zu Studierenden von Behörden, Privatpersonen usw.“.

Die Handreichung finden Sie unter https://www.htwg-konstanz.de/datenschutz/newsletter-handreichungen-und-links/

E. Sensibilisierungsmaßnahme zu Phishingmails

Wie in den Medien und auch in der Hochschule beobachtet werden konnte, ist die Verbreitung von Schadsoftware im vergangenen Jahr stark angestiegen. Ein wichtiges Einfallstor hierbei sind glaubhaft gestaltete E-Mails mit der Absicht, den Nutzer zum Klicken eines Links oder zum Öffnen eines Dokumentes zu verleiten und so die Nutzerdaten abgreifen oder schädliche Software installieren zu können. Als erste Maßnahme zur Schulung und Sensibilisierung vor diesen Gefahren lief eine Kampagne, bei der Hochschulangehörigen Mails zugestellt wurden, die einen echten Angriff simulieren. Anstatt eine schädliche Aktion auszuführen, wurde den Benutzern bei einer versehentlichen Öffnung gezeigt, woran sie den Betrug hätten erkennen können.

Im Rahmen dieser Maßnahme wurden an eine Gruppe von 100 zufällig ausgewählter Teilnehmer E-Mails versendet, um aktuelle Phishing-Angriffe zu simulieren und Reaktionen wie das Öffnen eines Links zu provozieren. Die im Rahmen des Trainings gewonnenen Daten wurden anonymisiert und gruppenbasiert ausgewertet, es kann an keiner Stelle Rückschluss auf Ihr persönliches Verhalten gezogen werden. Nach Abschluss der Auswertung wurde jeglicher Personenbezug gelöscht.

Leider wurde bei rund 63% der Teilnehmer ein kritisches Verhalten beobachtet!

WICHTIG:
Wenn Sie in einer verdächtigen Nachricht auf einen Link geklickt oder einen Anhang geöffnet haben und Sie haben keine Erklärseite von IT-Seal gesehen, so trennen Sie Ihr Gerät bitte umgehend vom Netzwerk und benachrichtigen Sie Ihren EDV Betreuer.

F. Schulungen

Auch für das Sommersemester 2019 sind Schulungen zum Thema Datenschutzrecht und IT-Sicherheit für den 17. April und 19. Juni jeweils von 10 bis 12 Uhr geplant. Die Räume werden rechtzeitig per E-Mail und auf der Seite des Datenschutzbeauftragten www.htwg-konstanz.de/datenschutz bekannt gegeben.

G. Zertifikate für eduroam verlieren 2019 ihre Gültigkeit

Die Nutzung des WLAN der Hochschule erfolgt über den Dienst "eduroam". Die hierfür benötigten Zertifikate werden im Frühsommer ungültig. Daher muss der Zugang auf allen Geräten neu eingerichtet werden. Zu Beginn des Sommersemesters 2019 wird das Rechenzentrum ausführlich hierzu informieren.

H. Neuer Bereich im Intranet mit Dokumenten zur Informationssicherheit

Im Intranet wurde unter

http://intranet.htwg-konstanz.de/Datenschutz-und-Informationssi.749.0.html

ein neuer Bereich für Dokumente zum Thema Datenschutz eingerichtet. Hier finden Sie die Verwaltungsvorschrift zu Informationssicherheit, die Präsidiumsrichtlinie zur Informationssicherheit und weitere Dokumente der Landesverwaltung.

I. Empfehlungen des Innenministeriums zum Schutz der eigenen privaten Daten

Anlässlich des jüngsten, medial sehr präsenten Daten-Leaks hat das Innenministerium Baden-Württemberg Hinweise zum Schutz von Daten veröffentlicht. Bei diesem

Daten-Leak wurden persönliche Daten deutscher Europa-, Bundes- und Landespolitiker und weiterer Personen des öffentlichen Lebens im Internet veröffentlicht. Die Hinweise finden Sie ebenfalls im Intranet:

http://intranet.htwg-konstanz.de/index.php?eID=tx_nawsecuredl&u=243&file=fileadmin/intranet/hochschule/Datenschutz_und_Informationssicherheit/Empfehlungen_zum_Schutz_eigener_Daten.pdf&t=1548181024&hash=596aa195393ffd20e360d5615cd7d07d437d157d

J. Warnung vor Spam-Mails mit Absenderadressen aus Organisationen in der Landesverwaltung

Aktuell sind im Landesverwaltungsnetz wieder vermehrt Spam-Mails mit Links im Umlauf, über die Schadprogramme verbreitet werden. Die Spam-Mails sind oft als Rechnungs-Mails getarnt und mit gefälschten Absenderangaben versendet.

Bitte um Vorsicht:

Die Absenderadressen sind oft **mit Absenderadressen aus Organisationen in der Landesverwaltung gefälscht**. Oft sind die SPAM-Mails bereits im Betreff mit „SPAM-Verdacht BITBW“ gekennzeichnet. Bei solchen E-Mails bitte besonders vorsichtig sein.

Die Absender- und Empfängerangaben enthalten häufig konkrete Organisationsbezeichnungen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) geht davon aus, dass die Absender- und Empfängerangaben inkl. Organisationsbezeichnungen auf infizierten Systemen von Nutzern ausgespäht wurden, an die in der Vergangenheit E-Mails von betroffenen Empfängern versendet wurden.

Der Betreff und der Text der E-Mails variieren. In manchen wird angegeben, dass sich im Anhang eine Rechnung befände, in anderen, dass ein Überweisungsbeleg anbei sei oder die gewünschten Dokumente. Tatsächlich handelt es sich stattdessen um einen Link. Beim Aufruf des Links wird Schadsoftware auf dem Rechner installiert, die höchstwahrscheinlich einen Verschlüsselungstrojaner nachlädt.

Beste Grüße und bis zum nächsten Newsletter.

Ihre

Prof. Dr. Marc Strittmatter und Prof. Dr. Jürgen Freudenberger