Prof. Dr. Hanno Langweg
Informationssicherheitsbeauftragter

Prof. Dr. Marc Strittmatter
Datenschutzbeauftragter

Newsletter Wintersemester 2024/2025

Themen u.a.

- Auskunftsersuchen von Dritten
- KI und Datenschutz
- Neues aus der Informationssicherheit

Liebe Mitglieder und Angehörige der Hochschule,

willkommen zu einer neuen Ausgabe des gemeinsamen Newsletters des Datenschutzbeauftragten und des Informationssicherheitsbeauftragten für das Wintersemester 2024/2025. Wie immer haben wir Ihnen aktuelle und wichtige Themen zusammengestellt. Dies gibt Ihnen einen Einblick in Datenschutz und Informationssicherheit und auch einige praktische Tipps für Ihren Arbeitsalltag.

Unsere Aufgabe als Hochschule ist es, jungen Menschen eine gute Ausbildung zu ermöglichen. Dafür brennen wir, dafür stehen wir, dafür setzen wir uns ein. Gleichzeitig gibt es Anforderungen rechtlicher und finanzieller Natur, die keinen unmittelbaren offensichtlichen Bezug zu unserer Hauptaufgabe als Hochschule haben. Brandschutz, Denkmalschutz, Datenschutz & Informationssicherheit – in allen diesen Bereichen sind wir an der HTWG bestrebt, pragmatische Lösungen zu finden, einen funktionierenden, effizienten und gleichsam sicheren wie rechtskonformen Betrieb zu ermöglichen. Was im Einzelfall manchmal vorschnell als unnötige Beeinträchtigung wahrgenommen wird, reduziert Risiken und dient der Aufrechterhaltung der Funktionsfähigkeit in schwierigen Situationen.

Risiken zu reduzieren schafft mehr Verlässlichkeit in einer sich wandelnden Welt.

Gerne empfehlen wir Ihnen das eLearning zum Datenschutz in Moodle und die Portalseite Informationssicherheit auf unserer Homepage.

Beste Grüße und Freude beim Lesen wünschen

Marc Strittmatter (DSB) und Hanno Langweg (ISB)

Inhaltsverzeichnis

A. News / Aktuelles

Informationen Datenschutz: Handreichungen, Vorlagen, Downloads im Intranet

An Hochschulen finden viele Prozesse statt, die personenbezogene Daten* beinhalten und bei denen diese Daten in verschiedensten Formen verarbeitet werden.

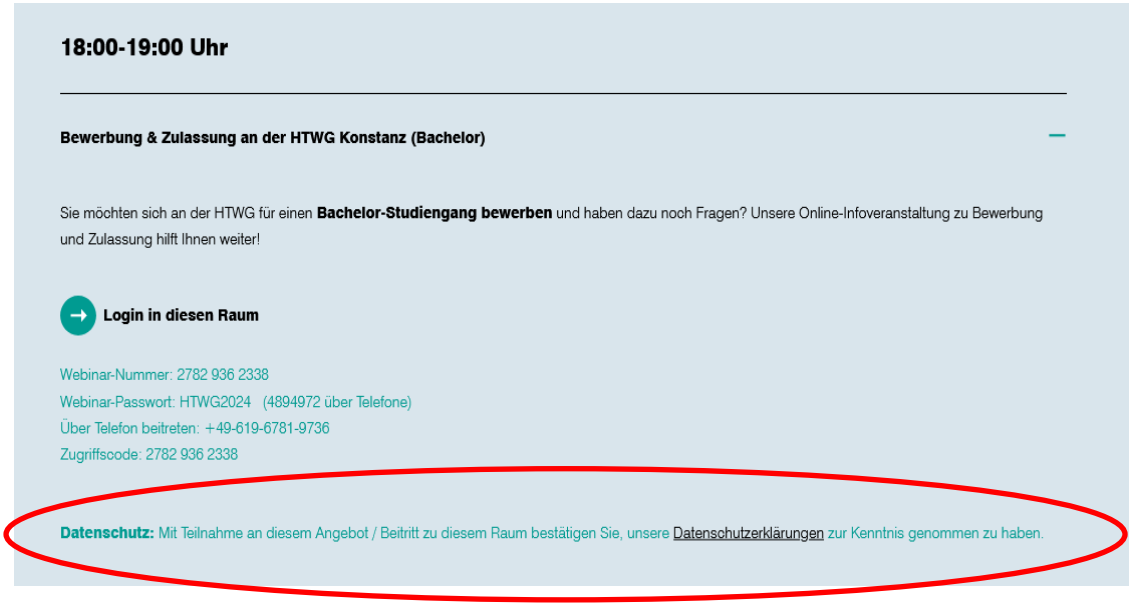
Das reicht von **Umfragetools** und **Anmeldemasken auf der Website** über **Listen mit Namen** bis zum **Veranstaltungsmanagement**. Und es **betrifft Studierende, Mitarbeitende und Dritte** (e.g. Kunden, Lieferanten, Kooperationspartner)

Sobald wir hier personenbezogene Daten verwenden (und das ist fast immer der Fall!), müssen verschiedene datenschutzrechtliche Anforderungen erfüllt werden.
Eine davon ist die **Erstellung und Zurverfügungstellung einer Datenschutzinformation**, mit der Betroffene* über die Verarbeitung ihrer Daten* und Rechte informiert werden.

Die **Vorlage unseres allgemeinen Datenschutzhinweises** (mit Ausfüllhilfen) finden Sie unter:

https://intranet.htwg-konstanz.de/arbeitskreise/initiativen/datenschutz/mustertexte-und-handreichungen

Platzieren Sie diesen Hinweis, ggf. über einen gut sichtbaren Link, direkt bei Ihrem Verarbeitungsprozess, also z.B. in einer Einladungsmail oder bei einer Veranstaltungseinladung auf der Website, wie zum Beispiel hier der Datenschutzhinweis zu WebEx (diesen finden Sie auch im Downloadbereich):



18:00-19:00 Uhr

Bewerbung & Zulassung an der HTWG Konstanz (Bachelor)

Sie möchten sich an der HTWG für einen **Bachelor-Studiengang bewerben** und haben dazu noch Fragen? Unsere Online-Infoveranstaltung zu Bewerbung und Zulassung hilft Ihnen weiter!

Login in diesen Raum

Webinar-Nummer: 2782 936 2338
Webinar-Passwort: HTWG2024 (4894972 über Telefone)
Über Telefon beitreten: +49-619-6781-9736
Zugriffscode: 2782 936 2338

Datenschutz: Mit Teilnahme an diesem Angebot / Beitritt zu diesem Raum bestätigen Sie, unsere Datenschutzerklärungen zur Kenntnis genommen zu haben.

*zu den genannten Begriffen finden Sie in unseren Schulungen Erklärungen und in unserem Schulungsscript

Erstellen Sie zu Prozessen, bei denen personenbezogene Daten verarbeitet werden, immer einen entsprechenden Datenschutzhinweis gem. Art 13 DSGVO.

Betroffene Personen müssen immer informiert werden, wenn deren Daten in irgendeiner Weise verarbeitet werden: von Erhebung bis Löschung umfasst das den gesamten Verarbeitungszyklus.

B. Wichtige Verfahren an der HTWG mit Blick auf den Datenschutz

Künstliche Intelligenz und Datenschutz: Ein Balanceakt

Der Siegeszug der Künstlichen Intelligenz (KI) ist weiterhin ungebremst. Besonders Sprachassistenten (sog. Large Language Models) erhalten Einzug in den Arbeitsalltag in Behörden und Unternehmen. Angesichts der ungeheuren Datenmengen mit denen diese gespeist werden, stellt sich unweigerlich die Frage, wie KI datenschutzkonform eingesetzt werden kann?

Zuerst stellt sich die Frage, nach welchem Kriterium eine KI-Anwendung überhaupt ausgewählt werden sollte. Dabei ist zwischen geschlossenen und offenen Systemen zu unterscheiden. Bei geschlossenen Systemen hat nur der Anwenderkreis Kontrolle über die Ein- und Ausgabedaten, während bei offenen Systemen die eingegebenen und entstehenden Daten vom Anbieter des Systems zum weiteren Training der KI verwendet werden. Im letztgenannten Fall besteht ein hohes Risiko, dass eine Offenlegung personenbezogener Daten stattfindet. Technisch geschlossene Systeme sind daher immer vorzugswürdig.

Schritte für die rechtskonforme Verwendung von Künstlicher Intelligenz

1. Klärung der Verantwortlichkeit im Sinne der Datenschutz-Grundverordnung
Verantwortlich ist immer derjenige, der über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet. In Frage kommt eine alleinige Verantwortlichkeit, ein Vertragsverhältnis zwischen dem Verantwortlichem und einem Auftragsverarbeiter oder eine gemeinsame Verantwortlichkeit.

2. Erfüllung der Transparenz- und Informationspflichten
Der Anbieter der KI-Anwendung muss hierfür ausreichende Informationen bereitstellen. Ebenso ist transparent zu machen, ob Texteingaben von Nutzern gespeichert werden, um den Dialog zu einem späteren Zeitpunkt wieder aufnehmen zu können.

3. Festlegung in welchen Bereichen und zu welchen Zwecken die Anwendung erfolgen soll
Dies ist entscheidend, um eine Verarbeitung personenbezogener Daten datenschutzrechtlich rechtfertigen zu können. Achtung! Personenbezogene Daten liegen auch schon dann vor, wenn keine konkreten persönlichen Daten eingegeben werden, sich jedoch aus dem Zusammenhang ein Bezug zu betroffenen Personen herstellen lässt.

4. Ohne Rechtsgrundlage geht es nicht
Für jedwede Form der Verarbeitung (Ordnen, Speichern, Verändern, etc.) von personenbezogenen Daten ist eine gesetzliche Grundlage erforderlich. Diese liegt bspw. bei Einwilligung der betroffenen Person oder bei Wahrnehmung der öffentlichen Aufgabe durch eine Hochschule nach dem Landeshochschulgesetz vor.

Auch wenn diese Voraussetzungen vorliegen, dürfen Entscheidungen, die Rechtswirkung entfalten, nicht lediglich von einer KI getroffen werden.

Beispiel: Eine KI-Anwendung, die über die Zulassung und Ablehnung von Studienbewerbern an unserer Hochschule entscheiden würde, wäre unzulässig. Denkbar wäre aber, dass eine KI solche Bewerbungen entgegennimmt, vorsortiert und einen ersten Vorschlag bezüglich einer Zulassung macht. Dieser Vorschlag ist von einem Menschen eingehend zu prüfen und anschließend zu bestätigen oder abzulehnen

Wichtige Punkte bei der Nutzung von KI im betrieblichen Kontext:

- Unterstützung/ Sensibilisierung von Mitarbeitern durch interne Handlungsanweisungen und Schulungen
- Einrichtung von betrieblichen Accounts

Die Ergebnisse von KI-Anwendungen sind dabei stets kritisch zu hinterfragen, da sie keinen Anspruch auf Richtigkeit besitzen und unter Umständen sogar zu unzulässiger Verarbeitung z.B. wegen Diskriminierung führen können.

Für weitergehende Informationen rund um eine mögliche Einbindung von ChatGPT in den Lehrbetrieb an unserer Hochschule können Sie gerne den passenden Artikel (S. 5-7) in unserem Newsletter aus dem Wintersemester 23/24 lesen.

Verwendete Quelle: https://www.datenschutzkonferenz-online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf

C. Check-Up´s zum Datenschutz!

Wann bindet man das Team Datenschutz in die Prüfung einer neuen Anwendung oder eines Tools ein? Kommunikationstools – Go oder No-Go?!

Ein neues Tool für die interne Kommunikation zu nutzen erscheint sehr verlockend – es verkürzen sich Zeiten und Wege, Abstimmungen erfolgen zeitnah und alle sind eingebunden.

Auch eine Anwendung, die ein Management von Daten vereinfacht und Zugriff Aller leicht ermöglicht, scheint doch etwas Gutes zu sein!

Der Haken bei der ausgesuchten IT-Anwendungen ist aber möglicherweise, dass z.B. der Anbieter in den USA sitzt oder in einem anderen außereuropäischen Land. Oder die vertraglichen Bestimmungen zur Auftragsverarbeitung ungenau sind. Oder ein anderes datenschutzrechtliches Problem vorliegt.

Die DSGVO sieht vor, dass bei Nutzung von Anwendungen, bei denen personenbezogene Daten verarbeitet werden, besondere Datenschutzbestimmungen vorliegen sollen, die geprüft werden müssen.

Im schlechtmöglichsten Fall kommt man nach dieser Prüfung zum Ergebnis, dass die ausgesuchte Anwendung nicht datenschutzkonform ist und daher nicht genutzt werden darf.

Das würde für Sie, wenn Sie die Anwendung bereits betreiben, bedeuten, dass Sie den Betrieb damit einstellen müssen, wenn diese Anwendung nicht vom Datenschutzbeauftragten freigegeben wird.

Um dies zu vermeiden, fragen Sie das TEAM Datenschutz bitte immer VOR Nutzung eines Tools, wie und ob Sie eine dafür Freigabe erreichen können.

D. Neues aus der Informationssicherheit

Grundlagenschulung Cybersicherheit

Die Schulung "Grundlagen der Cybersicherheit" bietet Ihnen einen leicht verständlichen Einstieg in die Thematik der Cybersicherheit. Dieser umfasst zunächst einen Überblick über die relevantesten Grundbegriffe. Darüber hinaus räumt die Schulung mit dem Stereotyp des "typischen Hackers" auf, der mit schwarzem Hoodie und Kapuze vor dem PC sitzt und gezielt und händisch einzelne Ziele angreift.

Die Vorstellung verschiedener Gruppierungen von Angreifenden sowie deren Motive für einen Angriff sind Teil der Schulung. Um den Wissenstransfer von der Theorie in die Praxis zu erleichtern, werden anhand aktueller Angriffsbeispiele die verschiedenen Angriffsvektoren beschrieben und Schutzmaßnahmen für die Beschäftigten sowie die Institution abgeleitet.

Neben diesen Schutzmaßnahmen steht das Erkennen von Angriffen anhand ihrer typischen Merkmale ebenso im Mittelpunkt der Schulung wie der Abbau von Hemmschwellen, einen Verdachts- oder konkreten Vorfall zu melden.

Die Schulung durch die Cybersicherheitsagentur Baden-Württemberg ist darauf ausgelegt, auf einer niederschwelligen Basis grundlegendes Wissen zur Cybersicherheit zu vermitteln und kann daher ohne Vorkenntnisse besucht werden.

Datum: Montag, 09.12.2024
Uhrzeit: 10:00-11:30 Uhr
Raum: Online
Zielgruppe: alle
Anmeldung bis 02.12.2024 unter: fortbildung@htwg-konstanz.de

CSBW CYBER SICHERHEITS AGENTUR BADEN-WÜRTTEMBERG

Notfallhandbuch

Es ist keine Frage, ob unsere Hochschule einen Angriff auf ihre IT-Systeme erleben wird, sondern wann. Auch Hochschulen, die mehr in präventive Informationssicherheit investieren als die HTWG, wurden in der Vergangenheit erfolgreich angegriffen. In solchen Situationen kommt es darauf an, schnell handeln zu können. Es geht um die Begrenzung von Schäden, um das Aufrechterhalten der nötigsten Funktionen und eine Wiederherstellung eines geordneten Betriebs. In der akuten Situation eines Informationssicherheitsvorfalls stellen sich viele Fragen und die Belastung der Beschäftigten ist groß.

Da hilft es, vorbereitet zu sein. Im IT-Notfall-Handbuch sind Verantwortlichkeiten, Reaktionen und Kommunikationswege festgelegt. Z.B. werden wir beim Ausfall unserer IT-Systeme über eine Notfall-Website kommunizieren: https://www.htwg-backup.de/. (Im Moment ist diese Homepage absichtlich noch nicht in Betrieb).

Wichtig sind auch eine schnelle Erkennung und Meldung eines möglichen Angriffs. Hinweise, Anzeichen und Erste-Hilfe-Empfehlungen für solche Szenarien finden Sie hier:

https://www.cybersicherheit-bw.de/sites/default/files/2024-04/CSBW-Factsheet_Informationssicherheitsvorfall_erkennen.pdf und praktische Tipps, was zu tun ist, hier: https://www.cybersicherheit-bw.de/sites/default/files/2024-04/CSBW-Factsheet_Erste_Hilfe_Cybernotfall.pdf

Das IT-Notfall-Handbuch finden Sie im Intranet: https://www.htwg-konstanz.de/hochschule/einrichtungen/informationssicherheit/. (Für den Link ist immer noch eine Vorab-Anmeldung im Intranet notwendig.) Schauen Sie sich das Handbuch bereits jetzt an. Im Fall eines Angriffs auf unsere IT-Systeme kann es gut sein, dass Sie auf die elektronische Fassung nicht werden zugreifen können.

Übung Krisenstab

Papier (oder eine PDF-Datei) ist geduldig. In den Worten des griechischen Philosophen Archilochos (680-645 v.Chr.): "Wir erreichen nicht das Niveau unserer Erwartungen, sondern fallen zurück auf das Niveau unseres Trainings." Daher hat der IT-Krisenstab geübt, wie wir an der Hochschule mit der Meldung eines fiktiven Notfalls umgehen. Wir haben erlebt, was schon reibungslos klappt. Wir haben aber auch notiert, was noch nicht auf Anhieb funktioniert hat, wo Prozesse noch nicht klar definiert sind, und was wir erneut üben sollten. An dieser Stelle herzlichen Dank an alle Beteiligten! Nicht nur die Mitglieder des IT-Krisenstabs haben mitgespielt, auch viele Beschäftigte aus unterschiedlichen Abteilungen der HTWG waren in das Szenario eingebunden. Für die Zukunft planen wir weitere Übungen: "Wie trennen wir das Hochschulnetz vom Internet und was funktioniert dann noch?" und "Wie aufwendig ist die Wiederherstellung eines Servers in der Praxis?"

Schwachstellen-Scans für IT-Systeme

Angriffe auf IT-Systeme von Hochschulen beruhen häufig auf der Ausnutzung von Schwachstellen. Dabei sind es gar nicht mal besonders ausgefuchste Angriffe, sondern vielfach Software, die in einer veralteten Version eingesetzt wird, für die Schwachstellen bekannt sind. Viel wäre damit getan, überall aktuelle Softwareversionen einzusetzen. Für die zentral gewarteten IT-Systeme haben wir das gut im Griff. Eine Herausforderung sind dezentral betriebene Server, Projekthomepages, individuelle Laptops usw. Es ist keine böse Absicht und auch kein Unvermögen, dass hier veraltete Software eingesetzt wird. Der Fokus in der Benutzung liegt schlicht auf anderen Prioritäten. Da diese Systeme im Hochschulnetz betrieben werden, sind sie aus Angreifenden Sicht attraktive Ziele, um von dort aus wertvollerem Server und Datenbestände der Hochschule zu erreichen.

Zur Unterstützung derjenigen, die dezentrale IT-Systeme betreiben, haben wir in der Vergangenheit Schwachstellen-Scans ausgeführt und Ergebnisse bereitgestellt. Das wollen wir in der Zukunft verstetigen durch regelmäßige Scans und durch die Erwartung, dass dabei erkannte Schwachstellen rasch behoben werden. Vielfach reicht ein Update der vorhandenen Software aus.

Sie können schon jetzt etwas tun. Prüfen Sie z.B. für von Ihnen betriebene Projekthomepages, ob Ihre Wordpress-Version aktuell ist. Sind auch alle Plugins aktuell? Verwenden Sie für Ihre Projekthomepage ausreichend lange Passwörter für Benutzerkonten? Alle Passwörter an der Hochschule haben eine Länge von 14 Zeichen als Mindestanforderung. Denken Sie darüber nach, ob Sie mit Ihrer Projekthomepage in das zentrale CMS der Hochschule umziehen können. Ja, da gibt es weniger Flexibilität bei der Nutzung von Plugins. Auf der anderen Seite haben Sie keinen Aufwand, sich um die Aktualisierung der technischen Plattform kümmern zu müssen.

Melden Sie auch in Ihrem eigenen Interesse jeden Informationssicherheitsvorfall. Dann steht Ihnen im Fall der Fälle die geballte Expertise der Hochschule zur Verfügung.

Portal Informationssicherheit

An dieser Stelle erinnern wir an die Portalseite der HTWG zur Informationssicherheit: https://www.htwg-konstanz.de/hochschule/einrichtungen/informationssicherheit/. Dort finden Sie praktische Tipps, wie Sie an Ihrem Arbeitsplatz zu einem sicheren Betrieb der IT-Systeme und Verfahren an der Hochschule beitragen können. Empfehlungen für die IT zu Hause oder beim mobilen Arbeiten sind auch dabei. Falls doch einmal etwas passiert, können Sie über die Seite unkompliziert einen Informationssicherheits- oder Datenschutzvorfall melden. Je früher Sie einen Vorfall melden, desto schneller kann die Hochschule reagieren und eine Ausbreitung auf weitere IT-Systeme steuern.

E. Datenschutz-Awareness – Schulungen und Qualifizierungen mit dem Team Datenschutz

Neue Termine für Datenschutz-Schulungen

Erste-Hilfe-Datenschutz

Auch dieses Semester bieten wir wieder ein spannendes **Schulungsprogramm** an.

Wir möchten Ihnen laufend und zur Erhaltung der Awareness zum Thema „Datenschutz generell und Umgang mit personenbezogenen Daten an der Hochschule“ die Möglichkeit bieten, an unseren Schulungen teilzunehmen.

Wir haben als Ansatz dazu implementiert, dass diese Schulungen als Teil des Onboarding-Prozesses an der HTWG fest verankert sind.

Unsere ReferentInnen aus dem Team Datenschutz werden Ihnen den sicheren Umgang mit personenbezogenen Daten an der HTWG näherbringen und/oder auffrischen und stehen Ihnen bei Fragen zur Verfügung.

Die **Schulung** zu **grundlegendem Wissen im Datenschutz** können Sie im WS 24/25 **entweder** als **Präsenz- oder als Online-Schulung** (jeweils gleicher Inhalt) absolvieren.

Termine:

- **13.12.2024, 10.00 Uhr bis 12.00 Uhr | Präsenztermin**

Raum: **OTL F007**
Anmeldung bis 5.12.24 zum über:
Inna Feldmann <ifeldman@htwg-konstanz.de>
30 Plätze - Anmeldung nach Windhundprinzip

- **20.02.2025, 15:00 Uhr bis 17.00 Uhr | Online**

Meeting-Link: https://htwg-konstanz.webex.com/meet/ifeldman

Anmeldung bis 15.02.2025 zum über:
Inna Feldmann <ifeldman@htwg-konstanz.de>

(Bitte informieren Sie sich ab dem 15.11.2024 auf https://www.htwg-konstanz.de/datenschutz/schulungstermine über mögliche Änderungen)

Bitte benachrichtigen Sie Ihre/n Vorgesetze/n und ggf. Vertretung kurz über Ihre Anmeldung.

Qualifizierung mit dem kleinen „Datenschutzführerschein" – Neuer Link!
Wir zeigen Ihnen in unserem kompakten eLearning, welche Datenschutzgrundsätze Sie kennen müssen und wir helfen Ihnen, Ihr Datenschutz-Knowhow digital zu stärken!

Qualifizieren Sie sich für den **kleinen „Datenschutzführerschein"** auf
https://moodle.htwg-konstanz.de/moodle/course/view.php?id=1521

Mit **wenigen Klicks werden Sie fit in den Grundzügen des Datenschutzrechts.** Mit unserem webbasierten eLearning zum Datenschutz für Mitarbeitende an der HTWG verschaffen Sie sich mehr Kenntnisse für den sicheren Umgang mit Daten in Ihrem Arbeitsalltag an der Hochschule.

Lassen Sie uns gemeinsam die Datenschutz-Awareness an der HTWG stärken!

Wir freuen uns auf Ihre rege Teilnahme!

Beste Grüße und bis zum nächsten Newsletter.

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