

Prof. Dr. Hanno Langweg
Informationssicherheitsbeauftragter

Prof. Dr. Marc Strittmatter
Datenschutzbeauftragter

4. Newsletter

des Informationssicherheitsbeauftragten und des Datenschutzbeauftragten an der HTWG

vom 28.06.2022

Themen u.a.:

- **News / Aktuelles**
- **DSGVO-Konformität neuer digitaler Verfahren**
- **Datenpanne – was tun?**
- **Tipps zur Informationssicherheit**
- **Datenschutz-Schulungstermine**

IMZ – Newsletter Sommersemester 2022

**des Informationssicherheitsbeauftragten
und des Datenschutzbeauftragten an der HTWG im Juni 2022**

Liebe Professorinnen und Professoren, liebe Mitglieder der Hochschule,

im Sommersemester 2022 möchten wir Ihnen wieder die aktuelle Ausgabe des gemeinsamen Newsletters des Datenschutzbeauftragten und des Informationssicherheitsbeauftragten mit Themen aus den Bereichen Datenschutz und IT-Sicherheit vorstellen.

A.	Team Datenschutz an der HWTG	2
B.	News / Aktuelles	3
	„Fakultäten-VVT“	3
C.	Neue digitale Verfahren: „Ist mein neues digitales Verfahren (Software / IT-Tool) DSGVO-konform?“	3
D.	Kleiner „Datenschutzführerschein“	6
E.	Datenpanne – was tun?	7
F.	Tipps zur Informationssicherheit	8
G.	Einführung IT-Grundschutz an der Hochschule	9
H.	Ausblick eLearning Informationssicherheit	11
I.	Weitere Online-Schulungen für Sie	11

Neben einem Einblick über aktuelle Projekte des Teams Datenschutz, freuen wir uns, Sie gleich zu Beginn mit dem ergänzten Team DS an der HTWG bekannt zu machen. Erneut möchten wir Sie zu unserem **eLearning zum Datenschutz** inkl. Erwerb des kleinen „Datenschutzführerscheins“ an der HTWG für Mitarbeitende einladen.

Sie möchten ein **neues digitales Tool** nutzen? In diesem Newsletter klären wir

darüber auf, was es auf dem Weg zur datenschutzrechtlichen Nutzungsfreigabe zu beachten gilt. Wir informieren über den **richtigen Umgang mit Datenpannen** und die Einordnung, wann solche vorliegen.

Aus dem Bereich der Informationssicherheit informieren wir über eine neue **Mindestlänge für Passwörter** an der HTWG und wie die HTWG ihren **IT-Grundschutz** stärken möchte.

Wir bieten im Sommersemester wieder Online-**Schulungen** zum Thema **Datenschutz** an – nehmen Sie teil und nutzen Sie die Möglichkeit, Ihre Datenschutzexpertise zu erhöhen!

Wir wünschen Ihnen eine angenehme Lektüre und ein erfolgreiches restliches Sommersemester. Bleiben Sie gesund!

Beste Grüße, Ihre Marc Strittmatter (DSB), Hanno Langweg (ISB), Inna Feldmann, Rechtsassessorin (Referentin Datenschutz), Lena-Marie Gentsch (Referentin für technische/juristische Datenschutzaufgaben).

A. Team Datenschutz an der HWTG

Das Team DS an der HTWG konnte ergänzt werden. Neben dem DSB, Herrn Prof. Dr. Strittmatter, und Frau Ass. Jur. Inna Feldmann ist seit 1. März 2022 Frau Lena-Marie Gentsch, Wirtschaftsjuristin (LL.B.), mit an Bord. Sie wird die Hochschule als Referentin für technische/juristische Datenschutzaufgaben bei allen datenschutzrechtlichen Fragen sowie bei der Bearbeitung, Beratung und Kontrolle datenschutzrechtlicher Angelegenheiten unterstützen und die Einführung und Implementierung eines Datenschutzmanagementsystems begleiten.

Bei Fragen rund um datenschutzkonforme Arbeitsabläufe, Verfahren und Prozesse erreichen Sie Frau Gentsch unter lgentsch@htwg-konstanz.de. Wir freuen uns zudem, unsere neue wiss. Hilfskraft, Frau Khadija Morr, im Team begrüßen zu dürfen. Frau Morr ist unter Khadija.Morr@htwg-konstanz.de zu erreichen.

B. News / Aktuelles

„Fakultäten-VVT“

Wir arbeiten aktuell daran, ein „Fakultäten-VVT“ (VVT – Verzeichnis von Verarbeitungstätigkeiten) zu erstellen, nachdem das zentrale VVT nun auf dem aktuellen Stand ist. Das Fakultäten-VVT wird alle Geschäftsprozesse an den Fakultäten, die einen eigenen Zweck erfüllen, umfassen, wenn darin personenbezogene oder -beziehbare Daten verarbeitet werden. Das Verzeichnis ist eine wichtige Grundlage zur Dokumentation des Datenschutzes an der HTWG und dient damit auch den Prozessverantwortlichen beim Nachweis der Datenschutzkonformität.

Hierfür werden wir in den kommenden Wochen und Monaten mit detaillierteren Informationen und Interviewanfragen auf die Fakultäten und Studiengänge zukommen, um gemeinsam relevante Verarbeitungstätigkeiten in Ihrem Verantwortungsbereich zu erfassen.

C. Neue digitale Verfahren: „Ist mein neues digitales Verfahren (Software / IT-Tool) DSGVO-konform?“

In den letzten Jahren kam es deutschlandweit in der Hochschullandschaft zu einem Digitalisierungsschub. Verstärkt wurde dieser Trend durch die Corona-Pandemie, die die Zulassung neuer Verfahren in der Lehre (bspw. für Online-Vorlesungen und Online-Prüfungen) und in der Verwaltung zur Aufrechterhaltung des Hochschulbetriebs erforderlich machte.

Wir unterstützen den Digitalisierungsprozess, indem wir die neuen Verfahren auf Datenschutz-Konformität prüfen und Sie beraten, wie Sie das neue Tool / die neue Software möglichst datensparsam und somit DSGVO-konform einsetzen können. Darüber hinaus unterstützen wir Sie bei der Erfüllung der Informationspflichten nach Art. 13 ff. DSGVO und ggf. durch Erfassung neuer Verfahren im VVT.

Um Verstöße gegen geltendes Recht zu vermeiden, ist es besonders wichtig, dass alle digitalen Verfahren, bei denen personenbezogene Daten verarbeitet werden und die an der Hochschule Anwendung finden, DSGVO-konform sind. Vor der Nutzung solcher Verfahren sollte deshalb stets eine Prüfung des jeweiligen Tools /

der jeweiligen Software durch die für den Datenschutz verantwortliche Stelle (das Team DS) stattfinden.

Da wir sehr viele Anfragen zur Datenschutz-Freigabe von neuen Verfahren haben, empfehlen wir Ihnen, wie folgt vorzugehen:

- **Bitte beziehen Sie das Team DS frühzeitig in Ihr Vorhaben ein; die Prüfung nimmt Zeit in Anspruch und kann nicht innerhalb weniger Tage gewährleistet werden. Darüber hinaus könnte Ihr Vorhaben offensichtlich gegen DS-Vorschriften für Hochschulen verstoßen, worauf wir Sie frühzeitig hinweisen könnten und dadurch Arbeitszeit und Mühe erspart bleiben.**

Nach dem ersten Kontakt werden wir Sie in der Regel um folgende Schritte / Informationen bitten:

- Bitte stellen Sie sicher, dass Sie die notwendigen Ressourcen / Freigaben vom Präsidium und / oder Ihrer Fakultät für die neue Software / das neue Tool haben.
- Bitte prüfen Sie, ob eine Datenverarbeitung personenbezogener Daten außerhalb des EWR-Raums stattfindet. (**Achtung!** Auch eine Datenverarbeitung in **US-Clouds** ist aus DS-Sicht problematisch). Sollte dies der Fall sein, prüfen Sie bitte eigenständig, ob es ein gleichwertiges Tool gibt, bei dem die Datenverarbeitung im EWR-Raum stattfindet. Nur wenn es kein gleichwertiges deutsches oder europäisches Tool gibt, könnte ein Tool, bei dem die Daten in ein Drittland übertragen werden, zugelassen werden, sofern dieses Tool für eine Aufgabenerfüllung der HTWG erforderlich ist.
- Bitte tragen Sie zusammen, welche personenbezogenen Daten bei dem neuen Verfahren verarbeitet werden (Achtung, bei IP-Adressen handelt es sich nach aktueller Rechtsprechung um personenbezogene Daten!). Sollte Ihnen nicht klar sein, welche Daten verarbeitet werden, bitten Sie einen IT-Mitarbeitenden der HTWG (aus Ihrer Fakultät, dem IuK oder dem RZ), der für den Betrieb des Verfahrens zuständig sein wird, um Unterstützung.
- Bitte tragen Sie alle für Sie verfügbaren Unterlagen (wie Datenschutzhinweise und Vertragsunterlagen des Anbieters) zu dem neuen Verfahren zusammen.

- Findet eine externe Auftragsdatenverarbeitung statt? Dann benötigen wir den „**Auftragsverarbeitungsvertrag**“ (**AVV**) mit dem Auftragsverarbeiter sowie die „Technischen und organisatorischen Maßnahmen“ (TOMs) des Auftragsverarbeiters für die Prüfung der DSGVO-Konformität. (**Tipp:** Die TOMs sind meistens dem AVV angehängt).
- Bitte lassen Sie die TOMs von einem IT-Mitarbeitenden der HTWG, der für den Betrieb des Verfahrens zuständig sein wird, beurteilen (**Tipp:** Stellen Sie konkret die folgende Frage: *Sind die beschriebenen Maßnahmen angemessen und ausreichend?*).

Sofern das neue IT-Tool DSGVO-konform ist, sind die Nutzer in einem Datenschutzhinweis über die Verarbeitung ihrer personenbezogenen Daten zu informieren (Art. 13 ff. DSGVO). Wir unterstützen Sie bei der Erarbeitung eines Datenschutzhinweises für das neue Verfahren. Erst wenn die Datenschutzhinweise vorliegen, kann das neue Tool zur Nutzung freigegeben werden. Abschließend muss das neue Tool in das Verzeichnis der Verarbeitungstätigkeiten (VVT) aufgenommen werden.

Kurz-Übersicht:

Von der Wahl eines neuen Tools bis zur DS-Freigabe zur Nutzung



Noch ein Tipp: Sie haben wahrscheinlich selbst ein Gefühl dafür, ob ein Tool intensiv personenbezogene Daten verarbeitet und wie sensibel diese Daten sind. Überlegen Sie einfach, wie Sie das beurteilen würden, wenn es Ihre Daten wären. Bitte überlegen Sie auch, wie wichtig das Tool für die Aufgabenerledigung der Hochschule ist. Sie finden wahrscheinlich auch im Netz schon Hinweise zur DS-Konformität. Sie helfen uns,

wenn Sie mit Ihrem eigenen Judiz schon erste Überlegungen anstellen und auch ein Stück weit priorisieren.

D. Kleiner „Datenschutzführerschein“

Fragen Sie sich manchmal, inwiefern Sie der Datenschutz betrifft und welche Pflichten Sie als HTWG-Mitarbeitende/r überhaupt beachten müssen, um sich datenschutzrechtlich konform zu verhalten? Wissen Sie, was die wichtigsten Schritte im Umgang mit personenbezogenen Daten sind?

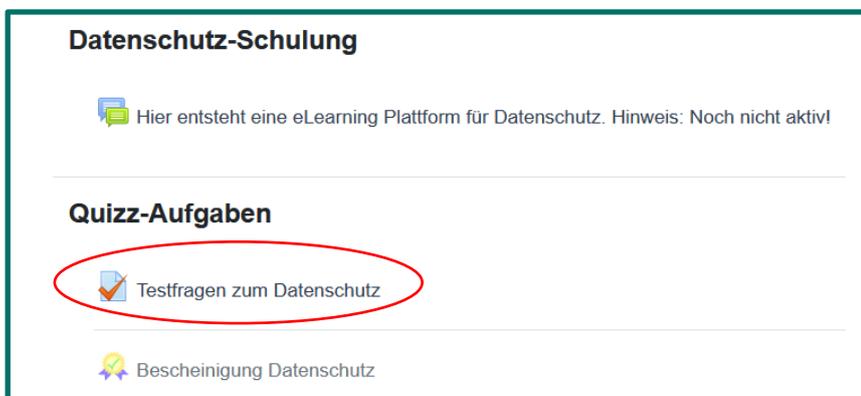
In unserem kompakten eLearning zeigen wir Ihnen, welche Datenschutzgrundsätze Sie kennen müssen und wir helfen Ihnen, Ihr Datenschutz-Knowhow digital zu stärken!

Machen Sie sich in **wenigen Klicks fit in den Grundzügen des Datenschutzrechts** mit unserem webbasierten eLearning zum Datenschutz für Mitarbeitende an der HTWG und 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 und helfen Sie mit, den Datenschutz an der HTWG zu leben und zu unterstützen.

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

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



The screenshot shows a Moodle course page titled "Datenschutz-Schulung". At the top, there is a message icon and the text "Hier entsteht eine eLearning Plattform für Datenschutz. Hinweis: Noch nicht aktiv!". Below this, under the heading "Quizz-Aufgaben", there is a list of activities. The first activity, "Testfragen zum Datenschutz", is circled in red. Below it is another activity, "Bescheinigung Datenschutz".

E. Datenpanne – was tun?

Haben Sie E-Mails mit dubiosen Anhängen aus Versehen geöffnet oder sind einem Cyberangriff zum Opfer gefallen?

Vielleicht haben Sie auch mitbekommen, dass persönliche Daten von Studierenden, wie z.B. Abschlussnoten, Adressen oder Geburtstage, (versehentlich) im Internet oder als Aushang veröffentlicht worden sind oder dass es zu einer Verwechslung im Rahmen der Mitteilung von Prüfungsleistungen gekommen ist?

Eine **Datenpanne** passiert schneller als gedacht und ist (meistens) nicht sehr gravierend. Es ist jedoch wichtig, rasch und richtig zu reagieren.

Eine Datenpanne ist eine Verletzung des Datenschutzrechts dadurch, dass sensible, vertrauliche oder anderweitig geschützte Daten verloren gegangen, gestohlen oder z.B. von unberechtigten / unautorisierten Personen eingesehen oder genutzt worden sind. Es kann zu einem Schaden für die Person(en) kommen, deren Daten betroffen sind (bspw. zu Rufschädigung oder zum Verlust der Kontrolle über die eigenen Daten), weshalb die DSGVO erheblich verschärfte Meldepflichten für derartige Vorfälle vorsieht.

Beispiele für Datenpannen finden Sie auf der Webseite der HTWG www.htwg-konstanz.de/datenschutz unter „Datenpanne melden“.

Liegt eine Datenschutzverletzung vor, **muss die HTWG** – als die für die Datenverarbeitung verantwortliche Stelle – **zeitnah handeln**, um die Nachteile für den/die Betroffene(n) so gering wie möglich zu halten.

Vermuten Sie, dass es – möglicherweise – in Ihrem Verantwortungsbereich zu einer Datenpanne gekommen ist, muss das unter www.htwg-konstanz.de/datenschutz unter „Datenpanne melden“ zur Verfügung gestellte **Formular umgehend ausgefüllt und abgeschickt** werden.

Das Formular wird sowohl an den Datenschutzbeauftragten als auch an den Informationssicherheitsbeauftragten versandt, die den Vorfall intern prüfen und **unverzüglich reagieren** müssen. Ggf. muss der Vorfall auch an die Datenschutzaufsichtsbehörde BW abgegeben werden (der Name des oder der Meldenden wird nicht übermittelt).

Eine ordentliche Meldung des Vorfalls ist wichtig, insbesondere, um die betroffenen Personen **richtig aufklären zu können, Gegenmaßnahmen zu ergreifen** und damit die HTWG ihrer **gesetzlichen Meldepflicht** an die Aufsichtsbehörde **innerhalb von 72 Stunden** nachkommen kann.

Seit April 2021 haben wir an der HTWG 6 Datenpannen gemeldet. Wir konnten dank schneller Reaktionen der Kolleginnen und Kollegen ein jeweils geringes Risiko für die betroffenen Personen verzeichnen und drohende Nachteile abwenden. Datenpannen passieren also; es geht nicht darum, Fehler zu benennen oder zu sanktionieren, sondern ausschließlich darum, Geschehenes rechtskonform zu managen und Risiken zu begrenzen.

Helfen Sie mit, dass die Persönlichkeitsrechte aller Hochschulangehörigen an der HTWG geschützt und Datenpannen durch eine verbesserte Sensibilität in Zukunft vermieden werden können!

F. Tipps zur Informationssicherheit

Sie werden es bemerkt haben: Seit dem Wintersemester 2021/2022 müssen **Passwörter an der HTWG mindestens 14 Zeichen lang** sein. Hintergrund der Anforderung ist, sogenannte Brute-Force-Angriffe auf Benutzerkonten zu erschweren. Bei einem Brute-Force-Angriff werden systematisch alle möglichen Passwörter ausprobiert. Je länger ein Passwort ist, desto mehr Möglichkeiten gibt es und desto länger dauert ein Brute-Force-Angriff. Das Passwort muss nicht kompliziert sein, aber es muss lang sein. Sie dürfen natürlich auch ein Passwort verwenden, das länger als 14 Zeichen ist (bloß mehr als 64 Zeichen sind nicht möglich, weil nicht gewährleistet ist, dass alle Dienste an der HTWG mit mehr als 64 Zeichen langen Passwörtern zurechtkommen).

Die Mindestlänge von 14 Zeichen wird bei allen Passwortänderungen umgesetzt. Schon bestehende kürzere Passwörter werden nach und nach auf die aktuelle Mindestlänge umgestellt. Das können Sie bereits jetzt freiwillig tun: HTWG-Homepage ⇒ Hochschule ⇒ Einrichtungen ⇒ Rechenzentrum ⇒ Dienste ⇒ Benutzerverwaltung bzw. direkt unter:

<https://www.htwg-konstanz.de/rz/dienste/benutzerverwaltung/>

In der Benutzerverwaltung wird nur die Mindestlänge von 14 Zeichen geprüft. Es gibt keine allgemeine Anforderung, ein Passwort regelmäßig zu ändern. Wenn Sie prüfen möchten, ob Ihr Passwort den aktuellen Anforderungen entspricht, geben Sie in der Benutzerverwaltung einfach ihr altes und neues Passwort identisch an.

Ab dem Spätsommer behalten wir uns vor, neue Passwörter auszugeben für Accounts, deren (historisch bedingt kurzes) Passwort bis dahin noch nie geändert wurde.

Ausblick: Wir untersuchen die Machbarkeit einer Zwei-Faktor-Authentisierung für Dienste der Hochschule, also z.B. die Nutzung eines Smartphones zusätzlich zum Passwort.

G. Einführung IT-Grundschutz an der Hochschule

Als Einrichtung des Landes ist die HTWG verpflichtet, den sogenannten IT-Grundschutz auf Basis der vom Bundesamt für Sicherheit in der Informationstechnik veröffentlichten Maßnahmenkataloge einzuführen. Dieser Prozess wird mehrere Jahre dauern und für alle Beschäftigten auch Veränderungen bei der Arbeit mit den IT-Systemen der Hochschule bedeuten. Die Anforderungen sind abhängig vom Schutzbedarf der IT-Systeme: Basis, Standard, erhöhter Schutzbedarf. In der ersten Phase der Einführung des IT-Grundschutz streben wir für alle IT-Systeme die Basis-Absicherung an. Später werden nach einer Risikobewertung für einzelne IT-Systeme höhere Anforderungen gestellt werden.

Für normale Büroarbeitsplätze wird üblicherweise die Basis-Absicherung gelten. Das heißt u.a. konkret:

- Verwenden Sie ein ausreichend langes Passwort von mindestens 14 Zeichen.
- Wenn Sie Ihren Arbeitsplatz oder PC-Pool verlassen, **sperrn Sie Ihren PC**, damit in Ihrer Abwesenheit niemand unter Ihrem Benutzerkonto unbefugt auf Daten zugreifen, seltsame Webseiten aufrufen oder Programme ausführen kann. Im Schadensfall entstünde der Eindruck, die Aktionen in Ihrer Abwesenheit wären durch Sie erfolgt. Das Sperren geht unter Windows ganz einfach: Sie drücken Strg+Alt+Entf gleichzeitig und wählen dann "Sperren". Zum Entsperren geben Sie ganz normal Ihr Passwort ein. Ausblick: Wir arbeiten daran, an der Hochschule auch alternative Techniken wie "Windows Hello" bereitzustellen, damit Sie zum Entsperren Ihr Passwort

seltener eingeben müssen. Stattdessen gibt es dann eine gerätebezogene PIN, Gesichtserkennung oder Fingerabdruckerkennung. Hier befinden wir uns noch in der Testphase; es findet aktuell keine allgemeine Bereitstellung statt.

- Falls Sie Ihren PC selbst verwalten, sorgen Sie für das Einspielen von Software-**Updates**, damit die von Ihnen genutzte Software stets aktuell und frei von bekannten Fehlern und Sicherheitslücken ist. Viele IT-Sicherheitsvorfälle sind vermeidbar, weil sie auf der Ausnutzung von Softwareschwachstellen basieren, für die bereits eine Fehlerbehebung bekannt ist, die aber zu spät angewendet wird. Am einfachsten funktionieren Software-Updates, wenn sie auf "automatisch" eingestellt sind.
- **Vermeiden Sie eine Speicherung dienstlicher Daten bei externen Cloud-Diensten.** Bequemlichkeit ist verlockend und manches ist ja auch bunter und praktischer gelöst – dennoch ist die Speicherung dienstlicher Daten außerhalb der Hochschule in vielen Fällen illegal und verstößt gegen die Informationssicherheitsrichtlinie der Hochschule oder gegen geltendes Datenschutzrecht. Dropbox, iCloud, GMail usw. sind für die Speicherung dienstlicher Daten nicht geeignet.
 - Auf dem Z:-Laufwerk können Sie 3 GB an Daten ablegen. Brauchen Sie mehr Platz, sprechen Sie mit dem Rechenzentrum. Brauchen Sie viel mehr Platz, sprechen Sie mit der EDV-Betreuung Ihrer Einrichtung bzw. Fakultät.
<https://www.htwg-konstanz.de/rz/dienste/zentrale-homedirectories/>
 - Das neue bwSyncAndShare ist besser als früher. Hier haben Sie ganz legal 50 GB Speicherplatz, dürfen personenbezogene Daten speichern, können Daten mit Ihrem PC synchronisieren (auch praktisch für unterwegs), können Zugriff für Beschäftigte, Studierende und Externe bequem per passwortgeschütztem Link freigeben und haben Zugang zu älteren Dateiversionen und einen Papierkorb für Notfälle:
<https://www.htwg-konstanz.de/rz/dienste/bwsync-share-neue-version/>
 - Für dienstliche E-Mails steht ein dienstliches E-Mail-Konto zur Verfügung. Die Nutzung einer privaten E-Mail-Adresse für dienstliche Zwecke oder die (ggf. automatische) Weiterleitung dienstlicher E-Mails an private E-Mail-Konten ist regelmäßig nicht zulässig.

Brauchen Sie mehr Platz für Ihre E-Mails, sprechen Sie mit dem Rechenzentrum, welche Lösungen es gibt.

- **Vermeiden Sie eine ausschließlich lokale Speicherung von Daten.** Datenverlust ist vermeidbar, wenn Sie Daten auf zentral gewarteten Servern oder Web-Anwendungen 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.

H. Ausblick eLearning Informationssicherheit

In Vorbereitung für den Herbst ist ein Angebot mit eLearning-Modulen. In kurzen Videos und Quizzes werden Sie umsetzbare Tipps für Ihren Arbeitsalltag erhalten. Thematisch geht es um Grundlagen der Informationssicherheit, Phishing, Social Engineering, Umgang mit USB-Speichermedien. Das eLearning-Portal ist Teil einer landesweiten Aktion.

I. Weitere Online-Schulungen für Sie

Um Ihr Grundlagenwissen aufzufrischen und Sie auf den neusten Stand zu bringen oder um Ihnen den Einstieg ins Datenschutz-Knowhow zu erleichtern, bieten wir auch dieses Sommersemester ergänzend zum eLearning wieder ein **Schulungsprogramm** an.

Unsere Datenschutz-Expertin Frau jur. Ass. Inna Feldmann wird Ihnen das Need-to-Know zum sicheren Umgang mit personenbezogenen Daten an der HTWG näherbringen und/ oder auffrischen und steht Ihnen gerne (auch außerhalb der Schulung) für Fragen zur Verfügung.

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

- **Donnerstag, 07. Juli 2022, 10.00 Uhr bis 11.30 Uhr**

Meeting-Link: <https://htwg-konstanz.webex.com/htwg-konstanz/j.php?MTID=m9643a06b1e99b7d583913b3eb5708401>

Meeting-Kennnummer (Zugriffscod): 2731 123 9019

Meeting Passwort: HhVpuVcM972

Über Telefon beitreten: +49-619-6781-9736 Germany Toll

- **Dienstag, 12. Juli 2021, 10.00 Uhr bis 11.30 Uhr**

Meeting-Link: <https://htwg-konstanz.webex.com/htwg-konstanz/j.php?MTID=m62e7b323fe5c99bcd7acc4ee3798167c>

Meeting-Kennnummer (Zugriffscod): 2732 296 2345

Meeting Passwort: ZKkMwV9Pf34

Über Telefon beitreten: +49-619-6781-9736 Germany Toll

Wir freuen uns auf Ihre rege Teilnahme!

Beste Grüße und bis zum nächsten Newsletter.

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