Achtung: Die Technische Universität Ilmenau nutzt das Datenschutzmanagementsystem Audatis und erstellt damit VVT strukturiert in einer Datenbank. Das Beispiel dient in dieser Form also nur noch dem Verständnis, was inhaltlich zu einem VVT gehört. Die tatsächliche Dokumentation erfolgt **NICHT** mehr auf Basis des Word-Formulars.

Das **VVT-Beispiel** ist ein Muster zur Umsetzung eines VVT mit Erläuterungen.

Das Muster basiert auf dem Formular für die Thüringer Hochschulen und kann hier als Word-Datei heruntergeladen werden.

Im Beispiel wird von folgendem Sachverhalt ausgegangen:

Ein Fachgebiet an der TU Ilmenau betreibt mittels des Dienstes „mailman“ einen Newsletter, um ehemalige MitarbeiterInnen und Studierende über aktuelle Entwicklungen auf dem Laufenden zu halten. Die Mehrzahl der Emails geht an externe Emailadressen.

Formularfeld	**Fußnoten**(nur inhaltliche; keine technischen Erläuterungen)	**Erläuterung**	**Beispiel**
1 Verantwortlicher und Datenschutzbeauftragter gem Art. 30 Abs. 1 Satz 2, lit. a) EU-DSGVO			
1.1 Name und Kontaktdaten des Verantwortlichen	(Gem. Art. 4 Nr. 7 DSGVO)	Als Verantwortlicher wird immer im öffentlichen Bereich immer der Rechtsträger, also in aller Regel die Körperschaft öffentlichen Rechts benannt. Als deren Vertreter wird der gesetzliche Vertreter gem. ThuerHG	Technische Universität Ilmenau Der Rektor Ehrenbergstraße 29 98693 Ilmenau
1.2 Innerorganisatorisch für das Verfahren Verantwortlicher (optional)	Eine schriftliche Delegation der Zeichnung des Verzeichnisses ist möglich.	An etwas größeren Institutionen sollte immer ein innerorganisatorisch Verantwortlicher benannt werden. Es kann auch zweckmäßig sein, mehrere Ansprechpartner zu benennen.	Fakultät Wirtschaft und Medien/Fachgebiet öffentliches Recht
1.3 Name und Kontaktdaten eines oder mehrerer gemeinsam Verantwortlicher	Gem. Art. 26 DSGVO; Auflistung dieser Daten in einer Anlage ist möglich.	Gemeinsam sind gemeinsam Verantwortliche (Joint Controlling) gemäß Artikel 26 DSGVO	(-)
1.4 Name und Kontaktdaten des Datenschutzbeauftragten (und ggf. seines Stellvertreters)		Anders als bei Datenschutzerklärungen, sollte hier eine konkrete Benennung erfolgen.	Martin Neldner, datenschutz@tu-ilmenau.de, Tel. -2524
1.5 Bei Auftragsverarbeitung : Name und Kontaktdaten des Auftragsverarbeiters	Gem. Art. 28 DSGVO		(-)
2 Zwecke und Grundlagen der Verarbeitung sowie Löschfristen gem. Art. 30 Abs. 1 Satz 2, lit. b) und lit. f) EU-DSGVO			

Formularfeld	**Fußnoten**(nur inhaltliche; keine technischen Erläuterungen)	**Erläuterung**	**Beispiel**
2.1 Bezeichnung der Verarbeitungstätigkeit und Kurzbezeichnung (8 Zeichen)	Allgemein verständliche Bezeichnung des Verfahrens (z. B. Immatrikulation, Stellenbewerbung, Einstellung, Personalkostenplanung, Stellplatzverwaltung, Notenverbuchung). Der datenschutzrechtliche Begriff der Verarbeitungstätigkeit ist an logischen Kriterien, wie Funktionalität, Zweckbindung, Verarbeitungslogik, Wirkung von Verknüpfungs- und Zugriffsregeln, orientiert. Die bloße Dokumentation der physischen Datenorganisation (z. B. Datenbankstruktur oder Dateibeschreibung) leistet für das Herbeiführen datenschutzrechtlicher Transparenz keinen geeigneten Beitrag.	Eine prägnante Bezeichnung ist hilfreich, damit das Verfahren wiedererkannt und beachtet werden kann. Eine Kurzbezeichnung ist optional - es ist offen, ob eine Datenbanklösung eingeführt wird, die eine Kurzbezeichnung mit fix 8 Zeichen verwendet. Mit der Bezeichnung und dem folgenden Punkt Zwecke wird auch die Entscheidung getroffen, wie weit oder eng ein Verfahren definiert wird. Dafür gibt keine zwingenden Vorgaben.	Newsletter Fachgebiet öffentliches Recht
2.2 Zwecke, zu deren Erfüllung die Daten verarbeitet werden		Vom Zweck der Verarbeitung hängt regelmäßig die Rechtsgrundlage ab. Bei Abwägungsentscheidungen ist der Zweck zudem das maßgebliche Argument FÜR die Datenverarbeitung. Je wichtiger der Zeck, desto eher wird in solchen Fällen die Verarbeitung zulässig sein.	Information über die Arbeit des Fachgebiets und aktuelle Entwicklungen im Medien- und Datenschutzrecht
2.3 Rechtsgrundlagen der Datenverarbeitung	Gem. Art. 6 Abs. 1 lit. c) und lit e) DSGVO.	**Zentraler Punkt** eines jeden VVT. Hier ist -ggf. gemeinsam mit dem Datenschutzbeauftragten- zu prüfen, auf welche Rechtsgrundlage die Verarbeitung gestützt wird und damit die Rechtmäßigkeit der Verarbeitung sichergestellt wird. Anders als die Fußnote andeutet sollte die Rechtsgrundlage umfassend angegeben werden. Also ggf. angefangen bei etwaigen Satzungen (z.B. Prüfungsordnung) über Verordnungen (Hochschuldatenschutzverordnung), Spezialgesetze ThürHG und allgemeine Datenschutzgesetze (ThürDSG, BDSG) bis hin zur DSGVO. Besondere Kategorien personenbezogener Daten gem. Art. 9 DSGVO bedürfen einer vertieften Prüfung.	Der Newsletter wird nur an Personen versandt, die hierzu ihre Einwilligung erteilt haben, Art. 6 Abs. 1 UA 1 lit. a.

Formularfeld	**Fußnoten**(nur inhaltliche; keine technischen Erläuterungen)	**Erläuterung**	**Beispiel**
2.4 Darlegung berechtigter Interessen nach Art. 6 Abs. 1 DSGVO: a) Einwilligung (Hinweis auf jederzeitiges Widerrufsrecht) b) vertragliches oder vorvertragliches Erfordernis c) Erfüllung rechtlicher Verpflichtung e) Erfordernis Aufgabenwahrnehmung (öffentliches Interesse / öffentliche Gewalt)	zu a) Gem. Art. 13 Abs. 2 lit. c) und Art. 14 Abs. 2 lit. d) DSGVO.	Ein missverständliches Feld, dass vorläufig nicht belegt wird: Eine Verarbeitung zur Wahrung berechtigter Interessen ist öffentlichen Stellen in der Regel nicht gestattet. Zudem **muss** unter 2.3 die Rechtsgrundlage einschließlich der passenden Regelung in der DSGVO angegeben werden.	(-)
2.5 Beginn der Verarbeitungstätigkeit / Verfahren eingesetzt ab/seit:			01.01.2019
3 Kategorien betroffener Personen und personenbezogener Daten gem. Art. 30 Abs. 1 Satz 2 lit. c) EU-DSGVO			
3.1 Bezeichnung der Kategorien betroffener Personen	Zum Beispiel: Studierende, Studienbewerber, ProfessorInnen, Mitarbeiter, Stellenbewerber, Alumni, externe Lehrbeauftragte	Betroffene Person ist die natürliche, lebende Person, deren personenbezogene Daten verarbeitet werden.	aktive und ehemalige Mitarbeiter, aktive und ehemalige Studierende, Gastwissenschaftler, sonstige am Fachgebiet interessierte Personen
3.2 Bezeichnung/Beschreibung der personenbezogenen Daten nach Kategorien	Gem. Art. 30 Abs. 1 Satz 2 lit. c DSGVO; besondere Kategorien personenbezogener Daten gem. Art. 9 DSGVO bitte als solche kennzeichnen	Zumindest soweit besondere Kategorien personenbezogener Daten vorhanden sind, muss die Rechtsgrundlage (2.3) in besonderem Maße auf ihre Tauglichkeit geprüft werden.	Email, Name, ggf. Grund der Aufnahme in den Newsletter
4 Bezeichnung der Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt wurden oder noch werden gem. Art. 30 Abs. 1 Satz 2 lit. d) EU-DSGVO			
4.1 Empfänger im Anwendungsbereich der DSGVO (schließt auch Auftragsverarbeiter ein)	~~Art 18 DSGVO~~	Empfänger (näheres siehe Artikel) ist in Art. 4 Nr. 9 DSGVO legal definiert. Der Hinweis in der Fußnote ist falsch: Gemeint ist Art. 28 DSGVO, der die Auftragsverarbeitung regelt.	Eine Weiterleitung personenbezogener Informationen findet nicht statt.

Formularfeld	**Fußnoten**(nur inhaltliche; keine technischen Erläuterungen)	**Erläuterung**	**Beispiel**
4.1.1 Empfänger innerhalb des Bereichs des Verantwortlichen (der Organisation/Behörde)		Eine Angabe, die in der DSGVO nicht vorgesehen ist. Empfänger meint eigentlich Stellen außerhalb des Verantwortlichen. Dennoch kann eine Angabe zweckmäßig sein: - Verfahren lassen sich verknüpfen, indem hier angegeben wird, an welches (andere) Verfahren personenbezogene Daten „übermittelt“ werden. Dazu sollten mindestens die Bezeichnung des anderen Verfahrens (Feld 2.1) und der innerorganisatorisch Verantwortliche (Feld 1.2) angegeben werden. - Wenn unsicher ist, ob eine Übermittlung tatsächlich innerhalb desselben Verantwortlichen erfolgt, sollte diese Übermittlung dokumentiert werden - Hier wenn es wahrscheinlich ein Verantwortlicher ist, ansonsten im folgenden Feld.	(-)
4.1.2 Empfänger außerhalb des Bereichs des Verantwortlichen (der Organisation/Behörde)			(-)
4.2 Empfänger im Drittland nach Kapitel V DSGVO		Übermittlung personenbezogener Daten in Drittländer ist an außerordentlich hohe Voraussetzungen geknüpft. Eine solche Übermittlung sollte nur nach Rücksprache mit dem Datenschutzbeauftragten erfolgen. Im Regelfall bleibt das Formularfeld frei.	(-)
4.3 Empfänger in internationaler Organisation		Siehe 4.2	(-)
5 Angaben zur Übermittlung von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation gem. Art. 30 Abs. 1 Satz 2 lit. e) EU-DSGVO		Siehe 4.2. Eine solche Übermittlung findet regelmäßig nicht statt. Daher bleiben die Felder im Abschnitt 5 regelmäßig frei. Sie werden daher in diesem Muster auch nicht abgedruckt.	Eine Weiterleitung personenbezogener Informationen findet nicht statt.
6 Löschfristen der verschiedenen Datenkategorien gem. Art. 30 Abs. 1 Satz 2 lit. f) EU-DSGVO		Auch das ist eine zentraler Punkt. In den meisten Fällen muss sichergestellt werden, dass die personenbezogenen Daten zu einem bestimmten oder bestimmbaren Zeitpunkt gelöscht werden.(Bloßes Sperren wird idR nicht genügen.)	
6.1 Vorgesehene Fristen für die Löschung, bezogen auf die Datenkategorie	Bezeichnungen wie in 3.2	Die Frist für die Löschung ergibt sich in der Regel aus der Aufbewahrungsfrist. An der TU Ilmenau steht eine Datenbank für die Aufbewahrungsfristen(TU) zur Verfügung.	Keine planmäßigen Löschfristen, auf Wunsch der betroffenen Person unverzügliche Löschung

Formularfeld	**Fußnoten**(nur inhaltliche; keine technischen Erläuterungen)	**Erläuterung**	**Beispiel**
6.2 Rechtsgrundlage der Löschfrist		Wenn möglich, sollten Rechtsnormen angegeben werden, aus denen sich die Löschfrist bzw. Aufbewahrungsfrist ergibt.(Siehe auch oben 2.3. zu möglichen Rechtsnormen)	(-)
7 Beschreibung der technischen und organisatorischen Maßnahmen gem. Art. 30 Abs. 1 Satz 2 lit. g) in Verbindung mit Art. 32 Abs. 1 EU-DSGVO	Hier ist die konkrete Rechtsgrundlage, die eine Löschung erfordert bzw. die Aufbewahrungsrist bestimmt, anzugeben (Hinweise können auch Verwaltungsvorschriften oder Satzungen geben)		
7.1 Datum der letzten Risikobewertung			15.12.2018
7.2 Ergebnis mit kurzer Begründung (Ausrichtung und zugrunde gelegte Beurteilungstechnik der Risikobewertung)		Idealerweise sollte ein standardisiertes Verfahren, z.B. Schutzbedarfsfeststellung nach BSI	normaler Schutzbedarf
7.3 Beschreibung allgemeiner technischer und organisatorischer Maßnahmen wie Pseudonymisierung und Verschlüsselung	Hier ist nicht hauptsächlich auf das IT-Sicherheitskonzept abzustellen, sondern vor allem die datenbezogenen Maßnahmen sind zu beschreiben, unter Berücksichtigung des Art. 32 DSGVO.	In einfachen Fällen sollte wenn möglich auf das „Infrastruktur-VVT“ verwiesen werden.	Siehe VVT „GNU Mailman“
7.4 Beschreibung der eingesetzten Hard- und Software	Hier ist auch Verweis möglich, z.B. auf vorhandenes Inventarverzeichnis.		Übliche Client-PC, GNU_Mailman auf virtualisiertem Server des UniRZ
7.5 Beschreibung der technischen und organisatorischen Maßnahmen zur Sicherstellung insbesondere von Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit der Systeme und Dienste	Die Sicherstellung bezieht sich auf Systeme und Dienste und nicht auf die Verarbeitung oder die personenbezogenen Daten selbst. Sicherzustellen ist die Fähigkeit von Systemen und Diensten (so Piltz in: Gola, DSGVO Kommentar, Art. 32. Rz. 30).		Siehe VVT „GNU Mailman“
7.5.1 Maßnahmen zur Zutrittskontrolle			(-)
7.5.2 Maßnahmen zur Zugangskontrolle			(-)
7.5.3 Maßnahmen zur Zugriffskontrolle			(-)
7.5.4 Maßnahmen zur Weitergabekontrolle			(-)
7.5.5 Maßnahmen zur Eingabekontrolle			(-)
7.5.6 Maßnahmen zur Auftragskontrolle (nur im Falle von Auftragsverarbeitung)			(-)
7.5.7 Maßnahmen zur Verfügbarkeitskontrolle			(-)
7.5.8 Maßnahmen zur Gewährleistung des Trennungsgebots			(-)

Formularfeld	**Fußnoten**(nur inhaltliche; keine technischen Erläuterungen)	**Erläuterung**	**Beispiel**
7.6 Fähigkeit zur Wiederherstellung der personenbezogenen Daten nach physischem oder technischem Zwischenfall insbesondere im Hinblick auf Verfügbarkeit, Zugang			(-)
7.7 Verfahren zur regelmäßigen Überprüfung der technischen und organisatorischen Maßnahmen (Evaluation)	Diese Regelung dient dazu, dass die verpflichtete Stelle den Nachweis erbringt, sowohl intern als auch extern, dass die von ihr umgesetzten Maßnahmen den Anforderungen des Art. 32 DSGVO gerecht werden. Hierzu müssen interne Prozesse und Abläufe, insb. auf organisatorischer Ebene, entwickelt und umgesetzt werden (so Piltz in: Gola, DSGVO, Kommentar, Art. 32, Rz. 36).		(-)
8 Angaben zur Datenschutz-Folgenabschätzung – nur, wenn bei Nr. 7.1 / 7.2 ein hohes Risiko festgestellt wurde oder die Voraussetzungen des Art. 35 Abs. 3 EU-DSGVO vorliegen			(-)
8.1 Ergebnis der Datenschutz-Folgenabschätzung			(-)
8.2 Datum der letzten Überprüfung der Verarbeitung anhand der Datenschutz-Folgenabschätzung			(-)
8.3 Information über vorherige Konsultation gem. Art. 36 Abs. 1 DSGVO			(-)

Artikel