Hinweise zum Formular
Verzeichnis von Verarbeitungstätigkeiten (VVT)

Stand 08.01.2019

I. Allgemeines:

Das VVT soll beschreiben, worum es bei einer konkreten Datenverarbeitung geht, z.B. wer verantwortlich ist und wie im Verlauf des Verfahrens/Projekts mit den Daten umgegangen wird.

Vorab ist das Verfahren abzugrenzen.

Dabei kann man zunächst vom äußeren Bild der tatsächlichen Abläufe ausgehen. Stellt das Vorhaben **einen zusammenhängenden** Prozess dar? Abläufe, bei der die gesamte Datenverarbeitung innerhalb einer Verantwortlichkeit und dem gleichen Zweck verbleibt, können in einem VVT beschrieben werden.

Ein Beispiel wäre die Verarbeitung in einem Forschungsprojekt: Daten werden durch das Projekt erhoben, gespeichert und verarbeitet (analysiert), Ergebnisse veröffentlicht, Rohdaten gem. Wiss. Praxis aufbewahrt. Danach werden die personenbezogenen Daten gelöscht/anonymisiert (bzw. archiviert gem. ArchivO), das Projekt ist (endgültig) abgeschlossen. Hier besteht über den gesamten 'Lebensweg' der Daten (von Erhebung bis Löschung) ein einheitlicher Zweck und eine einheitliche Verantwortlichkeit.

Andere Verfahren sind **mehrstufig**, wobei insbesondere die Verantwortlichkeiten wechseln, ggf. auch Zwecke der Verarbeitung wechseln. In den Bereichen spielen sich also nur Teile des gesamten Verfahrens ab. Diese Verfahren sind mehrteilig beschreibbar, in Abschnitte je nach den zuständigen Abteilungen aufgeteilt.

Ein Beispiel wäre das Einstellungsverfahren:
Bewerbungen gehen dezentral ein, werden gespeichert, Gespräche geführt, der zuständige PR beteiligt, Entscheidungen getroffen, Zu- und Absagen versandt (Federführung: Bereich); anschließend werden die Daten des erfolgreichen Bewerbers an die PersAbtlg abgegeben. (Ende Verfahren, Verantwortlichkeitswechsel). Umgang und weitere Datenverarbeitung durch die Personalabteilung stellt dann wieder ein eigenes Verfahren dar (Personalverwaltung).

In diesen Fällen kann das Feld „kurze Beschreibung des Verfahrens(ablaufs)“ für eine zusätzliche Abgrenzung genutzt werden. (z.B. 'Verfahren dient der Seminarorganisation von Anmeldung bis einschl. Themenverwaltung', 'Durchführung und Organisation von Bewerbungsverfahren bis Übergabe an PersAbtlg', 'Übernahme (Studierenden-)Daten von Abteilung xy und Bearbeitung zur Erfüllung von Meldepflichten gegenüb. Behörde xz‘). Dieses Feld kann man auch ansonsten für eine nähere Beschreibung nutzen: ‚Bearbeitung von Moodle-Kursen‘, 'Büroorganisation: Bearbeitung allgemeiner Anfragen einschl. Kontaktaufnahme per Mail und Telefon'.

II. Zu den einzelnen Punkten des Formulars

Datum: Datum, an dem die Verarbeitung begonnen wurde.

Zu 1) Verantwortlichkeiten für das Verfahren/Projekt

Idealerweise sind die Verantwortlichkeiten bereits zugewiesen. Andernfalls muss bestimmt werden, wer für das Verfahren (bzw. den Abschnitt) den 'Hut aufhat'. Dies ist danach zu beurteilen, wer über die Gestaltung des Ablaufs zuständigerweise zu entscheiden hat.

Üblicherweise wird dies die **Leitung des jeweiligen Bereichs** (Forschungsprojektes) sein. Bestehen Unklarheiten, müssen diese beseitigt werden, da die/der Verantwortliche namentlich zu nennen ist.

Selten, z.B. **bei Kooperationen**, legen mehrere Stellen „auf gleicher Augenhöhe“ ein Verfahren fest. In diesem Fall sind beide Stellen einzutragen und in einer **Anlage** die konkrete Verteilung der Verantwortlichkeiten hinsichtlich des Gesamtprozesses darzulegen, vgl. Art. 26 DSGVO. Diese Aufteilung wird in anderen Zusammenhängen, z.B. Erfüllung der Informationspflichten nach Art. 13 DSGVO, öffentlich mitgeteilt.

Bitte geben Sie sowohl Name als auch Kontaktdaten des/der Verantwortlichen an. Diese Daten werden später auch z.B. für Pflichtinformationen gem. Art. 13 DSGVO benötigt.

Kontaktperson für Betroffenenrechte

Die Kontaktperson muss nicht Verantwortliche_r sein. Sie sollte aber in der Lage sein, die erforderlichen Informationen nach Art. 15 DSGVO innerhalb der gesetzlichen Antwortfrist (z.B. 1 Monat) zusammenzutragen. Gleiches gilt für die Umsetzung von Betroffenenrechte zur Löschung, Sperrung und Widerspruch, soweit dies zu erfolgen hat.

Zu 2a) Zwecke der Datenverarbeitung

Die Zwecke müssen eindeutig und so aussagekräftig sein, dass die Aufsichtsbehörde die Angemessenheit der Schutzmaßnahmen und die Zulässigkeit der Verarbeitung vorläufig einschätzen kann. Der Zweck der Datenverarbeitung ist möglichst präzise zu benennen. Die Benennung begrenzt allerdings auch die Anwendbarkeit der Daten auf diesen genannten Zweck.

Zwecke können sein z.B. Verwaltung der personenbezogenen Daten im Zusammenhang mit der Vergabe von Seminarräumen; *Personalaktenführung/Stammdaten, Lohn-, Gehalts- und Bezügeabrechnung, Arbeitszeiterfassung, Urlaubsdatei, Bewerbungsverfahren, Verwaltung von Studienleistungen, Videoüberwachung.*

Zu 2b) Rechtsgrundlage

Für die Datenverarbeitung muss eine Rechtsgrundlage gem. Art. 6 DSGVO gegeben sein. Die DSGVO sieht dafür verschiedene Alternativen vor:

Art. 6 Abs. 1 lit. a) DSGVO
Einwilligung (Muster Einwilligungserklärung bitte als Anlage beifügen)
Die Verarbeitung von Daten im Rahmen von Adresslisten, Newslettern oder Forschungsprojekten erfolgt häufig aufgrund einer Einwilligung der jeweilig Betroffenen.

Rechtskonforme Einwilligungen müssen gesetzlich bestimmte Mindestangaben enthalten. Hinweise zur Gestaltung siehe www.hu-berlin.de/datenschutz

Art. 6 Abs. 1 lit. b) DSGVO

(Verarbeitung ist für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen).

Hier können sämtliche Verträge angegeben werden, im Rahmen derer Daten verarbeitet werden. Dies können z.B. Kaufverträge, Miet- oder Leasingverträge, Dienst- oder Werkverträge mit Dienstleistern (Abrechnungsdaten oder Kontaktdaten wg. Gewährleistungsrechten, Kundendienst usw.) sein. Auch der Informationsaustausch bei möglicher Vertragsanbahnung wie Kontaktaufnahme oder unverbindliche Angebotseinholung passen hierher; ferner die Datenverarbeitung aufgrund von Arbeitsverträgen oder sonstigen Verträgen.

Bitte die konkreten Verträge/Vertragsarten *(z.B. Dienstleistungsverträge, Kauf-/Leasingverträge, Mietverträge usw.) nennen.*

Art. 6 Abs. 1 lit. c) DSGVO

(Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt.)

Dieser Fall ist (nur) einschlägig, wenn eine konkrete Rechtsvorschrift besteht, welche die Hochschule verpflichtet, eine bestimmte Datenverarbeitung (meist Übermittlung an andere Stellen) vorzunehmen. Diese Rechtsvorschrift muss zusätzlich genannt werden, z.B. gesetzliche Meldepflicht oder Mitteilungspflichten gem. § 27 MuSchuG, § 8 IfSG usw.

Art. 6 Abs. 1 lit. d) DSGVO

(Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen),

z.B. Eingreifen in Notfällen – diese Kategorie ist nur der Vollständigkeit halber aufgeführt und dürfte normalerweise nicht zutreffen.

Art. 6 Abs. 1 lit. e) DSGVO

(Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde). Dieser Fall ist einschlägig, wenn eine konkrete Rechtsvorschrift besteht, welche die Verarbeitung erlaubt, *z.B. Studierendenverwaltung, Prüfungsverwaltung.*

Grundsätzlich fallen hierunter potentiell alle Handlungen, in denen die Universität als Behörde, handelt, z.B. § 6 Abs. 1 Satz 1 BerlHG i.V.m der Rechtsverordnung gem. § 6b Abs. 1 BerlHG (Studierendendatenverordnung [StudDatenVO]), Informationsverarbeitungsgesetz (IVG), Satzung der Hochschule *(z.B. ZSP HU, CBO, UBOrdnung),* Videoüberwachung in öffentlich zugänglichen Bereichen gem. IVG/DV Video, §§ 56 ff. LBG (Landesbeamtengesetz), usw.

Art. 6 Abs. 1 lit. f) DSGVO

(Verarbeitung ist zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person , die den Schutz personenbezogener Daten erfordern, überwiegen). ***!*** *Diese Vorschrift gilt* ***nicht, wenn*** *die Behörde (=HU) in Erfüllung ihrer (hoheitlichen) Aufgaben Daten*

verarbeitet. Die Vorschrift ist daher nur sehr eingeschränkt für die HU anwendbar. Im Zweifel bitte bei den DSB nachfragen.)
Erforderlich ist die Nennung/Begründung des Vorliegens eines berechtigten Interesses, welches die Datenverarbeitung rechtfertigen soll.

Zu 3) Personengruppen, deren Daten verarbeitet werden (es sind Mehrfachnennungen möglich)

„Sonstige Personengruppen" sind z.B. Gäste, Teilnehmer_innen einer Veranstaltung, Besucher_innen der Bibliothek.

Zu 4) Welche Daten werden verarbeitet (Kategorien von Daten)?

Hier sind die konkreten Daten anzugeben, z.B. „Mitarbeiter-Stammdaten mit Adressdaten (Adresse, Telefon, E-Mail), Geburtsdatum, Bankverbindung, Steuermerkmale, Lohngruppe, Arbeitszeit, bisherige Tätigkeitsbereiche, Qualifikationen"; Bewerbungen mit Kontaktdaten, Qualifikationsdaten, Tätigkeiten; Videoüberwachung; Lieferanten-Kontaktdaten mit Adressdaten, Ansprechpartnern etc.; Studierenden-Stammdaten; Studierenden-Prüfungsdaten, Leistungsnachweise; Forschungsrohdaten, und Adressdaten der Probanden usw.).

Sofern mehrere Personengruppen betroffen sind, ist zuzuordnen, von wem welche Daten verarbeitet werden. (z.B.: „Prof: Name und HU-Einrichtung; Besucher: Name, Adresse, E-Mail")

Werden sog. ‚besondere Arten' personenbezogener Daten oder Datenkategorien verarbeitet?
Dies sind Daten zur rassischen und ethnischen Herkunft, politischen Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung, vgl. Art. 9 Abs. 1 DSGVO.

Soweit aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung ein hohes Risiko für Rechte und Freiheiten natürlicher Personen bestehen kann, bestehen besondere Pflichten. Dies ist insbesondere der Fall bei:

1. *systematischer und umfassender Bewertung persönlicher Aspekte natürlicher Personen,*
2. *Profiling, welches als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen können;*
3. *umfangreicher Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1*
4. *umfangreicher Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten oder systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche*

Nehmen Sie in diesen Fällen bitte Kontakt zu dem/der DSB auf. Hier sind datenschutzrechtlich ggf. gesonderte Anforderungen zu erfüllen.

zu 5) Herkunft bzw. Quelle empfangener Daten

Woher stammen die Daten? Hier kommen z.B. infrage: Direkterhebung/Auskunft beim/bei der Betroffenen, Melderegisterauskunft, Studienabteilung der HU, Personalabteilung, CMS, Partnerhochschule.

Zu 6) Wer hat Zugriff auf die Daten?

Eine Aufteilung nach Personengruppen bzw. Stellenzeichen ist ausreichend, möglichst mit Umfang der Berechtigungen, z.B.:
Leiter Einrichtung, volle Schreibrechte; Mitarbeiter nach Abteilung/Aufgabengebiet, beschränkte Schreibrechte; IT-Admin, volle Schreibrechte; oder: Leiter und wiss. Mitarbeiter des Projektes, Schreibberechtigung alle Daten; SHK, Schreibberechtigung außer Rohdaten)

Zu 7) Empfänger, gegenüber denen die personenbezogenen Daten offengelegt werden

Hier sind alle *Stellen anzugeben, an die Daten übermittelt werden oder die auf sonstige Weise Zugriff/Kenntnis von den Daten erhalten) Als Angaben reichen hier aus:*

a) intern: HU-Stelle / Funktion: *(z.B. Studienabteilung, Personalabteilung, Fakultäten, angegliederte Institute, Personalrat; keine)*

b) extern Empfängerkategorie: *(z.B. HU Innovation, HUG, Sozialversicherungsträger, Finanzämter, Landes/Bundes-Statistikamt, Gläubiger bei Lohn-/Gehaltspfändungen, ggf. Auftragsverarbeiter, Partneruniversitäten, Drittmittelgeber, keine)*

zu 8) Fristen für die Löschung der Daten

Grundsatz: Daten sind zu löschen, wenn die Aufbewahrungsfrist abgelaufen ist.

Infrage kommen gesetzliche Aufbewahrungsfristen, z.B. Buchhaltungsunterlagen 10 Jahre gem. 59 LHO; Bewerbungsdaten Studierende: nach Ablehnungsbescheid höchstens 4 Jahre gem. §4 StuddatenVO, Stammdaten Studierende nach Exmatrikulation, 50 Jahre, gem. §4 Abs. 2 StuddatenVO; Bewerbungen: 6 Monate nach Stellenvergabe (interne Regel); Aufbewahrungsfrist für Inventare, Jahresabschlüsse gem. § 147 AO: 10 Jahre; Handelsbriefe: 6 Jahre gem. § 257 HGB; Forschungsrohdaten: 10 Jahre gem. Regeln guter wiss. Praxis.

Sofern keine gesetzliche Frist: *Festlegung durch Verantwortlichen (z.B. nach Abschluss des Projektes inkl. Abrechnung: 6 Monate; Einstellung des Newsletters; Ende der Veranstaltung (inkl. Nachbetreuung)) Hierbei können auch z.B. Gewährleistungsfristen, Fristen für Anspruchsstellung, Widerspruchsfristen eine Rolle spielen.*

Zu 9) Auftragsverarbeitung

Liegt eine Auftragsverarbeitung vor?
So lange die Daten hier in der Universität verarbeitet werden, ist keine Auftragsverarbeitung gegeben (Normalfall).
Anders ist es, wenn personenbezogene Daten unter Mithilfe eines externen Dienstleisters/Stelle verarbeitet werden (Z.B. Analyse von Daten in einem externen Büro, Datenverarbeitungen in einem externen Rechenzentrum (nicht CMS), Nutzung von Daten-Clouds oder Cloud-Programmen, externe Gehaltsabrechnungen. Keine Auftragsverarbeitung

ist gegeben, wenn die Datenverarbeitung nur ganz gering bzw. nachrangig personenbezogene Daten betrifft (z.B. Druck eines Prospekts, in dem auch eine Kontaktadresse enthalten ist).
Ist von einer Auftragsverarbeitung auszugehen, raten wir Kontakt zu dem/der DSB aufzunehmen.

Zu 10) Werden Daten übermittelt an ein Drittland (= Stelle in einem Nicht-EU-Staat) oder eine internationale Organisation

Erfolgt eine solche Übermittlung, raten wir Kontakt zu dem/der DSB aufnehmen, da eine Reihe von Vorschriften und Bedingungen zu beachten sind.

Zu 11) Technisch-organisatorische Maßnahmen (TOM) gemäß Artikel 32 Abs.1 DSGVO

a) Werden Systeme/Infrastruktur des CMS (bzw. der Fakultäten Rewi, Informatik oder WiWi) genutzt?
Falls JA: Bitte nennen Sie das/die für das Verfahren genutzte/n Systeme
(z.B: Mailsystem der Uni; Laufwerke im inneren Verwaltungsnetzwerk (UVA); HUIAM (Identitätsmanagement der HU); OTRS (Ticketsystem zur Behandlung einer großen Anzahl von Anfragen); HU-Box (Online-Speicher der HU usw.) Eine Übersicht der CMS-Dienste siehe unter: https://hu.berlin/44475
Die einzelnen technischen IT-Sicherheitsmaßnahmen werden von o.g. Bereichen dokumentiert. Ausnahme: Es werden noch eigene Maßnahmen betrieben bzw. sind aus besonderen Gründen erforderlich, z.B. bei Nutzung von USB-Sticks (-> Verschlüsselung der Sticks?); bei großen Datenmengen: frühzeitige Datentrennung?; Pseudonymisierung von Daten usw.
Nutzen Sie nur CMS-Technik, ist hier also Schluss.

c) Soweit Systeme genutzt werden, die nicht vom CMS (bzw. der Fakultäten WiWi, Jura, Informatik) administriert werden, müssen Sie die Sicherheitsmaßnahmen dieser genutzten Systeme selbst beschreiben (sog. Sicherheitskonzept (SiKo)).

Vorzugsweise ist ein Sicherheitskonzept, welches hierüber Aufschluss gibt, dem VVT als Anlage beizulegen, da Sicherheitskonzepte üblicherweise den Platz sprengen, der hier vorgesehen ist.

Sicherheitskonzepte basieren auf einer Risikoanalyse hinsichtlich der Gefährdungen und des drohenden Schadens durch die (Probleme bei der) Datenverarbeitung. Die Sicherheitsmaßnahmen nehmen Bezug auf die analysierten Bedrohungen und minimieren diese so weit, dass das verbleibende Betriebsrisiko vertretbar ist.

Sofern es für das eingesetzte IT-System kein Siko gibt, halten Sie bitte Rücksprache mit den behDSB.)

Über folgende Maßnahmen/Schutzziele ist mindestens Auskunft zu geben (gem. Art. 32 DSGVO):

- **Pseudonymisierung, Verschlüsselung**:
  Daten werden verarbeitet, wobei die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können vgl. Art. 4 Nr. 5 DSGVO

- **Vertraulichkeit, Integrität, Verfügbarkeit (einschließlich Wiederherstellung) und Belastbarkeit der Systeme und Dienste:**
  - **Vertraulichkeit:** Vertrauliche Informationen müssen vor unbefugter Preisgabe geschützt werden, z.B. Passwortschutz, *Chipkarten, Verschlüsselung, Aufbewahrung in gesicherten Räumen*
  - **Integrität:** Schutz der Daten vor (unerlaubter) Veränderung. *Bsp.: Signatur, Verschlüsselung*
  - **Verfügbarkeit:** Daten müssen zur Verfügung stehen, z.B. regelmäßige Datensicherung/Backups, Bereithalten von Ausfallsystemen, Redundanz.

- **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen:**
  Regelmäßige Kontrollen der Wirksamkeit der Systeme, Angriffs/Fehleranalyse und ggf. Anpassung der Sicherheitsmaßnahmen.

- **Authentizität, Revisionsfähigkeit:**
  - Bestimmbarkeit der Herkunft der Daten, z.B. signierte Daten, Zusatzinformationen
  - Nachhaltbare Dokumentation von Änderungen (wer, wann, welche) z.B. Dokumentation, Verfahrensbeschreibung, Protokollierung.

- **Transparenz, Information der Betroffenen:**
  - Nachvollziehbare Dokumentation der Verarbeitung.
  - Protokollierung
  - Sicherstellung der Auskunftsrechte von Betroffenen
  - Ggf. Entsprechende Information des Betroffenen

Unter **Sonstiges** können weitere technische Maßnahmen, welche nicht in die obigen Kategorien fallen, aufgeführt werden.

Zu 12) Referenzdokumente

Hier können jeweils weitere Anlagen zum VVT hinzugefügt werden. (Auch selbst erstellte Anhänge, falls die vorgesehenen Textfelder zu klein sind oder die Inhalte zu unübersichtlich werden lassen).

Zu 13) Änderungen

Es sind gem. DSGVO Änderungen am System nachzuhalten. Wenn also nachträglich z.B. zusätzliche Datenfelder erfasst, zusätzliche Funktionen hinzugefügt, Berechtigungen geändert, die Löschfristen neu gestaltet werden oder das IT-System gewechselt wird, sind diese Änderungen im VVT nachzuhalten.

Bei Fragen nehmen Sie bitte Kontakt zu dem/der DSB auf.