„Was wollen die eigentlich von mir?“

Zum Dialog mit Datenschutzbeauftragten...

... für Beschäftigte in Fachbereichen und Verwaltung im Jahr 7+ nach Inkrafttreten der DSGVO.

Vortragsfolien mit Inhaltsverzeichnis und Glossar zum Nachlesen für alle, die beim Vortrag überwältigt oder abwesend waren.

Stand: Feb. 2025

Inhaltsverzeichnis

1. Was ist Datenschutz?
2. Wozu gibt es eigentlich Datenschutzbeauftragte?
3. DS-Grundlagen: Was sind personenbezogene Daten?
4. DS-Grundlagen: Grundsätze für Verarbeitungen
5. DS-Grundlagen: Rechtmässigkeit von Verarbeitungen
6. DS-Grundlagen: Zweckbindung und Datenminimierung
7. DS-Grundlagen: Speicherbegrenzung
8. DS-Grundlagen: Richtigkeit, Integrität und Vertraulichkeit
9. DS-Grundlagen: Transparenz und Betroffenenrechte
10. DS-Grundlagen: Strafbarkeit und Geldbusse
11. Einzelheiten: VVT, AVV & Co. - Übersicht
12. Einzelheiten: Technische und organisatorische Massnahmen („TOM“)
13. Einzelheiten: Verarbeitungen in Drittländern/„Cloud“
14. Einzelheiten: Schutzverletzungen
15. Praxis: Ein paar Tipps in loser Reihenfolge...
16. Glossar

Was ist Datenschutz?

- **Der Datenschutz schützt keine Daten, sondern Personen** vor der Verletzung ihrer grundrechtlich garantierten Persönlichkeitsrechte durch den fehlerhaften oder rechtswidrigen Umgang mit ihren Daten.
- Daraus folgt u.a.:
  1. Der beste Datenschutz wird erreicht, indem man die Verarbeitung von personenbezogenen Daten vermeidet.
  2. Wenn es bei zu verarbeitenden Daten keinen Personenbezug gibt (evtl. auch deshalb, weil man ihn geschickt vermieden hat), sind keine datenschutzrechtlichen Massnahmen erforderlich.
- **Zum Inhalt:** Nachfolgend werden wir
  - kurz auf die Grundlagen des Datenschutzes eingehen,
  - eine subjektiv getroffene Auswahl von daraus abgeleiteten Einzelheiten diskutieren und abschliessend
  - einige Praxistipps verinnerlichen.

Aber zunächst...

... wozu gibt es eigentlich Datenschutzbeauftragte?

- Rolle und Aufgaben sind festgeschrieben in Art. 37-39 DSGVO und LDSG (z.B. §§ 5-7 HDSIG); insbesondere sollen Datenschutzbeauftragte (DSB) auf die Einhaltung der DSGVO hinwirken.
- Alle von Verarbeitungen einer Hochschule betroffenen Personen können sich jederzeit direkt an die DSB wenden (oder auch direkt an die zuständige Aufsichtsbehörde, also die LDSB). Die DSB sind regelmässig auch Anlaufstelle zur Ausübung von Betroffenenrechten.
- DSB sind in Datenschutzangelegenheiten zu Vertraulichkeit verpflichtet.
- Hochschulleitungen („Verantwortliche“ i.S.v. Art. 4 DSGVO für Verarbeitungen innerhalb der jeweiligen Hochschule) werden direkt von den DSB unterrichtet und beraten.

DS-Grundlagen: Was sind personenbezogene Daten?

Wenn nachfolgend von Daten die Rede ist, sind immer **personenbezogene Daten** („**pbD**“) gemeint.

- „PbD sind alle Informationen, die sich auf eine identifizierte oder identifizierbare lebende Person beziehen. **Verschiedene Teilinformationen, die gemeinsam zur Identifizierung einer bestimmten Person führen können, stellen ebenfalls pbD dar.**“
- „PbD, die [...] verschlüsselt oder pseudonymisiert wurden, aber zur erneuten Identifizierung einer Person genutzt werden können, bleiben pbD und fallen in den Anwendungsbereich der DSGVO.“
- „PbD, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann, gelten nicht mehr als pbD. Damit die Daten wirklich anonymisiert sind, muss die Anonymisierung unumkehrbar sein.“

(https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_de)

DS-Grundlagen: Grundsätze für Verarbeitungen

- Eine **Verarbeitung** von personenbezogenen Daten schliesst so ziemlich alles ein, was man mit diesen Daten tun kann (speichern, ändern, übermitteln, etc. etc.).
- Art. 5 DSGVO regelt die Grundsätze dazu:
  - **Rechtmässigkeit**,
  - **Treu und Glauben**,
  - **Transparenz**,
  - **Zweckbindung**,
  - **Datenminimierung**,
  - **Richtigkeit**,
  - **Speicherbegrenzung**,
  - **Integrität und Vertraulichkeit**.
- Für die Einhaltung dieser Grundsätze gibt es eine **Rechenschaftspflicht** des Verantwortlichen (Art. 5 Abs. 2 DSGVO).

DS-Grundlagen: Rechtmässigkeit von Verarbeitungen 1/2

- Verbot mit Erlaubnisvorbehalt: Die Verarbeitung personenbezogener Daten (pbD) ist verboten, es sei denn, sie ist erlaubt.
- Die Erlaubnis kann sich **entweder** über Öffnungsklauseln in der DSGVO in Verbindung mit anderen Rechtsvorschriften (Beispiel: Datenverarbeitung zur Aufgabenerfüllung, Art. 6 Abs. 1 UAbs. 1 e, Art. 6 Abs. 3 DSGVO i.V.m. Landeshochschulgesetz)
- **oder** der Einwilligung der Betroffenen (Art. 6 Abs. 1 UAbs. 1 a) DSGVO) ergeben.
- Die Verarbeitung **besonderer Kategorien** pbD (sowas wie ethnische Herkunft, Gesundheitsdaten, etc.) wird in Art. 9 DSGVO nochmal strenger geregelt.

DS-Grundlagen: Rechtmässigkeit von Verarbeitungen 2/2

Kleiner Exkurs „**Einwilligung** als Rechtsgrundlage“ (da an Hochschulen zumindest im Forschungsbereich häufig benutzt):

- Geregelt in Art. 7 und 8 DSGVO; Einwilligungen
  - müssen nachweisbar und informiert gegeben werden; die Informationen zur Verarbeitung müssen in verständlicher Sprache abgefasst sein, ausserdem
  - müssen Einwilligungen freiwillig gegeben werden (das ist z.B. bei einem Beschäftigungsverhältnis schon fraglich) und
  - sind jederzeit ohne Angabe von Gründen mit Wirkung für die Zukunft widerrufbar.
- Aus Sicht von Verantwortlichen macht dies die Einwilligung u.U. zu einer „vergifteten“ Rechtsgrundlage für Verarbeitungen. Beispiel: Bebilderte Broschüre muss eingestampft werden, weil eine abgebildete Person ihre Einwilligung widerrufen hat.
- Auch bei Art. 9-Daten ist eine Verarbeitung auf Basis einer **ausdrücklichen Einwilligung** möglich (Art. 9 Abs. 2 UAbs. 2 a DSGVO).

DS-Grundlagen: Zweckbindung und Datenminimierung

- Art. 5 Abs. 1 UAbs. 1 b DSGVO: „PbD müssen für **festgelegte**, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; [...] (**Zweckbindung**); [...]“.
  Die Festlegung der Zwecke erfolgt **durch den Verantwortlichen** und **vor** der Verarbeitung.
  Es gibt Ausnahmen von der Zweckbindung, u.a. für die Forschung; diese sind jedoch wiederum an Bedingungen gebunden.
- Art. 5 Abs. 1 UAbs. 1 c DSGVO: „PbD müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (**Datenminimierung**); [...]“

DS-Grundlagen: Speicherbegrenzung

- Aus dem Grundsatz der **Speicherbegrenzung** (Art. 5 Abs. 1 UAbs. 1 e) und dessen Konkretisierung in Gestalt des Rechts auf Löschung („**Recht auf Vergessenwerden**“, Art. 17 DSGVO) ergibt sich, dass eine **Löschung oder** (wirksame!) **Anonymisierung** erfolgen muss, wenn (häufigster, aber nicht einziger Grund) die pbD zur Erfüllung des vorgesehenen Zwecks nicht mehr erforderlich sind **und** gewisse andere Umstände **nicht** gegeben sind (z.B. eine gesetzliche Aufbewahrungspflicht).
- Der Grundsatz der Speicherbegrenzung wird durch den Grundsatz der Zweckbindung ergänzt:
  Ohne einen klar definierten Zweck wäre der Zeitpunkt der Löschung von Daten nach dessen Erfüllung möglicherweise nicht eindeutig festzulegen.
  Die Zweckbindung verhindert zudem, dass der Zweck im Nachhinein geändert werden kann (es gibt Ausnahmen) und damit potentiell die Löschpflicht aufgeweicht oder gar umgangen wird.

DS-Grundlagen: Richtigkeit, Integrität und Vertraulichkeit

Der Verantwortliche muss mithilfe technischer und organisatorischer Massnahmen sicherstellen, dass

- die zu verarbeitenden Daten „**sachlich richtig** und erforderlichenfalls auf dem neuesten Stand [sind]“,
- die Daten **verfügbar** sind („kein Backup, kein Mitleid“) und
- nur diejenigen Zugriff auf die Daten haben, die diesen benötigen, um den Verarbeitungszweck zu erfüllen. Der Umfang des Zugriffs soll sich am „**Need-to-know-Prinzip**“ orientieren, d.h. so weitgehend wie nötig, aber so beschränkt wie möglich sein.

Die DSGVO sieht eine **Verschwiegenheitspflicht** zwar nicht ausdrücklich vor, aus dem Gebot der nur weisungsgebundenen Verarbeitung in Art. 29 DSGVO i.V.m. Art. 32 Abs. 4 DSGVO wird jedoch auch ein **Datengeheimnis** abgeleitet (also ein Verbot von unbefugten Verarbeitungen, das implizit auch eine Verschwiegenheitspflicht beinhaltet). Ein Datengeheimnis besteht auch nach Beendigung eines Beschäftigungsverhältnisses fort.

DS-Grundlagen: Transparenz und Betroffenenrechte

Mit der DSGVO wurden Betroffenenrechte erheblich erweitert (Art. 12-22). Im Einzelnen gibt es

- eine **Informationspflicht** des Verantwortlichen bei der Erhebung von Daten sowohl von den Betroffenen direkt als auch bei der Erhebung von Daten aus anderen Quellen als den Betroffenen selbst,
- ein **Auskunftsrecht** der Betroffenen (mit Fristen, diesem nachzukommen),
- sowie Rechte auf **Berichtigung**, **Löschung**, **Einschränkung der Verarbeitung**, **Datenübertragbarkeit** sowie **Widerspruch gegen die Verarbeitung**, jeweils beim Vorliegen bestimmter Voraussetzungen.

Fussnote: Die Erweiterung der Betroffenenrechte gehört (neben den Regelungen zu Geldbussen) zu den wenigen wirklich erheblichen Änderungen, die das Inkrafttreten der DSGVO im Jahr 2018 (eigentlich schon 2016) im Vergleich zur Rechtslage in Deutschland vorher mit sich gebracht hat. Die meisten anderen Regelungen der DSGVO galten so oder ähnlich bereits vorher im Rahmen von Bundes- und Landesgesetzen - es hat sich nur kaum jemand drum geschert, weil Verstösse milde oder gar nicht geahndet wurden.

DS-Grundlagen: Strafbarkeit und Geldbusse

- (Nach aussen) verantwortlich für die Einhaltung datenschutzrechtlicher Bestimmungen ist die Leitung der Hochschule. Der deutsche Gesetzgeber hat (leider?) Geldbussen gegen öffentliche Stellen ausgeschlossen (nicht aber Haftung, d.h. **Hochschulen sind gegen Schadenersatzklagen nicht gefeit** - bei krassen Verstössen oder auch „nur“ vielen Betroffenen kann das teuer werden).
- Für Sie persönlich gilt: Wenn Sie personenbezogene Daten **fahrlässig oder vorsätzlich** unzulässig verarbeiten, kann das als Ordnungswidrigkeit oder (bei Vorsatz) als Straftat verfolgt werden. Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe kann bestraft werden, wer z.B. Adresslisten der Hochschule an Dritte übermittelt, um sich oder einen anderen zu bereichern (§ 37 Abs. 1 HDSIG - andere Bundesländer haben ähnliche Regelungen).

Einzelheiten: VVT, AVV & Co. - Übersicht 1/3

- Ein **Verarbeitungsverzeichnis** (**VV**, auch: **VVT** für „Verzeichnis von Verarbeitungstätigkeiten“) ist praktisch für jede Verarbeitung erforderlich und enthält eine Beschreibung dieser Verarbeitung in dem von der DSGVO vorgegebenen Umfang. Ein VVT ist ein „lebendes“ Dokument, d.h. es wird bei evtl. Änderungen in der Verarbeitung aktualisiert.
- Aus der Informationspflicht des Verantwortlichen ergibt sich die Notwendigkeit zur Erstellung einer **Datenschutzinformation** für die Betroffenen (im Fall einer Verarbeitung mit Einwilligung als Rechtsgrundlage: Datenschutzinformation mit **Einwilligungserklärung**).

Einzelheiten: VVT, AVV & Co. - Übersicht 2/3

- Soll ein externer Dienstleister Daten **im Auftrag und auf Weisung** des Verantwortlichen verarbeiten (Art. 28 DSGVO), ist der Abschluss eines **Auftragsverarbeitungsvertrags** (**AVV**) erforderlich. Beispiele: Hoster, SaaS-Anbieter u.ä.
  - Bei Auftragsverarbeitung bleibt die Verantwortung für die pbD beim Auftraggeber, geht also nicht etwa an den Auftragsverarbeiter über. Das ist der wesentliche Unterschied zur gemeinsamen Verantwortlichkeit (nachfolgender Punkt).
- Gibt es eine externe Einrichtung, die **gemeinsam mit dem Verantwortlichen über Mittel und Zwecke der Verarbeitung entscheidet**, ist der Abschluss eines Vertrags zur **gemeinsamen Verantwortlichkeit** erforderlich (Art. 26 DSGVO). Beispiel: Kooperation mehrerer Hochschulen bei einem Forschungsprojekt.
- AVV und Verträge zur gemeinsamen Verantwortlichkeit werden grundsätzlich von der Hochschulleitung geschlossen (unterschrieben).

Einzelheiten: VVT, AVV & Co. - Übersicht 3/3

- Die DSGVO über **Datenschutz-Folgenabschätzungen (DSFA)**: *Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.*
  - Es gibt eine „Muss-Liste“ von Verarbeitungen, die zwingend eine DSFA erfordern (normalerweise bei den LDSB einsehbar).
  - DSFA können schnell aufwendig und komplex werden - reden Sie mit Ihren DSB.

Der „perfekte Sturm“: Hochrisiko-Verarbeitung als gemeinsames Vorhaben mit externem Dienstleister und Einwilligung als Rechtsgrundlage $\longrightarrow$ Bingo! Alle o.g. Massnahmen/Dokumente erforderlich (wäre noch zu toppen durch eine zusätzliche Datenübermittlung in ein Drittland).

Einzelheiten: Technische und organisatorische Massnahmen („TOM“)

- Art. 32 DSGVO „Sicherheit der Verarbeitung“
- Die TOM, die Sie (und ein evtl. Auftragsverarbeiter) ergreifen, um den ordnungsgemässen Umgang mit den personenbezogenen Daten in Ihrer Verantwortung sicherzustellen, müssen geeignet sein, um ein **dem Risiko angemessenes Schutzniveau zu gewährleisten**(*). „Unter anderem“ werden Massnahmen gefordert
  - zu Pseudonymisierung und Verschlüsselung,
  - zur Sicherstellung der dauerhaften Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung,
  - zur raschen Wiederherstellung der Verfügbarkeit der pbD bei einem physischen oder technischen Zwischenfall sowie
  - zu Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der getroffenen TOM.

(*) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der von Ihrer Verarbeitung betroffenen natürlichen Personen.

Einzelheiten: Verarbeitungen in Drittländern/„Cloud“ 1/2

- Für in Drittländer (alle Länder, in denen die DSGVO nicht gilt) übermittelte pbD **soll ein mit dem der DSGVO vergleichbares Schutzniveau gelten**.
- Von Ausnahmen abgesehen kann das vom Verantwortlichen nur gewährleistet werden, wenn entweder für das fragliche Land ein **Angemessenheitsbeschluss** besteht oder ein AVV mit sog. „**Standard-Vertragsklauseln**“ abgeschlossen wird.
- Bei der Nutzung von Clouddiensten sind oft nicht nur datenschutzrechtliche Regelungen, sondern auch andere Verpflichtungen zu beachten (z.B. NDAs).

Einzelheiten: Verarbeitungen in Drittländern/„Cloud“ 2/2

Da die Nutzung der meisten Clouddienste eine Übermittlung pbD in die USA bzw. unter US-Kontrolle impliziert, hier die momentane Rechtslage für den Problemfall USA:

- Für das aktuelle „Data Privacy Framework“ („DPF“) existiert ein Angemessenheitsbeschluss der EU-Kommission.
- Sofern ein US-Anbieter „DPF-zertifiziert“ ist **und** ein AVV geschlossen wurde, ist eine Übermittlung pbD zulässig.
- Eine DPF-Zertifizierung muss vorab (von Ihnen!) geprüft werden: `https://www.dataprivacyframework.gov/s/participant-search`
- Das DPF wird möglicherweise (wie dessen Vorgänger) in absehbarer Zukunft „weggeklagt“ oder aufgekündigt, also Vorsicht mit allzu grossen Abhängigkeiten von US-Anbietern.

Einzelheiten: Schutzverletzungen

- Art. 33 DSGVO regelt „Meldungen zu Verletzungen des Schutzes personenbezogener Daten“.
- Wenn personenbezogene Daten
  - abhanden gekommen sind (allgemein: **Kontrollverlust**) bzw. Anlass zu der Annahme besteht, dass dies passiert sein könnte(!) oder
  - zum Nachteil der Betroffenen **kein Zugriff mehr** darauf besteht,

  ist eine Meldung an die Aufsichtsbehörde fällig.
- Die **Meldefrist** beträgt 72 Stunden nach Bekanntwerden - deshalb nicht lange überlegen, sondern zum Telefonhörer greifen, die eigenen DSB anrufen und „beichten“.
- Typische und häufige Schutzverletzungen: Laptop oder USB-Stick im Bus vergessen, verloren oder gestohlen, E-Mail mit hunderten Adressen im „CC:“, Postbriefe falsch kuvertiert, Programmier- oder Konfigurationsfehler verursacht Zugriff durch unberechtigte Dritte, Restore nach Datenbank- oder Filesystem-Crash funktioniert nicht oder nur mit Datenverlust, etc. pp.

Praxis: Ein paar Tipps in loser Reihenfolge... 1/3

... basierend auf den Erfahrungen des Datenschutzteams der Universität aus gefühlt zahl- und endlosen E-Mails und Telefongesprächen:

- Bedenken Sie beim Verfassen eines VVT, dass i.d.R. weder Ihre DSB noch die Aufsichtsbehörde die näheren Gegebenheiten Ihrer Verarbeitung kennen. Schreiben Sie deshalb (speziell beim Zweck) ein paar Sätze zum „grossen Ganzen“ Ihrer Verarbeitung (aber keine Romane!). Erklären Sie Abkürzungen, die nicht allgemein bekannt sind.
- Insbesondere beim Verfassen eines VVT mag es hilfreich sein, sich die eigene Verarbeitungstätigkeit als einen Datenfluss vorzustellen: Woher stammen die Daten (z.B. aus einer Umfrage oder dem Campus-Management-System)? Wohin gehen sie (z.B. Übermittlung an eine andere Einrichtung oder einfach Löschung bzw. Anonymisierung)? Was geschieht dazwischen (z.B. Verarbeitung durch einen Auftragsverarbeiter)? Welche Massnahmen ergreifen Sie, um z.B. die Vertraulichkeit und Integrität der Daten zu gewährleisten?

Praxis: Ein paar Tipps in loser Reihenfolge... 2/3

- Denken Sie Datenschutz mit, wenn Sie Entscheidungen für eine bestimmte Software oder Plattform treffen:
  - Verarbeitungen auf internen Systemen durch eigenes Personal („on premises“) sind besser als Auftragsverarbeitungen im Geltungsbereich der DSGVO. Diese wiederum sind besser als Auftragsverarbeitungen in einem Drittland.
  - Open Source Software „telefoniert“ nicht „nach Hause“ (und wenn doch, kann man es abstellen).
  - Art. 25 DSGVO fordert Massnahmen für den Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen; z.B. wurde beim sog. „hessischen Modell“ für Zoom (eine Plattform für Videokonferenzen) u.a. durch Voreinstellungen erreicht, dass Zoom nur noch minimal pbD an den Hersteller übermittelt und so zumindest für die Lehre einsetzbar blieb.
- Auftragsverarbeiter (zumindest die im Geltungsbereich der DSGVO) haben typischerweise fertige DSGVO-konforme AVV parat, die Sie auf Anfrage erhalten und prüfen (oder besser durch Ihre DSB prüfen lassen) können.

Praxis: Ein paar Tipps in loser Reihenfolge... 3/3

- Benutzen Sie in den Datenschutzinformationen für Ihre Betroffenen nicht den Begriff „anonym“, wenn Sie eigentlich „pseudonym“ meinen (anonyme Daten sind nicht personenbezogen, pseudonyme schon).
- Wenn Sie mit Einwilligung als Rechtsgrundlage arbeiten, erwähnen Sie, dass diese freiwillig ist, bei Nichteinwilligung keine Nachteile entstehen und die Einwilligung jederzeit ohne Angabe von Gründen widerrufen werden kann. Eine Kontaktadresse u.a. hierfür ist ebenfalls Pflicht.
- Die TOM sind erfahrungsgemäss der schwierigste Teil eines VVT. Ihr Leben ist leichter, wenn Sie, zumindest für zentrale Verarbeitungen, auf ein bestehendes Datensicherheitskonzept oder Zertifikat verweisen können.
- Denken Sie auch an den Datenschutz, wenn Sie interne Dokumentation oder Anleitungen für zentral genutzte Software oder Dienste schreiben. Im Zweifel konsultieren Sie Ihre DSB.

Glossar

- Art./Abs./UAbs. - Artikel/Absatz/Unterabsatz
- AV/AVV - Auftragsverarbeiter (Dienstleister)/ Auftragsverarbeitungsvertrag
- DPF - EU-US Data Privacy Framework
- DSFA - Datenschutz-Folgenabschätzung
- DSB - Datenschutzbeauftragte
- DSGVO/DS-GVO - Datenschutz-Grundverordnung der EU
- HDSIG - Hessisches Datenschutz- und Informationsfreiheitsgesetz (Nachfolger des Hessischen Datenschutzgesetzes, HDSG)
- Hoster - Dienstleister für Internetdienste
- LDSG - Landesdatenschutzgesetz
- NDA - Non-Disclosure Agreement (Vertraulichkeitsvereinbarung)
- PbD - Personenbezogene Daten
- SaaS - Software-as-a-Service
- TOM - Technische und organisatorische Massnahmen
- VV/VVT - Verarbeitungsverzeichnis/Verzeichnis von Verarbeitungstätigkeiten (synonym)