TECHNISCHE UNIVERSITÄT WIEN






Richtlinie – Datenschutz und Informationssicherheit

(Online 30.04.2019)

Beschluss des Rektorates vom 16.04.2019

Verlautbarung im Mitteilungsblatt Nr. 15/2019 vom 02.05.2019 (lfd. Nr. 135)

GZ: 30002.04/028/2019

Richtlinie – Datenschutz und Informationssicherheit

PRÄAMBEL

Die Technische Universität Wien (TU Wien) verarbeitet zur Erfüllung ihrer Aufgaben unter anderem personenbezogene Daten. Der Schutz dieser Daten ist der TU Wien ein großes Anliegen. Dieses Dokument enthält Richtlinien, die zum einen sicherstellen, dass personenbezogene Daten entsprechend den Vorgaben der Datenschutzgrundverordnung (DSGVO) verarbeitet werden und zum anderen sollen diese gewährleisten, dass an der TU Wien ein möglichst hohes Niveau an Informationssicherheit erreicht und eingehalten wird.

Im ersten Abschnitt dieses Dokuments werden die allgemeinen Grundsätze bzgl. Datenschutz und Informationssicherheit angeführt. Die weiteren Abschnitte enthalten die einzelnen Richtlinien. Bei Verfügbarkeit weiterer den Datenschutz und die Informationssicherheit betreffenden Richtlinien wird das vorliegende Dokument entsprechend erweitert.

1 ALLGEMEINE GRUNDSÄTZE

Dieses Dokument adressiert alle Angehörigen der TU Wien gem. § 94 Universitätsgesetz (UG). Dritte werden gegebenenfalls zur Einhaltung der in diesen Richtlinien enthaltenen Anforderungen in gesonderten Verträgen verpflichtet. Die in diesem Dokument enthaltenen Richtlinien gelten ohne zeitliche und örtliche Einschränkungen. Die einzelnen Richtlinien können Spezifizierungen hinsichtlich des Geltungsbereichs vorsehen.

1.1 DATENSCHUTZ UND INFORMATIONSSICHERHEIT

Das Grundrecht auf Datenschutz gilt für sämtliche personenbezogene Daten. Das sind alle Informationen die sich auf eine identifizierte oder identifizierbare Person beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.[1]

[1] Siehe Art. 4 DSGVO.

Für personenbezogene Daten gelten umfassende, zwingend zu beachtende Schutzerfordernisse. Diese Daten sind mit entsprechenden technischen und organisatorischen Mitteln unter wirtschaftlich vertretbarem Aufwand abzusichern. Der gesetzliche Datenschutz ist stets zu gewährleisten.

Informationssicherheit hat den Schutz von Informationen zum Ziel. Alle Geschäftsabläufe in einer Organisation sind von Informationen und einem geregelten Informationsfluss abhängig, weshalb es von großer Bedeutung ist, ein angemessenes Niveau der Informationssicherheit zu erreichen und aufrechtzuerhalten. IT-Sicherheit beschäftigt sich an erster Stelle mit dem Schutz von Vertraulichkeit, Verfügbarkeit und Integrität elektronisch gespeicherter Informationen und deren Verarbeitung.

Informationssicherheit ist auf den Schutz personenbezogener und unternehmensbezogener Information sowie auf kritische Geschäftsprozesse fokussiert. Damit soll verhindert werden, dass Daten verloren gehen, manipuliert oder verfälscht werden bzw. unberechtigtem Zugriff ausgesetzt sind.[2]

1.2 MELDUNG VON SICHERHEITSVORFÄLLEN UND -MÄNGELN

Sicherheitsrelevante Vorfälle und Sicherheitsmängel sind von allen Personen, die im Geltungsbereich der nachfolgenden Richtlinien definiert sind, umgehend an den_die Unmittelbar Vorgesetzte_n, den_die Informationssicherheitsbeauftragte_n und – wenn personenbezogene Daten betroffen sind – an den_die Datenschutzbeauftragte_n zu melden.

1.3 EINHALTUNG DER RICHTLINIEN

Die Einhaltung der in den nachfolgenden Richtlinien enthaltenen Regelungen und Sicherheitsmaßnahmen wird regelmäßig, aber auch anlassbezogen überprüft. Die in diesem Dokument enthaltenen Richtlinien sind zum Zweck der Gewährleistung des Datenschutzes und der Informationssicherheit sowie zur Vermeidung von Rechtsansprüchen unbedingt einzuhalten.

[2] Vgl.: Institut für Interne Revision Österreich IIA Austria (Hrsg.): Informationssicherheitsmanagementsystem. Damoklesschwert Daten-Gau – Systematische Prüfung und wirksame Prävention. Wien 2016. S. 6.

1.4 AUSNAHMEN VON EINZELNEN RICHTLINIEN

Es ist generell zunächst eine Vorgehensweise zu wählen, die den geltenden Richtlinien entspricht. Erst wenn dies

a. technisch oder organisatorisch nicht möglich ist, ODER
b. nicht wirtschaftlich ist, ODER
c. wenn es der Forschungszweck, ODER
d. die Förderrichtlinien eines Fördergebers verlangen,

kann über eine Ausnahmeregelung entschieden werden. Ausnahmen müssen

- zeitlich begrenzt sein,
- auf einen Zweck und Benutzer_innenkreis eingeschränkt werden,
- hinsichtlich Antrag, Genehmigung/Ablehnung, Änderungen und Auslaufen dokumentiert werden,
- kontrolliert und im Falle des Auslaufens ohne Neuantrag nach entsprechender Frist aufgehoben werden,
- im Falle der Nichtbeachtung anderer einschlägiger Richtlinien der TU Wien umgehend aufgehoben werden.

Der Antrag zur Erteilung einer Ausnahme in Bezug auf Informationssicherheit ist von Mitarbeiter_innen der TU Wien an das laut Geschäftsordnung zuständige Rektoratsmitglied zu stellen.

Die aktuell gewährten Ausnahmen werden getrennt von dieser Richtlinie von dem_der Leiter_in der TU.it verwaltet. Die dokumentierten Ausnahmen werden auf Anfrage von dem_der TU.it Leiter_in bereitgestellt.

2 LOGGING RICHTLINIE

Diese Richtlinie gilt verpflichtend für alle Personen, die im Namen oder im Auftrag der TU Wien Protokolldaten („Logdaten“) erzeugen oder verwenden.

Zur Erfüllung der Aufgaben der TU Wien ist die Erfassung von Protokolldaten in Informationssystemen erforderlich. Zweck dieser Richtlinie ist es, Regelungen für die Verwendung derart erzeugter Protokolldaten, insbesondere im Hinblick auf den Datenschutz und die Informationssicherheit zu treffen. Adressiert wird in dieser Richtlinie ausschließlich die Protokollierung personenbezogener Daten im Sinne der Datenschutzgrundverordnung (DSGVO) und des Datenschutzgesetzes (DSG) inklusive verwandter Gesetze wie z.B. das Forschungsorganisationsgesetz (FOG).

2.1 BEGRIFFSBESTIMMUNGEN

Im Kontext dieses Dokuments werden Begriffe wie folgt definiert:

Logging
Unter Logging wird die manuelle und rechnergestützte Protokollierung von im Zuge von IT-Prozessen entstehenden Ereignissen und Zuständen verstanden.

Logdatei, Logdaten
Unter einer Logdatei wird ein automatisch geführtes Ereignisprotokoll von Prozessen auf einem IT-System verstanden. Die dadurch entstandenen Daten werden als Protokolldaten oder Logdaten bezeichnet. History-, cache- und temporäre Dateien werden nicht zentral gespeichert und in der Regel nur für sehr kurze Zeit von IT-Systemen aufbewahrt und sind daher nicht Gegenstand dieser Richtlinie.

Daten im Sinne der Datenschutzgrundverordnung und des Datenschutzgesetzes:

a. „Personenbezogene Daten“
   Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (siehe Unterabschnitt 1.1) – im Folgenden „betroffene Person“ – beziehen.

b. „Besondere Kategorien von Daten“
   (besonders schutzwürdige Daten; früher: sensible Daten)

Personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische und biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

„Betroffene_r“
Jede natürliche Person, deren Daten verarbeitet werden.

2.2 GRUNDLAGEN

Das Logging hat nach dem Prinzip der Datensparsamkeit zu erfolgen. Dies bedeutet, dass die Erfassung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung der Informationssysteme und Protokollierungsmechanismen am Ziel auszurichten sind, so wenig personenbezogene Daten wie möglich zu erheben und zu verwenden.

2.3 ZWECKE DES LOGGINGS UND AUFBEWAHRUNGSDAUER VON LOGDATEN

Aufzeichnungen personenbezogener Logdaten dürfen nur zu folgenden Zwecken durchgeführt bzw. verwendet werden:

a. Gewährleistung der Systemsicherheit;
   Aufbewahrung der Logdaten: bis zu 90 Tage (da möglicherweise zur Gewährleistung der Datenintegrität erforderlich).

b. Gewährleistung der Systemfunktionalität;
   Aufbewahrung der Logdaten: bis zu 30 Tage.

c. Analyse und Korrektur von technischen Fehlern im System:
   Aufbewahrung der für die Behandlung des Problems relevanten Daten: so lange, bis der Fehler identifiziert bzw. behoben ist, längstens jedoch 30 Tage.

d. Optimierung der Systemleistung;
   Diese setzt großteils auf bereits existierende Logdaten auf und ist u.a. im Zusammenhang mit der Leistungsverrechnung und möglichst effektiven Nutzung existierender Systemressourcen zu sehen.

Aufbewahrung: bis zu 30 Tage. Ergibt sich die Notwendigkeit einer längeren Aufbewahrungsdauer, sind die benötigten Daten nur in anonymisierter Form zu halten.

e. Leistungsverrechnung für den Systembetrieb;
Aufbewahrung: über den Abrechnungszeitraum hinweg, zuzüglich allfälliger Einspruchsfristen.

2.4 VERWENDUNG VON LOGDATEN BEI VERDACHT AUF RECHTSWIDRIGES VERHALTEN

Bei begründetem Verdacht der Verletzung gesetzlicher, vertraglicher oder dienstlicher Pflichten durch eine_n Mitarbeiter_in erhält diese_r zunächst die Möglichkeit, sich persönlich gegenüber der_dem Unmittelbar Vorgesetzten zu dem Verdacht zu äußern. Auf Wunsch des_der Mitarbeiter_in ist ein_e Vertreter_in des Betriebsrats über den Verdacht zu informieren und/oder beizuziehen.

Kann die Angelegenheit nicht aufgeklärt werden, so wird entweder auf ausdrücklichen Wunsch des_der Mitarbeiter_in oder aber durch den_die Unmittelbar Vorgesetzte_ n nach Information und/oder Beiziehung des_der Datenschutzbeauftragten sowie des Betriebsrates in die entsprechenden Logdaten Einsicht genommen. Bei der Einsichtnahme ist möglichst schonend vorzugehen und sie ist auf den konkreten Verdacht des Missbrauchsfalls zu beschränken. Die Einsichtnahme ist zu protokollieren.

Besteht der Verdacht auf regel- oder rechtswidriges Verhalten, können relevante Logdaten durch den_die Leiter_in der TU.it im notwendigen Ausmaß auf Basis der Entscheidung des_der Datenschutzbeauftragten und in Abstimmung mit der Abteilung Interne Revision (Vier-Augenprinzip) gesichert und bis zur Klärung des Sachverhalts – unabhängig von den oben genannten Löschfristen – gespeichert werden. Die Speicherung ist zu protokollieren.

2.5 ÜBERMITTLUNG VON LOGDATEN (INTERN SOWIE AN DRITTE)

Mitarbeiter_innen dürfen Logdaten nur auf Grund einer ausdrücklichen Anordnung ihres_r Unmittelbar Vorgesetzten übermitteln. Bevor Logdaten übermittelt werden, ist sicherzustellen, dass diese Daten anonymisiert sind oder entsprechende Vertraulichkeitsvereinbarungen mit dem_der Empfänger_in bestehen.

Eine Übermittlung von personenbezogenen Daten darf nur auf gesetzlicher Basis, insbesondere unter Beachtung der DSGVO, des Datenschutzgesetzes (DSG) sowie verwandter Gesetze, erfolgen.

Intern dürfen Logdaten ausschließlich an die Interne Revision, an das Rektorat, an den_die Leiter_in der TU.it, den_die Datenschutzbeauftragte_n und den_die Informationssicherheits-beauftragte_n übermittelt werden.

An Dritte dürfen Logdaten ausschließlich auf Anweisung des Rektorats übermittelt werden.

2.6 AUSWERTUNG VON LOGDATEN

Eine Auswertung von Logdaten im Hinblick auf das Verhalten einzelner Personen ist untersagt, es sei denn,

- die Auswertung ist zur Erfüllung der in Unterabschnitt 2.4 genannten Zwecke erforderlich und erfolgt mit Zustimmung bzw. auf Wunsch der betroffenen Person (wobei Betriebsrat und Datenschutzbeauftragte_r über die Auswertung zu informieren und/oder beizuziehen sind), oder
- die Auswertung ist zur Erfüllung gesetzlicher Pflichten erforderlich (z.B. Weitergabe an Ermittlungsbehörden).

Eine Leistungskontrolle von Mitarbeiter_innen anhand von Logdaten ist in jedem Fall untersagt.

2.7 EINZELPERSONENBEZOGENE LÖSCHUNG VON LOGDATEN UND BACKUPS

Eine Löschung einzelpersonenbezogener Logdaten, z.B. nach dem Austritt einer Person, ist nicht durchzuführen. Logdaten, die in Backups enthalten sind, fallen nicht unter die Löschfristen dieser Richtlinie.

3 CLOUD-RICHTLINIE

Die TU Wien regelt den Umgang mit Cloud-Services und zielt dabei primär auf unter allen Umständen einzuhaltende rechtliche Anforderungen, wie z.B. Datenschutz sowie Daten und Informationssicherheitserfordernisse ab, gefolgt von den Anforderungen hinsichtlich Funktionalität, Leistungsfähigkeit, Wirtschaftlichkeit und Bedienkomfort.

IT-basierte Services wurden bisher nahezu ausschließlich durch die TU Wien selbst zur Verfügung gestellt. Zunehmend werden sie aber auch von externen Anbietern in hoch standardisierter Form angeboten. Solche Cloud-Services können eine Ergänzung zu den von der TU Wien selbst betriebenen Services sein.

3.1 BEGRIFFSBESTIMMUNGEN

Im Kontext dieses Dokuments werden Begriffe wie folgt definiert:

Cloud-Computing

Unter Cloud-Computing wird eine IT-Infrastruktur verstanden, die es erlaubt bei Bedarf, jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen zuzugreifen, die schnell und mit minimalem Managementaufwand oder geringer Serviceprovider-Interaktion zur Verfügung gestellt werden können.[3]

Cloud-Services

Unter Cloud-Services werden IT-Dienstleistungen verstanden, die auf Basis von Cloud-Computing in der Regel dynamisch an den Bedarf angepasst über das Internet angeboten, genutzt und abgerechnet werden können, z.B. Netze, Server, Speichersysteme oder Anwendungen.

3.2 GRUNDLAGEN

Die folgenden Ausführungen gelten für Cloud-Services wie unten beschrieben, umfassen aber auch andere Auslagerungsvarianten („Sourcing“-Varianten), die Cloud-Computing-ähnlich ausgestaltet sind.

[3] Siehe: https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Grundlagen/Grundlagen_node.html (zuletzt abgerufen am 23.10.2018).

3.3 BEREITSTELLUNGSMODELLE (DEPLOYMENT MODELS)

Im Rahmen dieser Richtlinie wird zwischen den folgenden Bereitstellungsmodellen von Cloud-Computing unterschieden:

Private Cloud: Die Cloud-Infrastruktur wird von einer Institution nur für eigene Zwecke betrieben. An der TU Wien sind das vor allem Services, die von der TU.it der TU Wien betrieben werden (z.B. TUownCloud bzw. TUproCloud).

Community Cloud: In diesem Fall wird die Infrastruktur von mehreren Institutionen geteilt, die ähnliche Interessen haben. Für die TU Wien wären das zum Beispiel Services, die von ausgewählten Anbietern innerhalb des akademischen Wissenschaftsnetzes betrieben werden (z.B. ACOnet, FileSender oder iMooX).

Public Cloud: Darunter versteht man Cloud-Services, die von der Allgemeinheit oder einer großen Gruppe genutzt werden können. Im konkreten Kontext bedeutet dies, dass die Infrastruktur nicht durch die TU Wien oder eine Organisation im akademischen Umfeld betrieben wird (z.B. ALMA, eRecruiter oder termino.gv.at).

3.4 ANWENDUNGSBEREICHE VON CLOUD-SERVICES

Diese Regelung betrifft alle Anwendungsbereiche von Cloud-Services. Die im universitären Umfeld wichtigsten sind:

- Nutzung von Anwendungen[4],
- Nutzung von Speicherplatz[5],
- Nutzung von Rechenleistung,
- Datenaustausch mit Externen.

3.5 VORGEHENSWEISE ZUR AUSWAHL EINES CLOUD-SERVICES

Bei der Überlegung, Cloud-Services zu nutzen, ist primär der Schutzbedarf der zugrundeliegenden Daten entscheidend.

[4] z.B. E-Mail, Termin- und Projektplanung, Projekt- und Teamplattformen, Kassenlösungen.
[5] z.B. zur Archivierung oder für Backup-Zwecke.

Personenbezogene Daten dürfen nur im Einklang mit den geltenden Datenschutzbestimmungen verarbeitet und übermittelt werden.

Bei der Auslagerung von personenbezogenen Daten und Anwendungen in die Cloud sind insbesondere die datenschutzrechtlichen Grundprinzipien[6] zu beachten.

Bei urheberrechtlich geschützten Inhalten sind ferner die Bestimmungen des Urheberrechts einzuhalten.

Darüber hinaus sind die von der TU Wien formulierten Grundsätze der Informationssicherheit zu beachten.[9]

Für die Wahl eines Cloud-Services gilt die folgende Reihenfolge:

1. **Private Cloud** Service;
2. **Community Cloud** Service;

nur dann, wenn von diesen die gewünschte Funktionalität nicht bereitgestellt werden kann, kommt die Inanspruchnahme eines

3. **Public Cloud** Service, explizit NUR nach Freigabe durch die TU.it in Frage.

3.6 NUTZUNG VON PUBLIC CLOUD SERVICES

Die Nutzung eines Public Cloud Services ist unter folgenden Voraussetzungen erlaubt:

- Es werden keine personenbezogenen Daten im Sinne der DSGVO Art. 9 und Art. 10 verarbeitet, ausgenommen der Speicherort der personenbezogenen Daten befindet sich in einem Vertragsstaat der Europäischen Union oder in einem Drittstaat mit angemessenem Datenschutzniveau[7] UND
- es werden keine Daten gespeichert, die einem Geschäfts- oder Betriebsgeheimnis unterliegen, UND

[6] Siehe dazu: Datenschutz-Handbuch der TU Wien Kapitel 2.

[9] Siehe dazu die im vorliegenden Dokument enthaltenen Richtlinien.

[7] Zum Zeitpunkt der Erstellung dieser Richtlinien gehören gem DSGVO zu den sicheren Drittstaaten: Andorra, Argentinien, Kanada (nur kommerzielle Organisationen), Färöer, Guernsey, Israel, Isle of Man, Jersey, Neuseeland, Schweiz, Uruguay und die USA (wenn der Empfänger „Privacy Shield“ zertifiziert ist). In diese Drittländer ist die Datenübermittlung ausdrücklich gestattet, wobei im Falle der USA der CLOUD (Clarifying Lawful Overseas Use of Data) Act zu beachten ist. Des Weiteren wird darauf hingewiesen, dass die Firma Google ihre Rechenzentren nicht ausschließlich in den USA betreibt.

- der Public Cloud Provider verfügt über eine aufrechte Zertifizierung nach ISO/IEC 27001 (Information technology – Security techniques – Information security management systems – Requirements) einschließlich der Umsetzung des erweiterten Kontrollsets und den Umsetzungsempfehlungen aus ISO/IEC 27018 (Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors) oder einem vergleichbaren Datenschutzsiegel.

Daten die allgemein verfügbar und bereits legal veröffentlicht sind, dürfen in einer Public Cloud gespeichert werden. An ihnen besteht kein schutzwürdiges Geheimhaltungsinteresse, womit eine Prüfung der obigen Voraussetzungen nicht notwendig ist.

3.7 UMSETZUNG

Für die Umsetzung dieser Richtlinie ist der_die Dateneigentümer_in verantwortlich.

Folgender Genehmigungsablauf ist für Public Cloud-basierte Anwendungen erforderlich:

- Bedarfsanforderung aus Forschungs-, Lehr- und zentralen Serviceeinheiten nach einer zentralen IT-Lösung an die TU.it.
- Ist eine der Lösungsvarianten eine Public Cloud-basierte Variante, ist die Einbindung der TU.it sowie die Abstimmung mit dieser verpflichtend.
- Wird eine Public Cloud-basierte Variante von der TU.it freigegeben, so muss der TU.it ausreichende Dokumentation zur Verfügung gestellt werden sowie die notwendigen Einträge in das Verzeichnis der Verarbeitungstätigkeiten inklusive Auftragsdaten-vereinbarung durch den_die Dateneigentümer_in mit Unterstützung des_der zuständigen Datenschutzkoordinator_in erfolgen.

4 PASSWORT-RICHTLINIE

Für die Gewährleistung des Datenschutzes und der Informationssicherheit ist die Verwendung von sicheren Passwörtern unerlässlich. Die gegenständliche Richtlinie ist im Rahmen der technischen Möglichkeiten auf alle IT- und Telekommunikationssysteme der TU Wien anzuwenden, deren Ressourcen und Daten durch Passwörter vor unberechtigtem Zugriff und missbräuchlicher Verwendung oder Veränderung geschützt werden sollen.

Abhängig von der Risikobewertung einzelner Bereiche hinsichtlich Datenschutz und Informationssicherheit kann vom laut Geschäftsordnung zuständigen Rektoratsmitglied für den Zugriff auf Daten dieser Bereiche eine Zweifaktor-Authentifizierung verpflichtend vorgeschrieben werden.

4.1 BEGRIFFSBESTIMMUNGEN

Im Kontext dieses Dokuments werden Begriffe wie folgt definiert:

Account
Unter einem Account, auch als (Benutzer_innen-)Konto bezeichnet, wird eine Kombination aus einer Benutzer_innen-ID und einem Passwort verstanden. Diese beiden Elemente bilden die sogenannten Zugangsdaten. Ein Account stellt eine Zugriffsberechtigung zu einem geschützten IT-System dar.

Die Begriffe Konto, Benutzerkonto, Zugriffsberechtigung oder User Credentials werden als Synonyme für Account verwendet.

Benutzer_innen-ID
Als Benutzer_innen-ID wird eine Zeichenfolge aus Buchstaben, Ziffern und/oder Sonderzeichen bezeichnet, die eine eindeutige Zuordnung zu einem Berechtigungsprofil darstellt und somit personenbezogen ist.

Die Begriffe Username, Benutzer_innenname oder User-ID werden als Synonyme für Benutzer_innen-ID verwendet.

Passwort
Als Passwort wird eine Zeichenfolge aus Buchstaben, Ziffern und/oder Sonderzeichen bezeichnet, die die Überprüfung einer Identität möglich macht.

Die Begriffe Kennwort, Schlüsselwort oder Password werden als Synonyme für Passwort verwendet.

Funktionsbenutzer_innen-ID
Eine Funktionsbenutzer_innen-ID darf im Gegensatz zu personenbezogenen Benutzer_innen-IDs von mehreren Personen verwendet werden.

Initial-Passwort
Als Initial-Passwort wird ein Passwort bezeichnet, das erstmalig für den Account gesetzt wird.

4.2 REGELUNGEN BEZÜGLICH DER WAHL VON PASSWÖRTERN

Die unten angeführten Anforderungen sind bestmöglich, im Rahmen der technischen Möglichkeiten auf allen IT- und Telekommunikationssystemen der TU Wien umzusetzen.

Passwörter müssen folgenden Mindestanforderungen entsprechen:

- Die minimale Passwortlänge beträgt acht Zeichen. Die Komplexitätserfordernisse werden in der anschließenden Liste beschrieben.
- Nach drei falschen Passworteingaben wird das Konto für zehn Minuten gesperrt.
- Zur Rücksetzung des Passworts oder zur Aufhebung der Kontosperre kann die Handy-Signatur verwendet, mit entsprechender Identitätsfeststellung der Helpdesk kontaktiert, das Service Center der TU.it aufgesucht oder der_die zuständige Adressmanager_in kontaktiert werden.
- Das selbe Passwort darf nicht bei verschiedenen Dienstleistern verwendet werden.
- Dienstlich genutze Passwörter dürfen nicht für private Zwecke (z.B. zum Chatten in einem Internet-Cafe) verwendet werden.
- Sensible Passwörter sollen in regelmäßigen Abständen geändert werden.

Komplexitätserfordernisse:

- Das Passwort muss aus einer Mischung von Buchstaben und Ziffern oder Satz- bzw. Sonderzeichen bestehen.
- Bei den Buchstaben von Passwörtern soll eine Kombination von Groß- und Kleinschreibung verwendet werden.

- Passwörter dürfen keinesfalls den Benutzer_innennamen (Benutzer_innen-ID) oder einen anderen Namen (wie z.B. Vor- oder Nachname) oder Informationen, die in unmittelbarem Zusammenhang mit dem_der Benutzer_in stehen, wie Geburtstag, Telefonnummer, Sozialversicherungsnummer, Ausweisnummer, Autonummer, Hausnummer, Wohnort, Straße usw. beinhalten.
- Es dürfen keine Buchstabenfolgen von der Tastatur wie "qwertz" oder ähnliches verwendet werden.
- Das Passwort darf keinen Begriff bilden, der in einem gängigen Wörterbuch (auch Fremdsprachen) enthalten ist.
- Passwörter müssen so gewählt werden, dass sie sich signifikant von anderen eigenen Passwörtern unterscheiden.
- In IT-Systemen in denen das Verwenden eines komplexen Passwortes nicht möglich ist, ist ein Passwort zu wählen, das sich möglichst nahe an ein komplexes Passwort anlehnt.

Vorschlag für die Erstellung von Passwörtern:

- Passwörter sollten aus den Anfangsbuchstaben eines Merksatzes gebildet werden. Beispiel: !1Pw=ig! (Merkregel: !Ein Passwort ist immer geheim!)
- Ein Passwort sollte so beschaffen sein, dass es schnell eingegeben und dabei von anderen Personen nicht erfasst werden kann.

Die oben stehenden Regelungen werden durch Empfehlungen auf der Homepage der TU.it (Bereich IT-Sicherheit) ergänzt, um die Umsetzung der Vorgaben zu erleichtern (z.B. mittels Tipps zur Findung sicherer Passwörter).

4.3 GEBRAUCH VON PASSWÖRTERN

- Passwörter sind von dem_der Inhaber_in geheim zu halten und dürfen nicht weitergegeben werden. Auf eine unbeobachtete Eingabe des Passworts ist zu achten.
- Passwörter dürfen nicht ungesichert über das Netzwerk (z.B. per E-Mail oder Chat) übertragen oder schriftlich festgehalten werden.

- Passwörter dürfen nicht auf Papier (z.B. Post-it) aufgezeichnet oder im Klartext und somit unverschlüsselt gespeichert werden (z.B. Textdatei oder mobiles Endgerät).
- Passwörter, von denen angenommen werden muss, dass sie Unberechtigten bekannt geworden sein könnten oder sind, müssen von dem_der berechtigten Benutzer_in umgehend geändert werden bzw. muss von diesem_r eine Passwortrücksetzung veranlasst werden.
- Wenn ein Passwort zurückgesetzt werden soll, ist durch eine Identitätsprüfung sicherzustellen, dass der_die Antragsteller_in auch der_die rechtmäßige Account-Inhaber_in ist.
- Die Weitergabe von Passwörtern von Funktionsbenutzer_innen darf nur durch die für die jeweilige Funktionsbenutzer_innen-ID verantwortliche Person erfolgen und nur an Personen, die das Passwort für die Erfüllung ihrer Aufgaben an der TU Wien benötigen.
- Passwörter für Funktionsbenutzer_innen-IDs müssen den gleichen Regeln gehorchen wie jene für Standardbenutzer_innen. Sie dürfen nur von der für die jeweilige ID verantwortlichen Person geändert werden. Bei Ausscheiden einer Person aus der von der ID umfassten Gruppe ist das Passwort umgehend zu ändern.
- Initial-Passwörter sind bei der ersten Anmeldung entsprechend den Minimal-anforderungen zu ändern.
- Werkseitig voreingestellte Passwörter sind umgehend, entsprechend den Minimal-anforderungen zu ändern.
- Zusätzliche Regelungen können, abhängig von der jeweiligen Situation, dann getroffen werden, wenn dies aus Risikogesichtspunkten notwendig erscheint.

4.4 VERGABE VON INITIAL-PASSWÖRTERN

Die Wahl von Initial-Passwörtern muss zumindest den Minimalanforderungen entsprechen (siehe 4.2 Regelungen bezüglich der Wahl von Passwörtern).

Initial-Passwörter müssen nach dem Zufallsprinzip individuell vergeben werden und sollen – so technisch umsetzbar - eine begrenzte Gültigkeitsdauer haben.

5 RICHTLINIE FÜR DIE SPEICHERUNG PERSONENBEZOGENER DATEN

5.1 BEGRIFFSBESTIMMUNGEN

Personenbezogene Daten

"Personenbezogene Daten“ sind Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist. Dabei ist es unerheblich, ob private, berufliche, wirtschaftliche Informationen, Eigenschaften, Kenntnisse oder physiologische Merkmale betroffen sind. Personenbezogene Daten sind daher z.B.: Name, Geburtsdatum, Adresse, Geschlecht, Einkommen, Vermögen, Lebensstil, Intelligenzquotient, Umsatz, Beschäftigtenzahl, Gewinn, Angaben zur Bonität sowie auch Bild, Stimme, Fingerabdrücke oder genetische Daten, also alle Daten die es ermöglichen, eine Person zu identifizieren.

IT-geschützte Speicherung personenbezogener Daten

Personenbezogene Daten sind in IT-Systemen so zu speichern, dass die zugrundeliegenden Speichermedien, auf denen die eigentliche technische Speicherung erfolgt, verschlüsselt sind. Damit soll gewährleistet werden, dass auch wenn das Speichermedium einem nicht autorisierten Zugriff ausgesetzt ist, auf die Daten nicht zugegriffen werden kann. Hierzu sind dem Stand der Technik entsprechende, geeignete Verschlüsselungsmaßnahmen einzusetzen.

5.2 MOBILE GERÄTE

Da mobile Geräte einem höheren Verlust- oder Diebstahlsrisiko ausgesetzt sind, ist für die Speicherung personenbezogener Daten eine Verschlüsselung des jeweiligen Endgeräts unbedingt erforderlich.[8]

[8] Hinweis: Die TU.it bietet mit dem Notebook-Service Notebooks an, die bereits mit verschlüsselten Festplatten ausgeliefert werden (https://iu.zid.tuwien.ac.at/15380645.asHTML).

5.3 DESKTOP-GERÄTE

Die Speicherung von personenbezogenen Daten direkt auf Desktop-Rechnern ist zu vermeiden. Für die Speicherung der Daten sind Netzwerklaufwerke einzusetzen, die die Daten auf verschlüsselten Datenträgern speichern.[9]

5.4 SYNC- UND SHARE-LÖSUNGEN

Bei Sync- und Share-Diensten handelt es sich um Cloud-Services. Es gelten die in der Cloud-Richtlinie festgelegten Regelungen.

Die TU.it stellt mit den Services TUownCloud und TUproCloud ein TU-eigenes Cloud-Service (Private Cloud) zur Verfügung. Die Daten werden in den Datacentern der TU Wien auf verschlüsselten Festplatten gespeichert.

Von den Nutzenden ist durch entsprechende Einstellungen am Client dafür zu sorgen, dass personenbezogene Daten nicht automatisch auf alle Endgeräte synchronisiert werden. Die Einstellungen sind selektiv so vorzunehmen, dass die Daten nur auf Endgeräte, die grundsätzlich für die Speicherung von personenbezogenen Daten geeignet sind, synchronisiert werden.

5.5 ENTSORGUNG UND SPEICHERMEDIEN

Speichermedien, die personenbezogene Daten enthalten, sind nachvollziehbar gesichert zu vernichten.[10]

[9] Hinweis: TU.it stellt mit dem Service TUfiles ein Netzwerklaufwerk zur Verfügung. Die Daten werden in den Datacentern sicher auf verschlüsselten Festplatten gespeichert (https://www.it.tuwien.ac.at/tufiles/).
[10] Hinweis: TU.it bietet hierzu das Service TUdiskShredder an, mit dem Festplatten, SSDs und Magnetbänder sicher vernichtet werden können (https://www.it.tuwien.ac.at/tudiskshredder/).