Handbuch zu technischen und organisatorischen Maßnahmen zum Datenschutz an der HTU Wien

Grundlagen

Rechtliche Regelungen

Das Recht auf Datenschutz ist ein Grundrecht und genießt damit umfangreichen Schutz.

Das Recht auf Datenschutz ist in der EU und in Österreich durch diverse Rechtsnormen geregelt, allen voran die Datenschutz Grundverordnung (DSGVO) auch bekannt unter dem englischen Titel General Data Protection Direcitve (GDPR)[1]. Die DSGVO hat in allen EU Mitgliedsstaten rechtlich bindenden Charakter und muss nich in nationales Recht umgesetzt werden (Im Unterschied zu einer EU-Richtline), es gibt jedoch Gesetze die die Umsetzung der DSGVO genauer spezifizieren, insbesondere in Österreich das Datenschutzgesetz [2].

Die DSGVO gilt für alle Datenverarbeitungen die nicht rein persönlichen oder Familiären Zweck haben.

Begriffsbestimmungen

- Betroffene_r
  Lebendige, natürliche Person deren Daten gespeichert werden.
- Verantwortliche_r
  Person oder Organisation die die Daten kontrolliert und über deren Verwendung entscheidet.
- Auftragsdatenverarbeiter_in
  Person oder Organisation die im Auftrag eines Verantwortlichen Daten Verarbeitet, jedoch nicht selbst über die Verwendung entscheidet. Es muss vertraglich und schriftlich festgelegt werden wie die Daten verarbeitet werden.
- Weitere Empfänger_in
  Weitere Personen oder Organisationen die die Daten erhalten, die jedoch keine Auftragsverarbeiter_innen sind, diese Personen oder Organisationen sind dann wieder selbst Verantwortliche.
- Personenbezogene Daten
  "Personenbezogene Daten“ sind Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist. Es sind alle Daten, die es ermöglichen, eine Person zu bestimmen. z.B. Matrikelnummer, Name, Geburtsdatum, Adresse, Geschlecht, Einkommen.
- Besonders schützenswerte Daten
  Besonders schützenswerte Daten laut Art. 9 DSGVO [1] sind: personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Weiters sind Daten aus denen auf die soziale oder finanzielle Lage oder Arbeitsverhältnisse schließen lassen im Sinne

dieses Handbuchs besonders schützenswert.

Grundsätze

Unter welchen Vorraussetzungen dürfen Daten verarbeitet werden?

Daten dürfen unter folgenden Vorraussetzungen verarbeitet werden:

- Einwilligung der Betroffenen
- Wenn die Verarbeitung zur Erfüllung eines Vertrages notwendig ist
- Wenn die Verarbeitung zur Erfüllung einer rechtlichen Pflicht notwendig ist
  Insbesondere also Plichten die im HSG [3] geregelt sind:
  - Für Referate der HTU
    - § 17 (1) HSG Vertretung der Interessen ihrer Mitglieder für den Bereich der jeweiligen Bildungseinrichtung sowie deren Förderung, soweit sie nicht in den Wirkungsbereich anderer Organe der Hochschülerinnen- und Hochschülerschaft fallen;
    - § 17 (10) HSG Beratung der Studienwerberinnen und Studienwerber sowie der Studierenden.
  - Für Faktultätsvertretungen
    - § 18 (1) HSG Vertretung der Interessen der Studierenden sowie deren Förderung in ihrem Wirkungsbereich
  - Für Studienvertretungen
    - § 20 (1) HSG Vertretung der Interessen der Studierenden sowie deren Förderung in ihrem Wirkungsbereich
    - § 20 (5) HSG Beratung der Studienwerberinnen und Studienwerber sowie der Studierenden.
- Lebenswichtige Interessen Betroffener Personen
- Wahrunge berechtigten Interesses (Z.b. offene Forderungen)

Betroffenenrechte

Abschnitt 2 der DSGVO [1] garantiert Betroffenen folgende Rechte:

- Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person
- Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden
- Auskunftsrecht
- Recht auf Berichtigung
- Recht auf Löschung (“Recht auf Vergessenwerden”)
- Recht auf Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit
- Widerspruchsrecht
- Recht keiner automatisierten Entscheidung unterworfen zu werden

Welche Grundsätze sind bei der Verarbeitung Personenbezogener Daten anzuwenden?

- Rechtmäßigkeit, Transparenz
  Personenbezogene Daten dürfen nur auf rechtmäßige, in für die Betroffenen

nachvollziehbarer Weise verarbeitet werden. Für die Betroffenen müssen insbesondere folgende Informationen leicht zugänglich sein:
  - Identität des Verantwortlichen
  - Zweck der Verarbeitung
  - Information darüber welche Daten verarbeitet werden
- Zweckbindung
  Daten dürfen nur für den Zweck für den sie erhoben wurden verwendet werden.
- Datenminimierung / Datensparsamkeit
  Es sind prinzipiell nur Daten zu erheben und zu verarbeiten die für den Zweck notwendig sind.
- Richtigkeit
  Die Richtigkeit der Daten hat sichergestellt zu sein.
- Speicherbegrenzung
  Speicherung der Daten sollte Zeitlich begrenzt sein.
- Vertraulichkeit
  Durch technische und organisatorische Maßnahmen muss sicher gestellt werden, dass nur befugte Personen Zugriff auf die Daten haben

Technische und organisatorische Maßnahmen zum Datenschutz

Organisatorische Maßnahmen

Klassifikation von Datenarten

Zur geneueren beschreibung von Organisatorischen Maßnahmen sowie zur Beurteilung notwendiger Schutzmaßnahmen ist die klassifikation von Daten in bestimmet Datenarten nützlich, wir nehmen hier folgende Klassifikationen vor:

Strukturiert / Unstrukturiert

Strukturierte Daten sind Daten die in einer definierten Struktur gespeichert sind, insbesondere in Form von Tabellen oder standardisierten Formularen. Unstrukturierte Daten sind zum Beispiel Korrespondenz oder Notizen.

Digital / Analog gespeichert

Sind die Daten digtial (z.B. Excel, Word, .pdf, etc. - Files) oder analog (z.B. ausgedruckte Formulare, handgeschriebene Listen, usw.) gespeichert.

Wer hat Zugriff auf welche Daten?

Eine wichtige organisatorische Maßnahme zur Datensicherheit ist den Kreis der Personen die Zugriff auf Persönliche Daten haben auf die Personen einzuschränken die tatsächlich Zugriff brauchen um die Aufgaben zu erfüllen und zu erheben wer auf welche Daten Zugriff hat.

Data Breach Notification

Sollte die Möglichkeit bestehen, dass persönliche Daten für nicht befugte Personen zugänglich geworden sind (Verlust eines Datenträgers oder Mobilgerätes,

technischer Defekt, ...) so sind unverzüglich der/die Datenschutzbeauftragte und der Vorsitz zu verständigen.

Technische Maßnahmen

Kein versenden Personenbezogener Daten per Mail

Personenbezogene Daten sind prinzipiell nich per Mail zu versenden. Die Übertragung der Daten per Mail erfolgt unverschlüsselt, außerdem besteht die Gefahr, dass durch falsch adressierte Mails Daten für nicht autorisierte Personen zugänglich werden.

In folgenden Fällen ist ein Versandt per Mail zulässig:

- Interne Weiterleitung von Daten die von den Betroffenen selbst per Mail geschickt wurden.
- Benützung starker Verschlüsselung und versandt des Schlüssels auf anderem Weg. (Zum Beispiel gnupg mit vorher ausgetauschtem public key, oder 7zip [4] Verschlüsseltes Archiv und weitergabe des Passwortes telephonisch.)

Mitarbeiter_innen der Referate haben Zugriff auf die HTU-Nextcloud, diese ist für den Austausch personenbezogener Daten zu verwenden. Für internen Austausch kann eine Datei oder ein Ordner direkt mit einem anderen HTU-Account geteilt werden, beim Teilen mittels Links sind Passwort und Ablaufdatum zu setzen.

Keine Weiterleitung an andere Mail Anbieter

Prinzipiell ist eine Weiterleitung aller eingehenden Mails an andere Mail-Anbieter nicht zulässig. Mail sollten über Fachschafts oder HTU Server abgerufen oder über die Webmail-Systeme gelesen und bearbeitet werden.

Sicherung von Geräten

Geräte der HTU sowie Privatgeräte die zur Verarbeitung von personenbezogenen Daten benützt werden müssen ausreichend geschützt sein. Zumindest muss der Zugriff durch ein starkes Passwort geschützt sein und die Daten müssen verschlüsselt gespeichert sein. Siehe dazu folgende Anleitung [4].

Sichere Entsorgung

Datenträger, ob analog oder digital die zur Speicherung personenbezogener Daten verwendet wurden müssen sicher entsorgt werden. Es gibt dafür ein Service der TU das auch die HTU nützen kann.

Passwörter

Passwörter sind ausreichend lange und komplex zu wählen, es empfiehlt sich die Anwendung eines Passwort Managers, siehe dazu folgende Anleitung [5].

Beipsiele

Beratung von Studierenden

Bei Organisations-Mail-Adressen die von mehreren Mitarbeiter_innen empfangen werden, sollten die Sender_innen darüber aufgeklärt werden, an welchen Personenkreis sie schreiben. Ein Einfacher Satz an Stellen an denen ihr die Mail-Adresse bekannt gebt reicht dazu aus. Einen entsprechenden Textbaustein findet ihr im Abschnitt Textbausteine.

Empfänger_innen der Mails müssen darüber aufgeklärt werden, dass sie persönliche Daten die über die Adresse empfangen werden persönlich zu behandeln sind und welche technischen und organisatorischen Maßnahmen zum Schutz der Daten anzuwenden sind.

Teilnehmer_innen-Listen

Solltet ihr Teilnehmer_innen-Listen für Veranstaltungen, Seminare, etc. oder ähnliches führen muss es eine Einwilligung geben, da die Verarbeitung dieser Daten (meistens) nicht auf einer gesetzlichen Grundlage basiert. Einen entsprechenden Textbaustein findet ihr im Abschnitt Textbausteine. Bitte beachtet dabei, dass dieses Muster nicht irgendwo versteckt aufliegen kann, sondern im selben Medium präsentiert werden muss.

Wenn die Daten zum Beispiel auf einer Papier-Liste erhoben werden, reicht es *nicht* aus die Einverständniserklärung auf der Website zu veröffentlichen. Druckt die Einverständniserklärung auf die Rückseite oder legt sie bei und weist auf der Vorderseite des Formulars in einer Fußnote darauf hin.

Socialmedia

Bei Socialmedia Auftritten speichern die Plattformen Daten über die Besucher_innen eures Auftrittes. Die Besucher_innen eures Socialmediaauftrittes sind darüber zu informieren, am besten mittels Link auf eine entsprechende Datenschutzerklärung in der Seiten Beschreibung oder ähnlichem. (Facebook Seiten Beschreibung, twitter-bio, ...) Einen Textbaustein dafür findet ihr ebenfalls im Abschnitt Textbausteine.

Newsletter

Bei Newslettern in die sich Abonnent_innen selbstständig eintragen müssen diese auch der dazu notwendigen Datenverarbeitung zustimmen. Bei Papier-Listen druckt den entpsrechenden Text so wie bei Teilnehmer_innen Listen auf das entsprechende Blatt, bei einer Online Anmeldung verlinkt die Erklärung und holt euch die Zutsimmung über ein entsprechend zu setzendes Häckhen. Auch hierzu gibt es einen Textbaustein.

Updates

Alle die im Rahmen ihrer Tätigkeit an der HTU persönliche Daten verarbeiten sind angehalten sich über Änderungen dieses Hanbuches, insbesondere der technischen und organisatorischen Maßnahmen zur Datensicherheit zu informieren. Größere Änderungen werden über die Fachschaften und Referate Mailverteiler

ausgeschickt, eine aktuelle Version dieses Dokuments ist auf der HTU-Website zu finden.

Anhänge

Textbausteine

Mailverteiler Beratung

Mails an diese Adresse werden von Studierendenvertreter_innen sowie weitere ehrenamtlichen Mitarbeiter_innen der <Fachschaft/...> gelesen und verarbeitet.

Social Media

Beim Besuch unsers <Plattform>-Aufrtittes erhebt <Plattform> persönliche Daten und macht diese der <Fachschaft/...> teilweise zugänglich, zu genaueren Infos welche Daten erhoben werden und entsprechenden Widerspruchsrechten siehe: <Link auf Datenschutzerklärung der Plattform>

Websites

Beim Besuch von <website> werden folgende Daten aus technischen Gründen und zu statistischen Zwecken erhoben: <Aufzählung>

Newsletter

Ich stimme der zum Versandt dieses Newsletters notwendigen Verarbeitung meiner personenbezogenen Daten (<e-mail Adresse, ggf. Name>) zu.

Anmeldelisten

Ich stimme der Verarbeitung der hier angegebenen Daten zum Zwecke der Abhaltung <Veranstaltung> zu.

Anleitungen

Festplattenverschlüsselung

Windows

In Windows kann Full-Disk Encryption wie folgt aktiviert werden:

1. Systemeinstellungen öffnen und BitLocker-Laufwerksverschlüsselung auswählen
2. Das Laufwerk auswählen und BitLocker aktivieren
3. Den Wiederherstellungsschlüssel drucken und an einem sicheren Ort verwahren
4. Gesamtes Laufwerk verschlüsseln auswählen
5. BitLocker-Systemprüfung auswählen, sollte die Überprüfung scheitern einfach noch einmal die obrigen Schitte ohne diese Auswahl wiederholen.

Achtung die Verschlüsselung läuft zwar im Hintergrund braucht aber Zeit, also nicht ausführen kurz bevor man den Rechner abschlaten muss, insbesondere bei Laptops.

Linux

Festplatten-Verschlüsselung ist in den Meisten Linux Distributionen mit graphischer Installation gleich bei der Installation eine Option, einfach bei der Installation auswählen.

Einen guten Überblick über Full Disk Encryption sowie Installations-Anleitungen, die sich auf alle anderen Linux-Distributionen übertragen lassen bietet das Arch Wiki [5]

Ordner-Verschlüsselung

Windows 10:

1. Rechtsclick auf den Ordner der verschlüsselt werden soll
2. Dann auf Allgemein > Erweitert
3. Inhalt verschlüsseln auswählen, angeben, dass auch alle untergeordneten Odner verschlüsselt werden sollen.

Die Verschlüsselung ist im Windows-Benutzerkonto gespeichert, wenn man bei Windows angemledet ist muss man also kein weiteres Passwort eingeben, der Zugriff ist jedoch auch nur mit diesem Benutzerkonto möglich.

Passwort Manager

Als Passwort-Manager bietet sich KeePass an. Hier werden die Passwörter in einer standardisierten Passwortdatenbank gespeichert die von KeePass und anderen Programmen geöffnet werden kann.

KeePass kann hier heruntergeladen werden, bzw. bei den meisten Linux-Distributionen über den Paketmanager installiert werden.

Für Android gibt es die App KeePass-Offline im offiziellen Google Store sowie KeePass im F-Droid store.

KeePass Dateien können dann z.b. als Dateien synchronisiert werden, wenn das Handy als Laufwerk angeschlossen ist.

Referenzen

[1] Europäisches Parlament, "REGULATION (eu) 2016/679 of the european parliament and of the council (gdpr)." https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679, 2016.

[2] Österreichischer Nationalrat, "Bundesgesetz zum schutz natürlicher personen bei der verarbeitung personenbezogener daten (datenschutzgesetz – dsg)." https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597, 1999.

[3] Österreichischer Nationalrat, "Bundesgesetz über die vertretung der studierenden (hochschülerinnen- und hochschülerschaftsgesetz 2014 – hsg 2014)."

https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20008892, 2014.

[4] Pavlov, Igor, "7zip." https://www.7-zip.org/.

[5] Arch Wiki Contributors, "Arch wiki: Dm-crypt/encrypting an entire system." https://wiki.archlinux.org/index.php/Dm-crypt/Encrypting_an_entire_system, 2018.