Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Hochschulversammlung

ETH Zürich
Prof. Dr. Dr. Dagmar Iber
Präsidentin
Mattenstrasse 26, BSD G 204.2
4058 Basel

Telefon +41 61 387 32 10
dagmar.iber@bsse.ethz.ch

ETH Zürich
Informatikdienste
Domenico Salvati
OCT G 51.1
Binzmühlestrasse 130
8092 Zürich

Zürich, 21. Mai 2024

Stellungnahme der Hochschulversammlung zur ETH-internen Vernehmlassung «Weisung Informationssicherheit und Benutzungsordnung für IT-Mittel an der ETH Zürich – Totalrevision»

Sehr geehrter Herr Salvati

Die Hochschulversammlung (HV) bedankt sich für die Möglichkeit sich äussern zu können im Rahmen der internen Vernehmlassung «Weisung Informationssicherheit und Benutzungsordnung für IT-Mittel an der ETH Zürich – Totalrevision».

Bitte finden Sie die Stellungnahme der Hochschulversammlung unten angefügt.

Freundliche Grüsse

Prof. Dr. Dr. Dagmar Iber
Präsidentin Hochschulversammlung

Beilage(n)
Antwort der Hochschulversammlung auf die interne Vernehmlassung

Antwort der Hochschulversammlung zur Vernehmlassung über die Weisung zur Informationssicherheit an der ETH Zürich RSETHZ 203.25: Totalrevision und die Benutzungsordnung für IT-Mittel an der ETH Zürich, RSETHZ 201.25: Totalrevision

Sehr geehrter Domenico Salvati

Mit dem Schreiben vom 16. Februar 2024 hat uns die Generalsekretärin zur Vernehmlassung "Weisung Informationssicherheit und Benutzungsordnung für IT-Mittel an der ETH Zürich - Totalrevision" der ETH Zürich eingeladen. Die Hochschulversammlung (HV) bedankt sich für die Einladung zur Vernehmlassung und äussert sich dazu folgendermassen:

Allgemeine Bemerkungen

Wir bedanken uns für die Möglichkeit zur Stellungnahme zu den obengenannten Dokumenten. Grundsätzlich begrüssen wir beide Totalrevisionen und erachten die Änderungen als notwendig.

Die HV begrüsst den vorbildlich organisierten Vernehmlassungsprozess. Auch dass wir in der vorbereitenden Kommission Einsitz erhielten, zeugt von einem ausgeprägten Verständnis der Mitwirkungsprozesse. Uns ist wichtig zu betonen, dass wir den Prozess der partizipativen Erarbeitung dieser Totalrevision sehr schätzen, insbesondere das Sounding-Board sowie die öffentlichen Zoom-Meetings, an welchen Fragen geklärt werden konnten, erwiesen sich als sehr hilfreich.

Da die Weisung und Verordnung auf bestehenden Gesetzestexten beruhen, führt die Interpretation für Nicht-Jurist*innen zu verschiedenen Missverständnissen. Dies wurde auch an den Online-Meetings klar. Deshalb erscheint es der HV hilfreich, der Weisung sowie der Verordnung eine Interpretationshilfe mit Beispielen beizufügen. Insbesondere sollten folgende Punkte, welche im Gespräch geklärt wurden aber von der Allgemeinheit tendenziell missverstanden oder falsch interpretiert werden, erklärt werden:

Detailbemerkungen zu BOT

Was gilt konkret für private Geräte, für die nun ETH-Angehörige als Systemverantwortliche gelten, insb. mit BYOD-Pflicht ab nächstem Semester? Ist man als Nutzer*in bei einem privaten Gerät, DV? Was bedeutet das konkret? Heisst das, dass man die sicherheitsrelevanten Patches installieren soll?

Art. 4, Abs. 3: Wie soll man das Einverständnis einholen? Es ist noch unklar, inwiefern dies geschehen soll. Was sind die Konsequenzen, wenn man keine Bewilligung einholt für den Versand privater Mails?

Artikel 6, Absatz 5: Gelten die Regeln zum Massenversand auch für ETH-nahe Organisationen wie AVETH und VSETH? Die 500er-Limite ist mit Exchange Online nicht mehr aktuell. Zudem ist nicht klar, inwiefern dies für E-Mails solcher Organisationen zutrifft und sollte daher präzisiert werden, da diese Versände automatisch mit der Mitgliedschaft zusammenhängen und mehr als 500 Adressat*innen erreichen.

Art. 8: Was macht man mit unbeaufsichtigten Messsystemen und Steuerungssystemen? Dies ist nicht möglich bei Experimenten, die länger laufen. Hier sollte ein Verweis auf "sofern nicht für den Betrieb erforderlich" angebracht werden. Zumindest im Begleitschreiben sollte dieser Punkt noch präzisiert werden.

Artikel 10: Dieser Artikel ist sehr strikt formuliert und die Konsequenzen drastisch. Was bedeutet das genau?

Art. 11, Abs. 2: Hier wäre in einem ersten Schritt der/die ISG oder Systemverantwortliche zu informieren, da diese beurteilen können, ob dies aus betrieblicher Sicht machbar ist.

Artikel 13: Klingt allgemein “drastisch” für Studierende, die eigentlich kein Anstellungsverhältnis an der ETH haben. Ein in einfacher Sprache verfasster, spezifisch für Studierende erstellter Leitfaden wäre sinnvoll. Für viele ETH-Angehörige klingt es nach einer Möglichkeit, in die Massenüberwachung hineinzugleiten, auch wenn dies, gemäss Fragestunde, nicht die Absicht ist. Spezifisch geht es um folgendes: Der Artikel soll festlegen, welche Personendaten, die sich aus der Nutzung oder dem Betrieb der Informatikmittel der ETH ergeben, gespeichert und verwertet werden können. An der Fragestundewurde erwähnt, dass dieser Abschnitt vom Rechtsdienst aus Transparenzgründen hinzugefügt wurde, um der Tatsache Rechnung zu tragen, dass Art. 57L RVOG und Art. 4 VBNIB bereits für ETH-Angestellte gelten. Unseres Erachtens gibt das vorgeschlagene BOT die genannten Artikel jedoch nicht korrekt wieder: Art. 13 erlaubt es der ETH, alle Personendaten, die sich aus der Nutzung oder dem Betrieb der IT-Ressourcen der ETH ergeben, zur Kontrolle der individuellen Arbeitszeiten zu verwenden (Abs. 3c). Art. 57L RVOG legt jedoch klar fest, welche Daten mit welchen Zielvorgaben gespeichert werden dürfen. Daten aus der Nutzung oder dem Betrieb von Informatikmitteln können für fünf Ziele verwendet werden, von denen keines mit der Steuerung der Arbeitszeit zusammenhängt. Für die Bewirtschaftung der Arbeitszeiten können nur Daten über die Arbeitszeiten (z.B. wie sie in ETHIS eingegeben werden) verwendet werden. Alle folgenden Artikel (wie z.B. Art. 57O RVOG und Art. 4 VBNIB) scheinen nur näher darauf einzugehen, was mit den bereits gespeicherten Daten im Rahmen der in Art. 57L RVOG, passieren darf. Nach unserem Verständnis des RVOG scheint es daher, dass das vorgeschlagene BOT viel mehr Spielraum für die Kontrolle der individuellen Arbeitszeit lässt, als der Bund erlaubt.
Es wäre uns deshalb sehr wichtig, dass dies in einem Begleitschreiben noch geklärt wird.

Detailbemerkungen Weisung zur Informationssicherheit

Wir schätzen die Bemühungen zur Totalrevision sehr und bedanken uns für die Möglichkeit zur Stellungnahme. Aus Sicht der Hochschulversammlung haben wir keine Anmerkungen.

Schlussbemerkungen

Wir möchten noch auf Artificial Intelligence (AI) sowie deren Anwendungen wie Chat-GPT, DeepL usw. eingehen: Wie werden die Risiken (allgemein) sowie die Anwendungen spezifisch geregelt? Insbesondere die Verwendung von externen cloudbasierten Services sollte angesprochen werden.

Die Informationssicherheit wird vermehrt über Werkzeuge wie 2-Faktor-Authentifizierung, welche vielfach auf BYOD-Geräten (persönliche Mobiltelefone) installiert sind, erreicht. Um einen Anreiz zu schaffen, dies ganzheitlich umzusetzen, wünscht sich die HV einen CMN-Vertrag für alle Angestellten der ETH Zürich.