

Antrag: Die Website und Kommunikation des AStA datenschutzkonform gestalten.

Antragssteller: Hartmut Phieler

Datum: 04.04.2025

Liebe StuPa-Abgeordnete,

bereits im November 2024 habe ich den AStA per Formular darauf aufmerksam gemacht, dass auf der Website a) Cookies erfasst werden ohne Zustimmung und b) eine Datenschutzerklärung fehlt. Zur Behebung hatte ich eine Frist von 1 Monat genannt, die am 15. Dezember 2024 endete. Innerhalb dieser Zeit wurde die Website angepasst, sodass keine Cookies mehr gesetzt werden und Punkt b) damit behoben wurde. Allerdings ist dem AStA seit spätestens 16. November 2024 über die fehlende Datenschutzerklärung informiert.

Dieser Missstand wurde bisher weder behoben, noch habe ich dazu eine Antwort vom AStA erhalten. Ich bitte Euch daher, in Eurer Kontrollfunktion tätig zu werden.

Das StuPa der Uni Potsdam weist den AStA an, die folgenden Sachverhalte zu lösen:

1. Die Website des Allgemeinen Studierendenausschuss (<https://astaup.de/>) verfügt seit Monaten über keinerlei Datenschutzerklärung, obwohl dort z.B. Daten per Kontaktformular eingegeben werden können.

Die Einwilligung zur Weiterverarbeitung der Daten wird nur mit folgender Erklärung erfasst: „Ich bin damit einverstanden, dass meine angegebenen personenbezogenen Daten zum Zweck der Bearbeitung meiner Anfrage gemäß der Datenschutz-Grundverordnung (DSGVO) verarbeitet und gespeichert werden.“

Hinweise zu den Verlinkungen zu Instagram und Whatsapp fehlen, sowohl Informationen zu IP-Adresse, User-Agent, etc. – Außerdem wird nicht auf die Rechte der Nutzer*innen verwiesen.

Forderung: Die Website des AStA ist schnellstmöglich mit einer gültigen und aussagekräftigen Datenschutzerklärung zu versehen.

Um weitere Verzögerungen zu vermeiden, ist eine Frist von 1 Monat nach Behandlung des Antrags einzuhalten.

2. Neben der Website des AStA (<https://astaup.de/>) und der allgemeinen Email info@astaup.de bestehen nur die Möglichkeiten Instagram und Whatsapp um mit dem AStA in Kontakt zu treten bzw. an Informationen wie Stellungnahmen zu kommen, die dort z.T. exklusiv veröffentlicht wurden (z.B. Statements zur aktuellen Lage in den letzten Monaten). Ohne ein Konto bei diesen Diensten ist es nicht möglich, darauf zuzugreifen.

Problematisch ist hieran die alleinige Abhängigkeit von Diensten der Meta Platforms, Inc. Studierende, die solche Diensten etwa aus Gründen des Datenschutzes oder inkompatiblen Geräten nicht nutzen können oder wollen, sind dadurch ausgeschlossen.

Kontinuierliche Probleme beim Datenschutz

Dienste und Apps von Meta weisen immer wieder erhebliche Schwächen und unlautere Praktiken beim Datenschutz auf [1]. Durch die Nutzung dieser Dienste besteht also stets das Risiko von Sicherheitslücken und Datenschutzpannen. Aktuell zeigt sich das z.B. in der aktuellen KI-Funktion bei Meta, die nicht aktiviert, sondern nur stummgeschaltet werden kann [2].

Warum das so problematisch ist, schreibt Mike Kuketz:

„Meta hat begonnen, KI-Assistenten in WhatsApp, Instagram und den Facebook Messenger zu integrieren – ohne den Nutzern eine Möglichkeit zur Deaktivierung zu geben. Besonders problematisch ist dabei, dass jede Interaktion mit der KI nicht nur die eigenen Nachrichten offenlegt, sondern Meta auch erlaubt, diese Daten zu speichern und für das Training der KI zu nutzen. Die Beta-Version treibt dies noch weiter: Sobald der Assistent geöffnet wird, beginnt er automatisch mitzuhören, verarbeitet die Sprachdaten in der Cloud und überträgt sie auf die Meta-Server. Damit unterliegt die Datenverarbeitung nicht mehr der Kontrolle der Nutzer, sondern den Zugriffsmöglichkeiten von Meta – und letztlich auch der US-Regierung.

Das zentrale Problem dabei: Die oft angeführte Ende-zu-Ende-Verschlüsselung, mit der WhatsApp vermeintlichen Datenschutz suggeriert, greift in diesen Fällen nicht mehr. Meta erhält direkten Zugriff auf die Inhalte. Selbst wer die KI-Funktionen nicht aktiv nutzt, kann nicht sicher sein, dass seine Kommunikation – insbesondere in Gruppenchats – nicht dennoch von der KI erfasst und analysiert wird.

Dieses Beispiel verdeutlicht, wie die Einführung von KI-Technologien nicht nur die Funktionalitäten eines Dienstes erweitert, sondern auch die Kontrolle über private Daten in die Hände von Unternehmen legt, die zunehmend intransparente Überwachungssysteme etablieren. Unter diesen Bedingungen ist eine wirklich sichere Nutzung von WhatsApp nicht mehr möglich.“ [3]

Möchte die Studierendenschaft der Uni Potsdam abhängig von solch problematischen Diensten sein? Durch die alleinige Nutzung dieser Dienste wird außerdem ein lock-in begünstigt, Studierende werden dazu gedrängt, unsichere Kommunikation zu nutzen - weil „es ja sowieso alle tun“? Für die sichere und datenschutzfreundliche Kommunikation per Messenger gibt es außerdem ausreichend alternative Möglichkeiten [4].

Forderung: Die alleinige Nutzung von Meta-Diensten ist nicht akzeptabel. Der AStA betreut mindestens eine weitere möglichst datenschutzfreundliche Alternative zu WhatsApp und Instagram. Die Wahl (insbesondere wenn keine Alternative genutzt wird) ist zu begründen. Die Möglichkeiten dafür sind zahlreich genug. Es besteht kein Bedarf, einen Dienst bereits im Antrag festzuschreiben. Der AStA prüft selbst im Rahmen der eigenen Möglichkeiten, welche Dienste in Frage kommen und auch betreut werden können.

[1]

https://en.wikipedia.org/wiki/Reception_and_criticism_of_WhatsApp_security_and_privacy_features

[2]

<https://netzpolitik.org/2025/angriff-auf-privatsphaere-meta-messenger-fuehren-ki-assistenten-in-europa-ein/>

[3] <https://www.kuketz-blog.de/ki-der-elefant-im-datenladen-wie-der-datenrausch-den-datenschutz-erdruickt/>

[4] <https://www.messenger-matrix.de/messenger-matrix.html>