University of Stuttgart
Germany

Levels of Confidentiality for Information in the Context of the Use of AI Systems

Classification	**PUBLIC**	**INTERNAL**	**CONFIDENTIAL**	**STRICTLY CONFIDENTIAL**
Abbreviation	C1	C2	C3	C4
Color Code	WHITE	GREEN	AMBER	RED
Restriction	Information already published and which may be shared without restriction.	Information that may only be shared within the university and with partners, where applicable.	Information that may only be shared within the university and, where applicable, with partners according to the principle of necessity (*need-to-know*).	Information that may only be shared within an explicitly defined group.
Potential for Damage	Unauthorized disclosure of this information would have no impact on affected persons, processes, systems or facilities and no consequences for the University of Stuttgart.	Unauthorized disclosure of this information would have very low to low impact on affected persons and/or processes, systems or facilities, with minimal to hardly noticeable consequences for the University of Stuttgart.	Unauthorized disclosure of this information would have moderate to significant impact on affected persons and/or processes, systems or facilities, with noticeable to serious consequences for the University of Stuttgart.	Unauthorized disclosure of this information would have major to very major impact on affected persons and/or processes or systems, with severe to catastrophic consequences for the University of Stuttgart.
Personal Data	Personal data that have been made freely accessible by the data subjects themselves.	Personal data whose impro per handling is unlikely to lead to particular impairment, but which have not been made freely accessible by the data subjects.	Personal data whose improper handling could impair the data subject in their social standing or in their financial circumstances (“reputation”).	Personal data whose improper handling could affect the health, life or freedom of the data subject and/or could severely impair the data subject’s social standing or financial circumstances (“existence”).
Examples	•Publicly accessible research and publication information (e.g. abstracts, presentations, conference papers). •Marketing and PR material (flyers, brochures, press releases). •Public information on the University website.	•Internal memos: organizational documents of departments without confidential personal references. •Non-public teaching materials that do not contain sensitive personal data. •Initial conceptual research approaches (without sensitive details). •Copyright-protected material.	•Personnel data (e.g. salary information, applications), student data (performance records, examination data). •Unpublished research data. •Internal minutes of committees and boards that contain sensitive topics.	•Medical or psychological data of study participants, patients or students. •Details of ongoing third-party-funded projects with strict patent protection, non-disclosure agreements or high reputational risks. •Trade secrets in cooperative research projects with companies (e.g. secret technical data, prototypes, new procedures).
AI Systems Criteria: •Contractual Safeguards •Hosting •Use of Inputs for Training by the Provider •Account Binding	Use of AI systems permitted without restriction. Hosting in cloud (EU / non- EU) as well as on premises is allowed. Inputs may be used for training. External account binding at the user’s discretion.	Use permitted, provided that inputs are not used for training. Hosting on premises or in EU cloud is allowed. Use of non- EU clouds only with contractual safeguards (e.g. DPA + SCC). External account binding only if no longterm logging or analysis.	Use permitted only with contractual assurance that inputs will not be used for training. Hosting only on premises or in EU cloud with strong contractual safe guards (no third-party access, end to end encryption). Use of non-EU clouds not permitted. Internal access restricted to university members. External account binding only with pseudonymized access.	Use of AI systems only on isolated on premises systems under full control. Cloud use (including EU) is generally not permitted. Inputs must under no circumstances be used for training – contractual safeguards are strictly required. Internal traceability is desired or even necessary to prevent misuse.
Examples of AI tools	•ChatGPT Free / Plus •MS Copilot with private account	•University tool “RAI” with HAWKI 2 interface and OpenAI models via Azure • MS Copilot with University MS account	•University tool “RAI” with HAWKI 2 interface and GWDG models	•Local open-source models such as LLaMA, Mistral (currently not available)

Legend / Short Guidelines

- **On-Premises** = Systems under University control (data center, dedicated GPU servers).
- **EU-Cloud** = Cloud region within EEA + EU-GDPR compliance.
- **Non-EU Cloud** = Any cloud region outside the EEA. Standard Contractual Clauses (SCC) or equivalent guarantees are required; for C3/C4 not permitted.
- **DPA** = Data Processing Agreement; **SCC** = Standard Contractual Clauses.
- **Account Binding:** Association of user inputs with a personal account at the provider of an AI system (e.g., login with email address or University account). The provider can track which person entered which content.
- **Internal Traceability:** Local internal traceability (e.g., login for on-prem systems) is not the same as external account binding and may be required for higher confidentiality levels.