

Zulässige Vertraulichkeitsklassen nach zentralen Anwendungen

Dienstliche bzw. studienbezogene Hochschuldaten dürfen nur in von der DVZ freigegebenen Anwendungen verarbeitet werden.

Die folgende Tabelle zeigt zentrale Anwendungen der HSBI und gibt an, welche Vertraulichkeitsklassen dort verarbeitet werden dürfen – vorausgesetzt, die Zugriffsrechte sind so eingestellt, dass nur autorisierte Personen Zugriff haben. Für einige Anwendungen sind vor der Verarbeitung bestimmter Informationen zusätzliche Sicherheitsmaßnahmen nötig (z.B. E-Mail-Verschlüsselung in Exchange Online beim Versand vertraulicher oder streng vertraulicher Inhalte).

Wichtig: Bei der Verarbeitung personenbezogener Daten muss immer ein konkreter Verarbeitungszweck vorliegen. Die Zulassung einer Anwendung für vertrauliche Informationen bedeutet nicht, dass dort beliebige vertrauliche personenbezogene Daten verarbeitet werden dürfen.

Beispiel ILIAS: Auf der E-Learning-Plattform dürfen grundsätzlich vertrauliche Informationen verarbeitet werden. Vertrauliche Finanz-, Bewerbungs- oder Gesundheitsdaten gehören jedoch nicht auf ILIAS, da dies nicht dem Verarbeitungszweck der Plattform entspricht.

Allgemeine Organisationsdaten	Organisations-intern	Vertraulich	Streng vertraulich
Adobe Creative Cloud	Zulässig	Zulässig (Inhalt verschlüsseln)	Nicht zulässig
CAT	Zulässig	Zulässig	Zulässig
Cisco Webex (Meeting)	Zulässig	Zulässig	Zulässig (Verwendung der Secured Pro Meeting Vorlage erforderlich)

Allgemeine Organisationsdaten	Organisations-intern	Vertraulich	Streng vertraulich
Cisco Webex (Softphone)	Zulässig	Zulässig (keine Sprachnachrichten auf Anrufbeantworter)	Nur interne Anrufe zulässig (keine Sprachnachrichten auf Anrufbeantworter)
Cisco Webex (Messenger)	Zulässig	Zulässig	Nur interne Übermittlung zulässig
Conceptboard	Zulässig (Beim Teilen bzw. Freigeben von Boards über einen Link muss ein Passwort gesetzt werden.)	Nicht zulässig	Nicht zulässig
Dokumentenmanagementsystem (DMS)	Zulässig	Zulässig	Zulässig
DVZ-Survey	Zulässig	Nicht zulässig bei Erstellung der Umfrage. Bei personenbezogenen Daten nur pseudonymisiert in Antworten der Befragten zulässig.	Nicht zulässig bei Erstellung der Umfrage. Bei personenbezogenen Daten nur anonymisiert in Antworten der Befragten zulässig.
Exchange Online	Zulässig	Zulässig (Verschlüsselung der Inhalte erforderlich)	Zulässig (Verschlüsselung der Inhalte erforderlich)
F4transkript (Online-Transkription)	Zulässig	Bei personenbezogenen Daten nur pseudonymisiert zulässig.	Nicht zulässig

Allgemeine Organisationsdaten	Organisations-intern	Vertraulich	Streng vertraulich
HSBI-Intranet	Zulässig	Mit Ausnahmeregelungen möglich	Nicht zulässig
HSBIKI Chat	Zulässig	Nicht zulässig	Nicht zulässig
HSBI-Netzlaufwerk	Zulässig	Zulässig	Zulässig (Verschlüsselung der Inhalte erforderlich)
ILIAS (E-Assessment)	Zulässig	Zulässig	Nicht zulässig
ILIAS (E-Learning)	Zulässig	Zulässig	Nicht zulässig
KI-Connect	Zulässig	Nicht zulässig	Nicht zulässig
LSF	Zulässig	Zulässig	Nicht zulässig
MACH	Zulässig	Zulässig	Nicht zulässig
MAXQDA (Online-Version)	Zulässig	Bei personenbezogenen Daten nur pseudonymisiert zulässig	Nicht zulässig
Medienportal	Zulässig	Zulässig bei Einschränkung auf autorisierten Personenkreis	Nicht zulässig
Sciebo-Cloud	Zulässig Beim Teilen bzw. Freigeben von Dateien und Ordern über einen Link muss ein Passwort gesetzt werden.	Zulässig 2FA muss aktiviert sein und Freigabe nur direkt an autorisierte Personen	Nicht zulässig
SVA	Zulässig	Zulässig	Zulässig

Allgemeine Organisationsdaten	Organisations-intern	Vertraulich	Streng vertraulich
Zoom X (Meeting)	Zulässig	Zulässig	Zulässig (Aktivierung von E2E mit lokal gespeichertem privatem Schlüssel erforderlich)
Zoom X (Messenger)	Zulässig	Zulässig	Nur interne Übermittlung zulässig