Stand: 19.07.2023

UNIVERSITÄT GRAZ

Datenschutzerklärung „*BenutzerInnenauthentifizierung und -autorisierung mittels des SSO-Dienstes ‚uniLOGIN'*"

Der Universität Graz ist der Schutz personenbezogener Daten ein besonderes Anliegen und wir behandeln alle verarbeiteten personenbezogenen Daten vertraulich und unter Einhaltung der gesetzlichen Bestimmungen.
Diese Datenschutzerklärung soll Sie gem Art 12, 13, 14 DSGVO über die Datenverarbeitungen im Rahmen der BenutzerInnenauthentifizierung mittels uniLOGIN (basierend auf der Open Source Software „Keycloak") über Zweck(e), Rechtsgrundlage(n) und über Ihre Rechte informieren.

<u>Zweck(e) und Rechtsgrundlage(n) der Datenverarbeitung:</u>
Die Daten werden für die Zwecke der Verwaltung von Zugriffsrechten und zur BenutzerInnenauthentifizierung und -anmeldung für uni-eigene und fremde Applikationen verarbeitet, um mit deren Hilfe universitäre und innerorganisatorische Aufgaben zu erfüllen bzw Lehr- und Arbeitsmittel bereitzustellen.
Somit ist die Rechtsgrundlage der Datenverarbeitungen das berechtigte bzw öffentliche Interesse der Universität Graz an IT-Sicherheit, also Zugriffsrechte an Applikationen mit deren Hilfe universitäre und innerorganisatorische Aufgaben erfüllt werden bzw die Lehr- und Arbeitsmittel darstellen, nur dann einzuräumen, wenn die eindeutige Identität der- bzw desjenigen, die/der zugreifen will und die Authentizität ihres/seines Ersuchens nachgewiesen sind (Art 6 Abs 1 lit e und f DSGVO iVm § 3 UG).
Bei Applikationen, bei denen ein (elektronischer) Nutzungsvertrag mit dem/der einzelnen NutzerIn geschlossen wird, sind die Datenverarbeitungen der Benutzerauthentifizierung zur Erfüllung dieses Vertrags erforderlich (vgl Art 6 Abs 1 lit b DSGVO).
Darüber hinaus werden die Logdatei-Einträge im Rahmen der Nutzung von uniLOGIN gespeichert und gegebenenfalls ausgewertet, um Angriffe auf den Authentifizierungsdienst erkennen und entsprechend reagieren zu können, in Ergänzung zu den Erhebungen bei sonstigen Sicherheitsvorfällen, Systemoptimierungen vorzunehmen bzw bei Fehlermeldungen zur Klärung der zugrundeliegenden Fehler. Diese Datenverarbeitungen erfolgen im berechtigten Interesse der Universität Graz an der Ergreifung von Daten- sowie Systemsicherheitsmaßnahmen bzw an der Systemverbesserung nach Art 6 Abs 1 lit f DSGVO.
Änderungen an der Multi-Faktor-Authentifizierung (zB Entfernung des vergebenen Tokens), welche nicht vollständig automationsunterstützt durchgeführt werden können, sind nur unter Vorlage eines Identifikationsnachweises (zB amtlicher Lichtbildausweis) möglich. Hierbei werden die unbedingt erforderlichen Informationen zum vorgelegten Lichtbildausweis (Art und Nummer) aus Beweisgründen für die erfolgte Identitätsüberprüfung intern dokumentiert. Diese Datenverarbeitungen iZm Identitätsüberprüfung und ihrer Dokumentation erfolgen aufgrund des berechtigten Interesses der Uni Graz zur Ergreifung von Maßnahmen zum Ausschluss von Unbefugten von der Verwendung des universitären Accounts und aufgrund des berechtigten

UNIVERSITÄT GRAZ

Interesses der Uni Graz zur Dokumentation der erfolgten Identitätsüberprüfung zur etwaigen Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (gem Art 6 Abs 1 lit f DS-GVO).

Datenarten:

Bestandsdaten, die aus den zentralen Verzeichnisdienst der Universität an die gewünschte Applikation übermittelt werden, sind von der jeweiligen anfragenden Applikation abhängig. Die angeforderten Daten werden vor der ersten Übermittlung zur Bestätigung angezeigt.

Bestandsdaten, die von uniLOGIN verarbeitet werden:

- Vorname
- Nachname
- E-Mail-Adresse
- Eindeutiger Benutzername
- Art der Zugehörigkeit zur Universität: z.B. Studierende, Bedienstete, Bibliotheksbenutzer/in, Externe
- Rollen und Berechtigungen
- Applikationsspezifische Benutzerkennzeichen
- bPK für den Bereich BF – optional, sofern auf freiwilliger Wahl der betroffenen Person eine Anmeldung zu universitären Diensten mittels ID-Austria erfolgt

Bei Studierenden zusätzlich:

- Matrikelnummer

Bei Bediensteten zusätzlich:

- Personalnummer
- Berufliche Telefonnummer
- Berufliche Adresse

uniLOGIN-Logdaten:

Der Authentifizierungsdienst uniLOGIN speichert bei jeder Authentifizierung folgende Informationen temporär in Logdateien:

- IP-Adresse des anfragenden Clients
- Zugehöriges Land einer IP-Adresse
- NetzproviderIn einer IP-Adresse
- Häufigkeit der Nutzung eines/r NetzproviderIn und geographische Zuordnung (Land)
- Datum und Uhrzeit des Zugriffs
- URL bzw Identifikator der aufgerufenen Applikation
- Benutzername
- Attributnamen der übermittelten Daten, nicht jedoch deren Inhalt
- Verwendete Anmeldemethode (OIDC, SAML2.0, Kerberos, Passwort)

UNIVERSITÄT GRAZ

- Verwendete externe Identität (ID Austria) – optional, sofern auf freiwilliger Wahl der betroffenen Person eine Anmeldung zu universitären Diensten mittels ID-Austria erfolgt

Beim Aufruf einer uniLOGIN zugehörigen Webseite werden vom Webserver Log-Dateien im Combined Log Format erstellt und gespeichert. Dieses Format beinhaltet die IP-Adresse, ggf. authentifizierter HTTP User, Datum und Uhrzeit sowie HTTP Methode der Anfrage, den Pfad, das genutzte HTTP-Protokoll, den Status-Code, den Referrer und die übertragenen Bytes.

SSO-Cookie:
Bei uniLOGIN handelt sich um eine Single-Sign-On-Lösung (SSO), dh solange die Session in Ihrem Browser und am SSO-System gültig ist, müssen Sie sich beim Besuch weiterer durch uniLOGIN geschützter Applikationen nicht erneut authentifizieren. Nach erfolgter Authentifizierung werden auf Ihrem Client technisch erforderliche Cookies ua mit einem Schlüssel gespeichert, worüber der Authentifizierungsdienst uniLOGIN lediglich Ihre Session und damit die SSO-Funktionalität realisiert. Wird die Funktion „Angemeldet bleiben“ genutzt (sofern diese Funktionalität aktiviert ist), wird im Cookie KEYCLOAK_REMEMBER_ME der BenutzerInnenname.

Von uniLOGIN werden folgende technisch notwendigen Cookies auf Ihrem Endgerät gespeichert:

Cookie	Speicherdauer	Zweck
AUTH_SESSION_ID AUTH_SESSION_ID_LEGACY	Bis zum Ende der Session	Ausstellender Keycloak Frontendserver für Sticky Sessions bei verwendeter Lasterverteilung
KC_RESTART	Bis zum Ende der Session	Dies ist ein verschlüsseltes Token, das als Cookie gespeichert wird, damit bei einer Zeitüberschreitung des Clients die Authentifizierungssitzung neu gestartet werden kann.
KEYCLOAK_LOCALE	Bis zum Ende der Session	Die eingestellte Sprache der Web-Oberfläche
KEYCLOAK_IDENTITY	Wird die Funktion „Remember me“ verwendet 10 Stunden, ansonsten bis zum Ende der Session	ID-Token des Users. In Kombination mit der Funktion „Angemeldet bleiben“ kann während der Speicherdauer eine Anmeldung ohne die Eingabe eines Passworts

UNIVERSITÄT GRAZ

		erfolgen, auch wenn der Browser ohne aktives Logout geschlossen wird.
KEYCLOAK_REMEMBER_ME	1 Jahr, sofern es gesetzt wird	Implementierung der Funktion „Angemeldet bleiben“, auch wenn der Browser ohne aktives Logout geschlossen wird.
KEYCLOAK_SESSION KEYCLOAK_SESSION_LEGACY	Maximal 10 Stunden.	Dieses Cookie wird nur verwendet, um festzustellen, ob der Benutzer angemeldet ist.
KEYCLOAK_3P_COOKIE_SAMESITE KEYCLOAK_3P_COOKIE	Max. 1 Minute	Dieses Cookie wird zur Überprüfung der Funktionalität von 3rd-Party-Cookies für den SSO-Dienst gesetzt.

Passwortlose Authentifizierung:
Liegt eine gültige Windows-Anmeldung an einem zentral von der Universität verwalteten IT-Endgerät vor (eingebunden ins Active Directory), können diese Anmeldeinformationen (Kerberos-Ticket) dazu verwendet werden, Sie bei Wunsch zur Nutzung eines durch Keycloak gesicherten Dienstes ohne die erneute Eingabe eines Passworts zu authentifizieren.

Multifaktor Authentifizierung:
Liegen besondere Gründe vor, kann bei einer Anmeldung die Eingabe eines weiteren Faktors zur Authentifizierung erforderlich sein. Die dafür benötigten kryptographischen Schlüssel werden dem jeweiligen Account in uniLOGIN zugeordnet.

Anmeldung mit ID-Austria:
Die Anmeldemöglichkeit „Anmelden mit ID-Austria“ steht aktuell testweise zur freiwilligen Nutzung zur Verfügung. Dadurch wird die Anmeldung für universitäre Dienste auch über Ihre ID-Austria ermöglicht. Die Verarbeitung erfolgt im berechtigten Interesse, um einen einfachen und sicheren Zugang zu den Systemen der Universität Graz zu ermöglichen (gem Art 6 Abs 1 lit f DSGVO). Darüber hinaus erfolgt die Nutzung dieser Möglichkeit freiwillig.

Bei einer Anmeldung via ID Austria werden folgende personenbezogenen Daten verarbeitet:

a. Vorname
b. Nachname
c. Geburtsdatum
d. bPK für den Bereich BF
e. Temporäre ID

UNIVERSITÄT GRAZ

Speicherdauer:

Bestandsdaten aus dem zentralen Verzeichnisdienst zur Übermittlung an die gewünschte Applikation, werden in uniLOGIN aus Gründen der Performance und der Dienstbereitstellung lokal gespeichert sowie periodisch vom Verzeichnisdienst aktualisiert. Dies erfolgt, grundsätzlich für die Dauer der Angehörigeneigenschaft zur Universität Graz (Bedienstete, Studierende, sonstige externe [Kooperations]partnerInnen). Nach Beendigung dieser, werden nur die unbedingt notwendigen personenbezogenen Daten weitergespeichert, wenn dafür gesetzliche Aufbewahrungsfristen bestehen bzw zur IT-Sicherheit.
So werden Logdaten zur IT-Sicherheit (Angriffskontrolle) und zur Verbesserung des Dienstes solange gespeichert als dies zur Wahrung der berechtigten Interessen notwendig ist bzw solange bis ein (begründeter) Widerspruch erhoben wird.
Die Informationen zur Dokumentation der erfolgten Identitätsüberprüfung (Art und Nummer des Identitätsnachweises)bei nicht vollständig automationsunterstützen Änderungen der Multi-Faktor-Authentifizierung werden für drei Monate gespeichert.
Darüber hinaus speichern wir Ihre Daten nur, wenn dafür gesetzliche Aufbewahrungsfristen bestehen oder Verjährungsfristen betreffend potentieller Rechtsansprüche offen sind.

Die von uniLOGIN verwendeten Cookies werden nach Ablauf der jeweiligen Gültigkeit in der oben angegebenen Tabelle durch Ihren Browser gelöscht. Sie können diese Cookies auch jederzeit über Ihren Browser löschen.

Übermittlung:

Ihre eingegebenen Daten zur Authentifizierung werden ausschließlich uni-intern verarbeitet. Benutzername und Passwort werden dabei ausschließlich zur Überprüfung auf ihre Gültigkeit gegen den internen Verzeichnisserver über eine TLS-gesicherte Verbindung verwendet. Die Applikation, bei der Sie sich anmelden wollen, erhält danach eine Authentifizierungsbestätigung über das SAML2.0 oder OIDC-Protokoll. Das Passwort selbst wird niemals an die zu nutzende Applikation übermittelt.
Eine Übermittlung der jeweils angefragten Daten erfolgt nur an die jeweils anfragende (ggf auch externe) Applikation, bei der Sie die Anmeldung vornehmen wollen. Vor der ersten Übermittlung des jeweiligen Datums wird Ihnen eine Oberfläche zur Bestätigung angezeigt. Wird die erstmalige Übermittlung nicht bestätigt, so kann es zu Problemen bei der Anmeldung zum betreffenden Dienst kommen.

Ihre Rechte:

Im Zusammenhang mit der Verarbeitung Ihrer personenbezogenen Daten verfügen Sie jederzeit über die sog „Betroffenenrechte“ gem Art 15 ff DSGVO, im Zusammenhang mit den konkreten Datenverarbeitungen, sind dies die folgenden Rechte, welche bei der Universität Graz als Verantwortlichen, Mailadresse: rektorsbuero@uni-graz.at geltend gemacht werden können:

- Recht auf Auskunft über die betreffenden personenbezogenen Daten (Art 15 DSGVO),

UNIVERSITÄT GRAZ

- Recht auf Berichtigung (Art 16 DSGVO) oder Löschung (Art 17 DSGVO) oder auf Einschränkung der Verarbeitung (Art 18 DSGVO),
- Recht auf Widerspruch (Art 21 DS-GVO),

Darüber hinaus besteht das

- Recht auf Beschwerde (Art 77 DSGVO),

welches bei einer Aufsichtsbehörde, in Österreich ist dies die österreichische Datenschutzbehörde, Barichgasse 40-42, 1030 Wien, Telefon: +43 1 52 152-0, E-Mail: dsb@dsb.gv.at, einzubringen wäre.

Unsere Kontaktdaten:

Unsere Kontaktdaten lauten: Universität Graz, 8010 Graz, Mail: rektorsbuero@uni-graz.at
Unsere Datenschutzbeauftragte erreichen Sie unter: dsba@uni-graz.at
Allgemeine Datenschutzanfragen richten Sie bitte an: datenschutz@uni-graz.at