All. 2 al modulo per la richiesta di accesso

Condizioni di utilizzo

1) Il soggetto fruitore assicura che la fruizione di tali dati è necessaria e avverrà esclusivamente per lo svolgimento dei propri compiti istituzionali, specifica la natura e la qualità dei dati richiesti, evidenzia altresì, i riferimenti normativi che giustificano la domanda di accesso alla banca dati studenti. I dati cui avrà accesso possono essere elaborati all'interno dei servizi e dei procedimenti attinenti i propri compiti istituzionali sotto la propria responsabilità.
   L'Università soggetto erogatore è sollevata da ogni responsabilità contrattuale ed extracontrattuale per danni di qualsiasi natura, diretti o indiretti, che possano derivare da eventuali interruzioni, ritardi e/o sospensioni dell'accesso da qualsiasi causa siano essi determinati.
   L'Università soggetto erogatore è sollevata altresì da ogni responsabilità contrattuale ed extracontrattuale per l'eventuale utilizzo e trattamento dei dati improprio o illecito da parte degli utenti abilitati dal soggetto fruitore o da parte di chiunque comunque riconducibile al soggetto fruitore, nonché per le conseguenti eventuali richieste di risarcimento da parte di terzi.

2) Il soggetto fruitore assicura il regolare e corretto utilizzo dei dati nel rispetto della normativa vigente, anche in materia di consultazione delle banche dati osservando le misure di sicurezza ed i vincoli di riservatezza; in particolare:
   - procede al trattamento dei dati personali, in particolare di quelli sensibili, osservando le misure di sicurezza ed i vincoli di riservatezza rispettando i canoni di pertinenza e non eccedenza nel trattamento delle informazioni acquisite, nonché di indispensabilità, nel caso di dati sensibili e giudiziari;
   - garantisce che non si verifichino divulgazioni, comunicazioni, cessioni a terzi, né in alcun modo riproduzioni dei dati nei casi diversi da quelli previsti dalla legge, provvedendo ad impartire, precise e dettagliate istruzioni agli incaricati del trattamento, richiamando la loro attenzione sulle responsabilità connesse all'uso illegittimo dei dati;
   - si impegna a non duplicare i dati resi disponibili e a non creare autonome banche dati non conformi alle finalità per le quali è stato autorizzato l'accesso;
   - garantisce che l'accesso ai dati verrà consentito esclusivamente a personale o assimilati ovvero a soggetti che siano stati designati dal fruitore quali incaricati o responsabili esterni del trattamento dei dati;
   - ha consapevolezza della possibilità di controlli ivi previsti per verificare il rispetto dei vincoli di utilizzo dei servizi, previo preavviso tra le rispettive funzioni organizzative preposte alla sicurezza. Per l'espletamento di tali controlli, che potranno essere effettuati anche presso le sedi del fruitore dove viene utilizzato il servizio, il fruitore si impegna a fornire ogni necessaria collaborazione;
   - si impegna, non appena siano state utilizzate le informazioni secondo le finalità dichiarate, a cancellare i dati ricevuti dal soggetto erogatore;
   - si impegna a formare gli utenti abilitati sulle specifiche caratteristiche, proprietà e limiti del sistema utilizzato per l'accesso ai dati ed a controllarne il corretto utilizzo;
   - garantisce l'adozione al proprio interno delle regole di sicurezza atte ad:
     - adottare procedure di registrazione che prevedano il riconoscimento diretto e l'identificazione certa dell'utente;
     - assicurare che l'accesso alla banca dati avvenga attraverso postazioni protette;
     - adottare regole di gestione delle credenziali di autenticazione e modalità che ne assicurino adeguati livelli di sicurezza, quali ad esempio: identificazione univoca di una persona fisica; processi di emissione e distribuzione agli utenti in maniera sicura seguendo una procedura operativa stabilita; le credenziali possono essere costituite da un dispositivo in possesso ed uso esclusivo dell'incaricato e provvisto di pin o da una coppia username/password, o, infine, da dispositivi che garantiscano analoghe condizioni di robustezza. Nel caso le credenziali siano costituite da una coppia

username/password, devono essere previste politiche di gestione della password che rispettino le misure di sicurezza previste dall'art 32 Regolamento UE 679/2016 la procedura di autenticazione dell'utente deve essere protetta dal rischio di intercettazione delle credenziali con meccanismi crittografici di robustezza adeguata;

- si impegna ad utilizzare i sistemi di accesso ai dati in consultazione on line esclusivamente secondo le modalità con cui sono stati resi disponibili e, di conseguenza, a non estrarre i dati per via automatica e massiva (attraverso ad esempio i cosiddetti "robot") allo scopo di velocizzare le attività e creare autonome banche dati non conformi alle finalità per le quali è stato autorizzato all'accesso;
- si impegna altresì a comunicare all'amministrazione erogatrice:
  - tempestivamente incidenti sulla sicurezza occorsi nell'attività di autenticazione qualora tali incidenti abbiano impatto direttamente o indirettamente nei processi di sicurezza afferenti la fruibilità dei dati;
  - ogni eventuale esigenza di aggiornamento di stato degli utenti gestiti (nuovi inserimenti, disabilitazioni, cancellazioni) in caso di consultazione on line;
  - ogni modificazione tecnica e/o organizzativa del proprio dominio, che comporti l'impossibilità di garantire l'applicazione delle regole sopra riportate e/o la loro perdita di efficacia;

3) Il soggetto fruitore, in quanto titolare del trattamento dei dati oggetto di comunicazione da parte dell'erogatore, deve designare gli incaricati e l'eventuale responsabile del trattamento dei dati.