UNIVERSITÀ
DEGLI STUDI DELLA
BASILICATA

Al Magnifico Rettore
dell'Università degli studi della Basilicata
PEC: protocollo@pec.unibas.it

RICHIESTA DI ACCREDITAMENTO PER L'ACCESSO ALLA BANCA DATI STUDENTI "ESSE3 PA" UNIVERSITÀ DEGLI STUDI DELLA BASILICATA

Il sottoscritto:

Nome _____ Cognome _____

Email _____ Tel _____

in qualità di _____

Denominazione Ente _____

C.F. o P.IVA_____ Indirizzo _____

Comune _____ Prov. _____

Codice IPA _____ PEC _____

Finalità specifiche per cui viene richiesto l'accesso (barrare la finalità specifica)**:**

☐ Verifica autocertificazioni riguardanti il possesso dei titoli di studio di coloro che intendono iscriversi o che sono iscritti ai corsi di studio offerti dall'Ateneo;

☐ Verifica autocertificazioni riguardanti il possesso dei titoli di studio presentati/dichiarati dai dipendenti e dai candidati che partecipano/hanno partecipato a procedure selettive per lo svolgimento delle funzioni del profilo di inquadramento richiesto presso l'amministrazione;

☐ Verifica autocertificazioni riguardanti il possesso dei titoli di studio di coloro che intendono iscriversi all'albo/ordine professionale per l'esercizio della professione di

_____

☐ Verifica autocertificazioni dei titoli di studio dichiarati dai docenti che si inseriscono nelle graduatorie di istituto (specificare la graduatoria)

_____

☐ Verifica autocertificazioni riguardanti il possesso dei titoli di studio per (specificare);

☐ Altro (specificare) _____;

Riferimento normativo che legittima l'accesso:

☐ art.li 71 D.P.R. 445/2000;

☐ Altro (specificare) _____

DICHIARA

☐ di essere Pubblica Amministrazione;

☐ di essere gestore di pubblici servizi (art. 43 del D.P.R. 445/2000);

☐ di aver preso visione delle modalità di erogazione e delle condizioni di utilizzo del servizio (Allegato 1);

☐ di accettare le condizioni di utilizzo del servizio che formano parte integrante della richiesta;

☐ di informare gli utenti abilitati sulle suddette condizioni di utilizzo del servizio

COMUNICA

che il referente responsabile dell'accesso è:

Cognome e Nome: _____

Codice Fiscale: _____

Luogo di nascita: _____ Data di nascita: _____

Email Istituzionale (2): _____

Ruolo nell'Ente _____

CHIEDE

l'abilitazione ad accedere alla banca dati ESSE3PA per i soggetti (1) indicati di seguito per le finalità specificate:

Operatori autorizzati al servizio

Cognome e Nome: _____

Codice Fiscale: _____

Luogo di nascita: _____ Data di nascita: _____

Email Istituzionale (2): _____

Struttura/Ufficio: _____

Indirizzo IP pubblico richiedente: _____

UNIVERSITÀ
DEGLI STUDI DELLA
BASILICATA

Operatori autorizzati al servizio

Cognome e Nome: _____

Codice Fiscale: _____

Luogo di nascita: _____ Data di nascita: _____

Email Istituzionale [2]: _____

Struttura/Ufficio: _____

Indirizzo IP pubblico richiedente: _____

[1] indicare non più di 2 utenti.
[2] e-mail personale istituzionale assegnata cioè dall'ente di appartenenza

IL RAPPRESENTANTE LEGALE
(atto sottoscritto in forma digitale)

Compilare in tutte le sue parti.
Inviare a protocollo@pec.unibas.it **il modulo compilato, allegando copia dei documenti di identità e Codice Fiscale degli Operatori da abilitare al servizio.**

ALLEGATO 1 – ACCORDO SULLE CONDIZIONI ATTUATIVE PER L'ACCESSO ALLA BANCA DATI "ESSE3 PA" DELL'UNIVERSITÀ DEGLI STUDI DELLA BASILICATA

1. L'Università degli Studi della Basilicata ("Ateneo"), in ottemperanza ai principi del D. Lgs. 7 marzo 2005, n. 82, recante il Codice dell'amministrazione digitale ("CAD"), mette a disposizione delle Pubbliche Amministrazioni e dei gestori di pubblici servizi (anche, "Soggetto fruitore" o "Ente richiedente"), al fine di agevolare l'acquisizione d'ufficio e il controllo sulle dichiarazioni sostitutive presentate da soggetti riguardanti informazioni e dati di cui agli articoli 46 e 47 del DPR 28/12/2000, n. 445 e successive modifiche, un servizio di accesso telematico, diretto e gratuito, attraverso la banca dati "Esse3 PA" accessibile dal sito istituzionale dell'Ateneo, ai dati di carriera auto dichiarati dai propri studenti e laureati ("Servizio"). L'accesso al Servizio deve avvenire esclusivamente nel rispetto del Regolamento UE 2016/679 ("GDPR"), del D. Lgs. 30 giugno 2003, n. 196 recante il Codice in materia di protezione dei dati personali e ss.mm.ii. ("Codice della Privacy"), e dei provvedimenti del Garante per la protezione dei dati personali in materia di accesso ai dati personali delle Pubbliche Amministrazioni (con particolare riferimento alle "Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche del 2 luglio 2015").

2. L'Ateneo si impegna, inoltre, a verificare l'esistenza di una idonea base giuridica, in caso di richiesta di accesso a dati particolari o giudiziari di cui agli artt. 9 e 10 del GDPR. L'Ateneo rende disponibili al Soggetto fruitore le informazioni personali nel rispetto dei principi di pertinenza e non eccedenza in considerazione delle finalità istituzionali perseguite con la richiesta.

3. Il Soggetto fruitore richiede l'accreditamento in base alle finalità istituzionali perseguite in modo tale da avere accesso ai soli dati personali necessari dichiarati dall'interessato, nel rispetto del principio di "minimizzazione dei dati" sancito dall'art. 5 c. 1 lett. c) del GDPR.
   In particolare, in osservanza del predetto principio, il Soggetto fruitore può richiedere l'accesso ai profili di seguito elencati:
   - Profilo 1 - Conferma Titolo: attraverso questo profilo l'operatore/l'operatrice PA accreditato/a, inserendo Codice Fiscale, può verificare i dati personali (Cognome; Nome; Data di nascita; Comune o stato straniero di nascita, Cittadinanza) e i dati di carriera di studenti e laureati (Matricola; Stato carriera; Anno Accademico e data di inizio carriera; Anno Accademico e data di fine carriera; Titolo della qualifica rilasciata/Titolo conseguito; Classe di laurea; Normativa di riferimento; Durata prevista; Motivo chiusura carriera; Voto conseguito). Per gli esami di stato i dati disponibili sono relativi a: Denominazione; Sessione Abilitazione; Voto Abilitazione; Professione Abilitazione.
   - Profilo 2 - Verifica dati di carriera: attraverso questo profilo l'operatore/l'operatrice PA accreditato/a, inserendo Codice Fiscale, può verificare i dati personali (Cognome; Nome; Data di nascita; Comune o stato straniero di nascita, Cittadinanza), i dati di carriera (Matricola; Stato carriera; Anno Accademico e data di inizio carriera; Anno Accademico e data di fine carriera; Titolo della qualifica rilasciata/Titolo conseguito; Classe di laurea; Normativa di riferimento), gli Anni Accademici di iscrizione (con tabella di dettaglio contenente Anno Accademico; Data di iscrizione; Corso di studio; Anno di corso) e gli Esami sostenuti" di studenti e laureati (con tabella di dettaglio contenente Codice AD/Attività Didattica; Denominazione AD; CFU/Crediti Formativi Universitari; Voto; AA e data superamento; Tipo convalida; TAF/Tipo Attività Formativa; SSD/Settore scientifico Disciplinare).

   Il Soggetto fruitore accreditato potrà, inoltre, procedere alla verifica delle dichiarazioni sostitutive presentate da studenti e laureati dell'Ateneo, inserendo il codice identificativo PA contenuto nell'intestazione del documento presentato, accedendo così alla versione originale del pdf corrispondente, prodotta da ESSE3.

4. L'accesso alla Banca Dati è disponibile attraverso una connessione ad accesso riservato realizzata con collegamento web e credenziali di autenticazione fornite ai soggetti individuati dall'Ente fruitore che comunicherà le generalità dei dipendenti incaricati da abilitare.

5. Per poter effettuare l'accesso al Servizio è necessaria una preventiva autorizzazione da parte dell'Ateneo. Il Soggetto fruitore richiede l'autorizzazione inviando alla casella di posta elettronica certificata dell'Ateneo (protocollo@pec.unibas.it) il modulo "Richiesta di accreditamento all'accesso alla Banca Dati "Esse3 PA" che riporta il nominativo del Richiedente accreditamento (qualora diverso dal rappresentante legale) e i nominativi degli/delle incaricati/e indicati dal Soggetto fruitore da abilitare al Servizio. La PEC dalla quale viene effettuata la richiesta deve coincidere con quella istituzionale dell'Ente. L'Ente che intende aderire all'accordo in oggetto potrà richiedere l'abilitazione al servizio di un numero massimo due utenze per sede territoriale.

6. L'accesso ai dati personali deve rispettare i criteri di legittimità, pertinenza e non eccedenza rispetto alle finalità della richiesta del Soggetto fruitore, nel pieno rispetto della normativa vigente e in presenza dei presupposti legittimanti l'accesso alle informazioni del soggetto dichiarante. Non sono consentite la duplicazione dei dati resi disponibili e l'estrazione dei dati per via automatica e massiva (attraverso ad esempio i cosiddetti "robot") allo scopo di velocizzare le attività e creare autonome banche dati che non sarebbero conformi alle finalità per le quali è stato autorizzato l'accesso. Il Soggetto fruitore non può in alcun caso cedere a terzi i dati personali a cui ha accesso in ragione della presente Convenzione. È, in ogni caso, esclusa la possibilità per il Soggetto fruitore di effettuare accessi alle banche dati dell'Ateneo in modalità diversa da quella prevista dalla presente Convenzione.

7. Con la sottoscrizione della domanda di accreditamento il Soggetto fruitore:

   - si impegna ad utilizzare le informazioni di cui viene a conoscenza attraverso il collegamento alla Banca Dati dell'Ateneo esclusivamente per i propri fini istituzionali, osservando in particolare i "Principi applicabili al trattamento di dati personali" ai sensi dell'art. 5 del GDPR lett. a) (liceità, correttezza e trasparenza), lett. b (limitazione della finalità), lett. c) (minimizzazione dei dati), lett. d) (esattezza), lett. e) (limitazione della conservazione), lett. f (integrità e riservatezza) specialmente quando le stesse abbiano ad oggetto dati particolari (alias, sensibili) o riguardino condanne penali e reati (qualificati quali dati particolari e giudiziari dagli artt. 9 e 10 del GDPR);

   - 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 e i vincoli di riservatezza previsti dal GDPR, dal Codice della Privacy e dai provvedimenti del Garante per la protezione dei dati personali in materia di consultazione dei dati per via telematica;

   - si impegna ad adottare le misure tecniche e organizzative necessarie ad evitare indebiti utilizzi delle medesime informazioni e dati, garantendone la riservatezza e assumendone la responsabilità dell'uso del canale d'accesso per le sole finalità istituzionali dichiarate;

   - si impegna a formare gli utenti abilitati sulle specifiche caratteristiche, proprietà e limiti del sistema utilizzato per l'accesso ai dati personali e a controllarne il corretto utilizzo;

   - garantisce che l'accesso ai dati personali verrà consentito esclusivamente a soggetti che siano stati designati dal Soggetto fruitore quali autorizzati al trattamento ai sensi dell'art. 29 del GDPR e 2-quaterdecies del Codice della Privacy;

   - autorizza l'Ateneo ad effettuare controlli volti a verificare il rispetto dei vincoli di utilizzo del Servizio, con congruo preavviso; la data dei controlli deve essere concordata tra le rispettive funzioni organizzative preposte alla sicurezza. Il Soggetto fruitore si impegna sin d'ora a fornire ogni necessaria collaborazione per l'espletamento di tali controlli, anche presso le proprie sedi;

   - garantisce l'adozione al proprio interno delle regole di sicurezza atte a:
     - 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 prescritte dal Garante in materia di consultazione dei dati per via telematica; la procedura di autenticazione dell'utente deve essere protetta dal rischio di intercettazione delle credenziali con meccanismi crittografici di robustezza adeguata;

- si impegna altresì a comunicare tempestivamente all'Ateneo:
  - eventuali incidenti sulla sicurezza occorsi nell'attività di autenticazione qualora tali incidenti abbiano impatto direttamente o indirettamente sui processi di sicurezza afferenti alla fruibilità dei dati e nel caso di violazione o sospetta violazione della sicurezza di uno o più account resi disponibili dall'Ateneo. Tali comunicazioni dovranno essere effettuate entro 48 ore dalla scoperta e dovranno contenere tutti gli elementi prescritti dall'art. 33, paragrafo 3, del GDPR;
  - ogni eventuale esigenza di aggiornamento di stato degli utenti gestiti (nuovi inserimenti, disabilitazioni, cancellazioni);
  - 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.

8. L'Ateneo potrà modificare i sistemi di elaborazione, ricerca, rappresentazione e organizzazione dei dati, nonché gestire le informazioni memorizzate. Resta inteso che l'Ateneo è libero di variare la base informativa in relazione alle proprie esigenze istituzionali e strutturali e alle innovazioni tecniche relative al proprio sistema informatico, e di modificare l'accesso, anche limitando l'utilizzo dei dati, in conseguenza a variazioni del contesto normativo o organizzativo che possono subentrare successivamente alla sottoscrizione della presente Richiesta di accreditamento. In tal caso, l'Ateneo fornirà al Soggetto fruitore adeguata notizia delle eventuali modifiche introdotte nei sistemi di elaborazione, ricerca, rappresentazione, accesso ed organizzazione dei dati. Nessuna responsabilità potrà gravare sull'Ateneo per danni di qualsiasi natura, diretti e indiretti, per le suddette variazioni, né per eventuali sospensioni o interruzioni del Servizio.

9. Il rappresentante legale dell'Ente richiedente, per effetto della comunicazione di dati personali effettuata dall'Ateneo, nell'ambito della presente Richiesta di accreditamento, diviene Titolare autonomo dei dati personali ricevuti ai sensi dell'art. 4, n. 7) del GDPR. Questi pertanto assume in sé tutti gli adempimenti derivanti per il Titolare dalla normativa vigente in materia di protezione dei dati personali, provvede ad individuare e nominare le persone autorizzate al trattamento dei dati, impartendo loro le istruzioni necessarie ai fini del corretto trattamento dei dati di cui vengono a conoscenza nell'ambito dell'accordo, provvedendo altresì al rispetto dei diritti dell'interessato di cui agli artt. 13 e 14 GDPR nonché fornendo riscontro ai diritti dell'interessato di cui agli artt. 15 – 22 del GDPR.

10. I dati personali cui il Soggetto fruitore avrà accesso dovranno essere elaborati, sotto la propria responsabilità, nell'ambito dei propri compiti istituzionali. L'Ateneo è sollevato da ogni responsabilità contrattuale ed extracontrattuale per l'eventuale utilizzo e trattamento dei dati personali impropri o illeciti effettuati dagli utenti abilitati dal Soggetto fruitore o da chiunque operi per conto dello stesso, nonché da ogni eventuale richiesta di risarcimento da parte di terzi derivanti in conseguenza a fatti o omissioni direttamente o indirettamente riconducibili al Soggetto fruitore.

11. Le credenziali di autenticazione al servizio, costituite da un identificativo della persona e di una password che verranno fornite a seguito dell'accoglimento della richiesta d'accesso, sono strettamente personali e per la loro custodia l'utente si impegna ad adottare le necessarie cautele. Esse non possono in alcun modo essere cedute o comunicate a terzi. Il referente responsabile dell'accesso dell'Ente fruitore si impegna a informare tempestivamente l'Università degli Studi della Basilicata in merito ad ogni variazione relativa

agli incaricati, mediante comunicazione a mezzo PEC. Ad ogni incaricato l'Ateneo erogatore associa individualmente una credenziale di autenticazione comunicata tramite posta elettronica all'indirizzo mail personale istituzionale assegnato al soggetto incaricato dall'ente di appartenenza. La password avrà una validità di **90 giorni**, alla scadenza dei quali l'utente dovrà obbligatoriamente cambiarla.

12. L'Ateneo si riserva di effettuare controlli periodici sugli accessi effettuati, attraverso strumenti di tracciatura, per monitorare gli utilizzi impropri e per prevenire accessi multipli. L'Ente fruitore si impegna a collaborare con ogni disponibilità con l'Università degli Studi della Basilicata nel garantire la massima trasparenza al soggetto su cui è stato effettuato l'accesso ai dati, sulla legittimità dell'azione amministrativa e ai sensi degli artt.15-23 di cui al Capo III GDPR.

13. Il presente accordo ha durata quinquennale, con facoltà di rinnovo previa richiesta scritta del Soggetto fruitore.

14. Per tutto quanto non espressamente previsto dal presente accordo in materia di obblighi e responsabilità dei Titolari dei trattamenti, si fa rinvio alla disciplina stabilita dal GDPR e dal D.Lgs. 196/2003 così come modificato e integrato dal D.Lgs. 101/2018.

15. L'Ateneo si riserva di disabilitare gli accessi in caso di rilevazione di anomalie nell'utilizzo del sistema. In casi estremi e motivabili, può procedere alla risoluzione immediata dell'accordo con segnalazione all'autorità competente, fatto salvo il risarcimento del danno.

16. In base a quanto previsto dalle disposizioni dell'AgID l'accesso alle banche dati della Pubblica Amministrazione è gratuito. Nel caso in cui l'Ente richiedente metta a disposizione le proprie banche dati dietro corrispettivo economico, l'Ateneo potrà applicare condizioni di reciprocità.

17. L'Ateneo (Ente erogatore) è sollevato da qualsiasi responsabilità contrattuale ed extracontrattuale per danni derivanti dall'eventuale uso e trattamento dei dati improprio o illecito da parte dell'Ente fruitore e oggetto dell'autorizzazione, per le conseguenti eventuali richieste di risarcimento da parte di terzi nonché per eventuali danni derivanti da interruzioni, rallentamenti o errori nell'erogazione o fruizione del servizio di accesso ai dati. Degli interventi programmati o straordinari sul servizio, come pure dei tempi di ripristino, l'Ente erogatore darà comunicazione mediante il proprio sito web istituzionale.

18. Per qualsiasi controversia tra l'Ateneo e l'Ente fruitore, che sia collegabile direttamente o indirettamente alla sottoscrizione dell'accordo, il foro competente è quello di Potenza.