All. 1 al modulo per la richiesta di Accreditamento

CONDIZIONI ATTUATIVE DELL'ACCORDO DI SERVIZIO PER L'ACCESSO ALLA BANCA DATI "ESSE3 PA" DELL'UNIVERSITÀ IUAV DI VENEZIA ("ACCORDO")

1) L'Università IUAV di Venezia ("**IUAV**" o "**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 IUAV, 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) Al fine di consentire l'accesso alla propria banca dati, IUAV ha proceduto a verificare, prima della sottoscrizione, che il Soggetto fruitore sia legittimato a concludere il presente Accordo in ragione del perseguimento della propria finalità istituzionale e IUAV 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.

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 richiede l'accesso ai profili di seguito selezionati:

a. **[] Profilo 1 - Conferma Titolo**: attraverso questo profilo l'operatore PA accreditato, 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.
b. **[] Profilo 2 - Verifica dati di iscrizione**: attraverso questo profilo l'operatore PA accreditato, 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) e gli Anni Accademici di iscrizione di studenti e laureati (con tabella di dettaglio contenente Anno Accademico; Data di iscrizione; Corso di studio; Anno di corso).
c. **[] Profilo 3 - Verifica dati di carriera**: attraverso questo profilo l'operatore PA accreditato, 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 di IUAV, inserendo il codice identificativo PA contenuto nell'intestazione del documento presentato, accedendo così alla versione originale del pdf corrispondente, prodotta da Esse3.

4) IUAV 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. Tale accesso avviene attraverso una connessione riservata realizzata con collegamento *https* e credenziali di autenticazione fornite ai soggetti nominativamente individuati dal Soggetto fruitore, autorizzati da IUAV.

5) Per poter effettuare l'accesso al Servizio è necessaria una preventiva autorizzazione da parte di IUAV. Il Soggetto fruitore richiede l'autorizzazione inviando alla casella di posta elettronica certificata dell'Ateneo (ufficio.protocollo@pec.iuav.it) il modulo "*Richiesta di accreditamento all'accesso alla Banca Dati "Esse3 PA" dell'Università IUAV di Venezia"* che riporta il nominativo del Referente responsabile dell'accesso (qualora diverso dal rappresentante legale) e i nominativi degli incaricati indicati dal Soggetto fruitore da abilitare al Servizio. La PEC dalla quale viene effettuata la richiesta deve coincidere con quella istituzionale dell'Ente. Quest'ultimo potrà richiedere l'abilitazione al Servizio di un numero massimo di tre utenze, oltre al referente responsabile dell'accesso. La consultazione della Banca Dati avviene attraverso la rete del server del Soggetto fruitore.

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. IUAV conserva l'esclusiva titolarità del dato; il Soggetto fruitore non può in alcun caso cedere a terzi i dati personali a cui ha accesso in ragione del presente Accordo. 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 dal presente Accordo.

7) Con la sottoscrizione della domanda d'accreditamento il Soggetto fruitore:
- si impegna ad utilizzare le informazioni di cui viene a conoscenza attraverso il collegamento alla banca dati di IUAV 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);
- 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 a IUAV:
▪ 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 da IUAV. 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) IUAV potrà modificare i sistemi di elaborazione, ricerca, rappresentazione e organizzazione dei dati, nonché gestire le informazioni memorizzate. Resta inteso che IUAV è libera 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 del presente Accordo. In tal caso, IUAV 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 su IUAV 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 da IUAV, nell'ambito del presente Accordo, diviene Titolare autonomo dei dati personali ricevuti ai sensi dell'art. 4, n. 7) del GDPR. Pertanto, quest'ultimo è tenuto ad effettuare tutti gli adempimenti che la normativa in materia di protezione dei dati personali prescrive in capo al Titolare del trattamento; ad esempio, provvede ad individuare e nominare le persone quali autorizzati al trattamento dei dati, impartendo loro le istruzioni necessarie ai fini del corretto trattamento dei dati personali di cui vengono a conoscenza in virtù dell'Accordo (art. 29 del GDPR), richiamando la loro attenzione sulle responsabilità connesse all'uso illegittimo dei dati, provvedendo altresì a rendere, ove necessario, le informative di cui agli artt. 13 e 14 del 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. IUAV è sollevata 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) Il Servizio si struttura ed esplica attraverso le seguenti modalità di erogazione:

a) Richiesta di accesso

Per essere accreditato ad accedere al servizio il *Soggetto fruitore* inoltra a mezzo pec all'indirizzo ufficio.protocollo@pec.iuav.it è necessario procedere alla compilazione e sottoscrizione (con firma digitale del legale rappresentante) del modulo denominato "*Richiesta di accreditamento all'accesso alla Banca Dati "Esse3 PA" dell'Università IUAV di Venezia"*.

b) Utilizzo dei dati

I dati personali di cui l'Università IUAV di Venezia è titolare sono resi accessibili esclusivamente quando il trattamento degli stessi è necessario per lo svolgimento dei compiti istituzionali del Soggetto fruitore. I dati personali cui si accede possono essere elaborati dai sistemi informativi dell'Ente richiedente sotto la propria responsabilità, all'interno dei servizi e dei procedimenti attinenti i compiti istituzionali dello stesso. Il Soggetto fruitore, pertanto, deve specificare i motivi per i quali richiede l'accesso ai dati, impegnandosi al loro corretto utilizzo nel rispetto della normativa in materia di protezione dei dati personali. Deve altresì utilizzare le informazioni acquisite esclusivamente per le finalità dichiarate, nel rispetto dei principi di pertinenza e non eccedenza (cd. "principio di necessità"), 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).

c) Termini di attivazione del servizio

L'Ateneo comunicherà al Soggetto fruitore la data di attivazione del Servizio, mediante posta elettronica certificata (PEC), entro sette giorni lavorativi dalla data di ricevimento della richiesta debitamente compilata. Le credenziali e le modalità di accesso al Servizio saranno trasmesse a ciascun soggetto autorizzato all'indirizzo di posta elettronica istituzionale personale comunicato. Qualora l'Ente richiedente non si trovi nelle condizioni previste dalla normativa vigente per l'accesso e il trattamento dei dati, IUAV si riserva di non accettare la richiesta e di non attivare il Servizio: l'esercizio di tale facoltà sarà motivato e prontamente comunicato al Soggetto fruitore nei termini di cui sopra.

d) Durata del servizio

L'Ateneo può verificare, con cadenza periodica almeno annuale, che continuino a ricorrere le specifiche finalità istituzionali per cui ha concesso l'accesso alla propria banca dati, anche con riferimento alle abilitazioni assegnate. L'accesso verrà disattivato qualora vengano meno le finalità per le quali il Servizio è stato autorizzato, o qualora il Soggetto fruitore cessi di trovarsi nelle condizioni previste dalla normativa vigente per l'accesso e il trattamento dei dati.

e) Infrastruttura tecnologica per l'accesso ai dati

Il Servizio è erogato da un'infrastruttura tecnologica dedicata con accesso via web, raggiungibile attraverso il sito istituzionale dell'Ateneo (http://www.iuav.it), sezione "Imprese e Enti" del menù "Servizi" http://www.iuav.it/studenti/tirocinio-/Verifiche-/ e specificatamente predisposta: https://iuav.esse3.cineca.it/Start.do . L'utilizzo del protocollo HTTPS garantisce il trasferimento sicuro delle credenziali di accesso e dei dati. L'accesso al sito è pubblico per la parte riguardante le informazioni di ausilio; il Servizio è disponibile nell'area riservata.

f) Modalità di trattamento dei dati e regole di accesso

Il sito https://iuav.esse3.cineca.it/Start.do contiene le informazioni per un corretto utilizzo del Servizio erogato e tali informazioni saranno aggiornate in tempo reale in caso di eventuali modifiche applicative.

L'accesso avviene tramite browser web in HTTPS a seguito di autenticazione inserendo le credenziali di accesso (login e password) negli appositi campi.

g) Servizi forniti e livelli di utilizzo

Attraverso il Servizio "Verifica Autocertificazioni" (funzionalità disponibile a seguito di autenticazione) è possibile accedere ai dati recuperabili in relazione al profilo assegnato o alla versione originale della documentazione prodotta dal sistema informativo dell'Ateneo, a partire dal suo codice univoco di intestazione, per confrontarla col documento presentato dal cittadino in sede di autocertificazione.

Il Servizio è accessibile 24 ore al giorno per 7 giorni la settimana.

h) Regole di sicurezza e di tracciabilità garantite dall'applicazione

L’accesso all’area riservata avviene sempre tramite credenziali d’accesso; l’uso e la custodia di tali credenziali (“login” e “password”) sono sotto la responsabilità del Soggetto fruitore. IUAV, in qualità di Soggetto erogatore, provvederà alla registrazione dell’utente al Servizio fornendo un login e un codice di prima attivazione (password da cambiare al primo accesso). Il sistema tiene traccia dell'orario di accesso, delle operazioni effettuate. Tali informazioni vengono mantenute per il tempo necessario alle attività di controllo sul corretto uso del Servizio da parte del Soggetto fruitore.

i) Modalità di assistenza

I riferimenti all’ufficio dell’Ateneo incaricato dell’assistenza sono riportati sul sito istituzionale www.iuav.it, sezione “Imprese e Enti”/ verifica autocertificazioni / contatti”.