Atto di Nomina del Responsabile del trattamento dei dati personali

ai sensi e per gli effetti dell'art. 28 del Regolamento (UE) 2016/679

Addendum al contratto stipulato in data _____

L'Università degli Studi di Messina_____, con sede in Messina, Piazza Pugliatti 1, 98122_____, in persona della Rettrice, prof.ssa Giovanna Spatari_____, nata _____, il _____ la quale dichiara di essere munito di tutti i poteri necessari per la sottoscrizione del presente Atto (di seguito **Titolare**)

E

Svelto! – Big Data Cleaning and Analytics *Srl* (di seguito Svelto!), con sede in Pignola (PZ), Via Tintera n. 2d, Codice fiscale/Partita IVA 01984490761, in persona del suo legale rappresentante p.t. Maria Grazia Russo, nata a Napoli, il 31 luglio 1969 (di seguito **Responsabile**)

congiuntamente indicate come **Parti**

Premesso che

a) L'Università degli Stuti di Messina_____ in data _____ ha aderito al contratto CRUI per l'accesso alla FORNITURA QUINQUENNALE DEL SOFTWARE CRITERIUM E SERVIZI CONNESSI - CIG [9208565C39], sottoscritto in data 12 Giugno 2023, di cui al D.R. n. 1797/2023 del 09 Giugno 2023 ratificato nella seduta del Consiglio di amministrazione del 14 Giugno 2023
b) l'Università si è dotata di un Regolamento di Ateneo per le Attività di Valutazione e Autovalutazione della Ricerca approvato nella seduta del _____;
c) le attività oggetto del Contratto comportano o possono comportare il trattamento di dati personali, ai sensi del Regolamento (UE) 2016/679 (di seguito Regolamento) nonché del D.Lgs. 196/2003 e ss.mm.ii recante il Codice in materia di protezione dei dati personali (di seguito Codice);

d) in particolare, l'art. 4, paragrafo 1, n. 7) del Regolamento, individua il Titolare del trattamento ne *"la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali […]"* e che l'art. 4, paragrafo 1, n. 8) del Regolamento, identifica il Responsabile del trattamento ne *"la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento";*

e) l'art. 28, paragrafo 1 del Regolamento, prevede *che "qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato"*;

f) Svelto! dichiara di possedere adeguate competenze tecniche e risorse idonee circa gli scopi e le modalità di trattamento dei dati personali, delle misure di sicurezza da adottare al fine di garantire la loro riservatezza, la completezza e l'integrità, nonché diretta e completa conoscenza delle norme che disciplinano la protezione degli stessi;

g) con il presente Atto – che costituisce parte integrante e sostanziale del Contratto innanzi citato – l'Università degli Studi di Messina_____(*denominazione dell'Ente*)_____, in qualità di Titolare del trattamento, intende nominare Svelto!, Responsabile del trattamento, ai sensi di quanto disposto dall'art. 28 del GDPR, in relazione all'erogazione dei Servizi forniti nell'ambito del rapporto contrattuale con il Titolare;

h) con la sottoscrizione del presente documento le Parti intendono regolare i reciproci rapporti in relazione al trattamento dei dati personali effettuato dal Responsabile del trattamento per conto del Titolare.

Tutto ciò premesso, da considerarsi parte integrante e sostanziale del presente atto, ai sensi dell'attuale normativa vigente, le Parti convengono e stipulano quanto segue

Art. 1- Oggetto

L'Università degli Studi di Messina_____, in qualità di Titolare del trattamento dei dati personali, nomina quale Responsabile del trattamento dei dati personali,

ai sensi e per gli effetti dell'art. 28 del Regolamento, Svelto!, con riferimento ai servizi forniti in virtù del Contratto – relativi alle modalità di autovalutazione e valutazione della produzione scientifica, indicate in tale contratto al punto 7) pag. 1 e 2,di cui il presente atto costituisce Addendum. La nomina viene espressamente accettata da Svelto! per mezzo del suo legale rappresentante che sottoscrive il presente atto per accettazione di tutte le sue parti, incluse le premesse, e, in particolare, di cui al punto f).

Con l'accettazione dell'incarico, Svelto! conferma la diretta e approfondita conoscenza degli obblighi che si assume e si impegna a procedere al trattamento dei dati personali attenendosi alle istruzioni ricevute dal Titolare attraverso la presente nomina o a quelle ulteriori che saranno conferite nel corso delle attività prestate in suo favore.

Art. 2 -Ambito di Trattamento

Il Responsabile è autorizzato a trattare, per conto del Titolare, i dati personali come descritto nell'allegato al presente atto di nomina.

Le finalità di trattamento, le categorie dei trattamenti, le categorie di interessati, i tipi di dati trattati, il periodo di conservazione e la descrizione generale delle misure di sicurezza adottate (se possibile) relativi ai diversi servizi erogati dal Responsabile, e gli specifici ed ulteriori obblighi a questi connessi, sono definiti nell'allegato al presente atto di nomina.

3 -Obblighi generali del Responsabile

Per la durata del Contratto, il Responsabile nominato è tenuto a trattare i dati personali solo ed esclusivamente ai fini della fornitura dei suddetti servizi, nel rispetto di quanto disposto dalla normativa applicabile e vigente in materia di protezione dei dati personali, nonché delle istruzioni del Titolare riportate nei successivi punti, e di ogni altra indicazione scritta che potrà essergli dallo stesso fornita, nei limiti delle prestazioni contrattualmente dovute in suo favore.

Il Responsabile, nei limiti delle prestazioni contrattualmente dovute, si impegna nei confronti del Titolare all'osservanza dei seguenti obblighi:

a) **Rispetto della normativa**. Trattare i dati personali, nel rispetto dei princìpi e delle disposizioni previsti dal Codice, dal Regolamento, dagli indirizzi e dai provvedimenti a carattere generale emanati dal Garante in materia di protezione dei dati personali e da ogni altra vigente normativa in materia di protezione dei dati personali.

b) **Divieto di trasferimento dei dati personali gestiti per conto del Titolare**. Non trasferire, né in tutto né in parte, in un Paese terzo o a un'organizzazione internazionale che siano al di fuori del territorio dello Spazio Economico Europeo (SEE) i dati personali trattati ai sensi del Contratto, senza la previa autorizzazione del Titolare. Nel trattare i dati personali per conto del Titolare, attenersi alle istruzioni documentate fornite dal Titolare stesso, anche in caso di eventuale trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o la normativa nazionale; in tal caso, il Responsabile si impegna a informare il Titolare circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico.

c) **Rispetto delle istruzioni impartite dal Titolare**. Sono considerate istruzioni documentate le prescrizioni previste dal Contratto, dagli eventuali suoi allegati e dalla presente nomina.

d) **Dovere di cooperazione.** Informare immediatamente il Titolare se ritenga che un'istruzione impartita dal Titolare comporti una violazione delle disposizioni del GDPR o, più in generale, della Legge Applicabile.

e) **Sicurezza.** Adottare tutte le misure di sicurezza di cui all'art. 32 del Regolamento. Nel caso in cui il trattamento, per la propria natura, il contesto e/o le tecnologie utilizzate, necessitasse di una valutazione d'impatto sulla protezione dei dati e/o evidenziasse la necessità di approntare ulteriori misure di sicurezza, il Titolare potrà richiedere al Responsabile la collaborazione nella conduzione della valutazione d'impatto e/o l'implementazione di tali misure. Nei casi in cui si evidenziasse una non piena corrispondenza tra la tipologia di trattamento prevista dal Contratto e le misure di sicurezza richieste, il Responsabile si impegna a comunicarlo per iscritto al Titolare, fornendo al medesimo l'effettuata analisi del rischio e indicando le misure di sicurezza ritenute adeguate;

f) **Riservatezza**. Garantire la riservatezza dei dati personali trattati e, in particolare, che l'accesso ai dati personali sia limitato alle sole persone autorizzate al trattamento che abbiano ricevuto le istruzioni idonee allo scopo e siano vincolate alla riservatezza o abbiano un obbligo legale di riservatezza su tutte le informazioni acquisite nello svolgimento della loro

attività, anche per il periodo successivo alla cessazione del rapporto di lavoro o collaborazione.

g) **Sub-Responsabili**. Procedere, se necessario, alla nomina di un altro Responsabile del trattamento (il c.d. "Sub-Responsabile del trattamento") per gestire attività di trattamento specifiche. In questo caso, il Responsabile dovrà informare il Titolare, mediante una comunicazione scritta, di eventuali modifiche comportanti la nomina, l'aggiunta o la sostituzione di eventuali Sub-Responsabili del trattamento e, in particolare, dovrà indicare chiaramente le attività di trattamento delegate, l'identità e i dati di contatto del Sub-Responsabile del trattamento ed i contenuti del contratto sottoscritto con quest'ultimo, dandone comunicazione, entro 15 giorni dalla data di sottoscrizione, al Titolare che ha facoltà di opporsi a tali modifiche entro 15 giorni dal ricevimento di tale comunicazione. Il Titolare dovrà quindi sommariamente indicare al Responsabile le ragioni della sua opposizione. Qualora il Responsabile ritenga di non essere in grado di eseguire le prestazioni di cui al Contratto senza l'apporto del Sub-Responsabile del Trattamento, il Titolare avrà diritto di risolvere il Contratto, ed il presente Addendum, ai sensi e per gli effetti di cui all'art. 1456 c.c. In ogni caso, le Parti convengono che, nel caso di nomina di un Sub-Responsabile del trattamento:

- prima che il Sub-Responsabile del trattamento cominci a svolgere le attività di trattamento dei dati personali delegategli, il Responsabile dovrà svolgere un'accurata *due diligence* volta ad assicurarsi che il Sub-Responsabile del trattamento sia in grado di garantire il livello di protezione dei dati personali richiesto dal Contratto e dall'Addendum;
- al predetto Sub-Responsabile del trattamento dovranno essere imposti, mediante la stipulazione di un contratto o di un altro atto giuridico vincolante, i medesimi obblighi in materia di protezione dei dati personali stabiliti in questo Addendum e, in particolare, garanzie sufficienti a mettere in atto misure tecniche e organizzative adeguate affinché il trattamento soddisfi i requisiti del GDPR;
- qualora il Sub-Responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile sarà integralmente responsabile nei confronti del Titolare dell'adempimento degli obblighi da parte del Sub-Responsabile.

Alla data di sottoscrizione del presente accordo, le parti si danno reciprocamente atto che il Responsabile si avvale dei seguenti sub-responsabili, con i quali s'impegna a concludere accordi contrattuali conformi al dettato dell'art. 28, par. 4 GDPR:

Sub-responsabile	**Attività di trattamento delegata**
Google Cloud – Data Center Europe West 1 - Belgium	fornitura dei servizi cloud per l'esercizio della piattaforma https://cloud.google.com/privacy/gdpr L'elenco dei subresponsabili è disponibile a questo indirizzo: https://cloud.google.com/terms/subprocessors

h) **Diritti degli Interessati**. Tenuto conto della natura del trattamento, assistere il Titolare con misure tecniche e organizzative adeguate, al fine di soddisfare l'obbligo del Titolare di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III del GDPR). Nell'ipotesi in cui gli interessati presentino richiesta per l'esercizio dei suddetti diritti al Responsabile, quest'ultimo dovrà entro 10 giorni dal ricevimento, inoltrare detta richiesta e le eventuali osservazioni, per posta elettronica al Titolare, utilizzando il seguente indirizzo mail di contatto del Responsabile per la Protezione dei Dati dell'Istituzione:

Indirizzo e-mail: rpd@unime.it**;**

Indirizzo PEC: protezionedati@pec.unime.it .

i) **Cooperazione in caso di Data Breach e redazione di DPIA**. Assistere il Titolare nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR e, pertanto, nella elaborazione e nell'attuazione delle misure di sicurezza, nella notifica e nella comunicazione dei data breach, nella redazione della DPIA e nella consultazione preventiva, tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile del Trattamento.

k) **Cessazione del Trattamento**. Cancellare/distruggere o restituire al Titolare (secondo quanto lo stesso deciderà e comunicherà al Responsabile di volta in volta) tutti i dati personali dopo la cessazione della prestazione dei servizi relativi al trattamento e cancellare/distruggere le copie esistenti, documentandone per iscritto l'intervenuta

cancellazione/distruzione, salvo che la normativa applicabile preveda la conservazione dei dati.

l) **Audit**. Mettere a disposizione del Titolare, dietro richiesta dello stesso, tutta la documentazione e le informazioni necessarie per dimostrare il rispetto degli obblighi stabiliti dall'art. 28 del GDPR e dal presente Addendum e consentire e contribuire allo svolgimento delle attività di revisione, comprese le ispezioni, realizzate dal Titolare o da un altro soggetto da questi incaricato. Le risultanze dell'audit saranno discusse in buona fede tra le Parti e il Responsabile si impegna sin d'ora ad attuare gli eventuali cambiamenti ritenuti necessari dal Titolare in seguito all'audit, al fine di garantire la conformità alla Legge Applicabile e all'Addendum.

m) **RPD/DPO**. Comunicare al Titolare del trattamento il nome ed i dati del proprio Responsabile della Protezione dei Dati, ai sensi dell'art. 37 del GDPR.

Responsabile Protezione Dati: Dott. Marcello Buoncristiano

e-mail: privacy@svelto.tech

n) **Registro delle attività di trattamento**. Nell'ambito delle responsabilità così affidategli, e nel rispetto delle relative istruzioni, al Responsabile incomberà l'obbligo di tenere costantemente aggiornato presso di sé, ed a disposizione in ogni momento del Titolare, un registro di tutte le categorie di attività relative al trattamento svolte per conto del Titolare, ai sensi dell'art. 30 del GDPR, in forma scritta, anche in formato elettronico. Allo stesso Responsabile competerà, in via esclusiva, l'obbligo di predisporre ed eseguire una periodica attività di verifica interna sull'operato dei propri eventuali sub-responsabili ed autorizzati al trattamento.

o) **Cooperazione nel corso delle ispezioni del Garante o dell'Autorità Giudiziaria**.

- Il Responsabile si impegna altresì a collaborare col Titolare in buona fede e nei limiti delle rispettive competenze, previa motivata richiesta scritta del Titolare, in caso di indagine svolta dalle su indicate Autorità.
- Informare tempestivamente il Titolare in merito ad ispezioni eseguite da parte del Garante Privacy o dell'Autorità Giudiziaria con riferimento ai Trattamenti dei dati personali.

Articolo 4 —Obblighi del Titolare del trattamento

L'Università dgli Studi di Messina_____, quale Titolare del trattamento, è tenuto a:

1) Fornire al Responsabile le informazioni ed i dati elencati nel presente Addendum, nonché ogni altra informazione utile per l'esecuzione delle attività di trattamento illustrate nello stesso;
2) Documentare per iscritto tutte le istruzioni impartite al Responsabile per il trattamento dei dati personali per conto del Titolare.

Articolo 5 – Violazione di dati personali ("Data Breach")

Il Responsabile si impegna, a decorrere dalla data di sottoscrizione del presente Addendum, ad informare tempestivamente il Titolare, per il tramite del RPD/DPO, di ogni violazione della sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita di dati personali o di loro aggiornamenti, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati, a prescindere da qualsiasi valutazione circa l'impatto e le conseguenze attese della violazione stessa, senza indugio e, in ogni caso, entro il tempo massimo di 24 ore dal momento in cui ne sia venuto a conoscenza utilizzando il seguente indirizzo PEC: protocollo@pec.unime.it _____, corredando detta comunicazione con ogni documentazione utile a consentire al Titolare di notificare, ove necessario, tale violazione al Garante e agli interessati nel rispetto delle tempistiche di cui all'art. 33 del GDPR.

La comunicazione dovrà, in ogni caso, contenere quantomeno i seguenti dettagli:

- la natura della violazione dei dati personali;
- la categoria degli interessati;
- il contatto presso cui ottenere più informazioni;
- i tempi trascorsi dall'incidente alla sua individuazione, ove determinabili;
- i tempi di presa in carico;
- indicazione della probabile causa della violazione;
- le conseguenze note o attese di tale violazione;
- la soluzione proposta;

- le misure che siano state già adottate per contenere e limitare le conseguenze della violazione.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
Il Responsabile garantisce sin d'ora che ogni informazione fornita a tal fine sarà completa, corretta e accurata.

Articolo 6- Valutazione d'impatto ("Data Protection Impact Assessment")

Il Responsabile s'impegna a fornire al Titolare ogni elemento utile all'effettuazione, da parte di quest'ultimo, della valutazione di impatto sulla protezione dei dati, qualora lo stesso sia tenuto ad effettuarla ai sensi dell'art. 35 del GDPR, nonché ogni collaborazione nell'effettuazione della eventuale consultazione preventiva al Garante ai sensi dell'art. 36 GDPR.
Nel caso in cui la valutazione d'impatto sulla protezione dei dati evidenziasse la necessità di approntare ulteriori misure di sicurezza, il Titolare potrà richiedere al Responsabile l'implementazione di tali misure.
Nei casi in cui si evidenziasse una non piena corrispondenza tra la tipologia di trattamento prevista dal Contratto e le misure di sicurezza richieste, il Responsabile si impegna a comunicarlo per scritto al Titolare fornendo al medesimo l'effettuata analisi del rischio e indicando le misure di sicurezza ritenute adeguate.

Articolo 7- Conseguenze della violazione delle disposizioni della Legge Applicabile da parte del Responsabile del Trattamento

Nel caso in cui dovesse violare le disposizioni della Legge Applicabile, determinando le finalità e i mezzi del trattamento, il Responsabile sarà considerato un autonomo Titolare del trattamento in questione, fatte salve le disposizioni del GDPR di cui all'art. 82 in tema di diritto al risarcimento e responsabilità, all'art. 83 in tema di condizioni generali per infliggere sanzioni amministrative pecuniarie e all'art. 84 in tema di sanzioni.

Articolo 8- Clausola di manleva

Il Responsabile assume piena responsabilità diretta verso gli interessati per i danni subiti derivanti da inadempimento o da violazione delle istruzioni legittime del Titolare nonché da mancato adempimento degli obblighi previsti dal GDPR e dalla Legge Applicabile.

Il Responsabile si impegna a manlevare e tenere indenne il Titolare da qualsiasi danno, pregiudizio, costo, spesa, onere che la stessa dovesse subire e/o dover risarcire a terzi a causa della violazione, da parte del Responsabile, o degli eventuali Sub-Responsabili da esso nominati, delle disposizioni della Legge Applicabile e delle istruzioni impartite dal Titolare.

Articolo 9- Clausola risolutiva espressa

Nel caso di inadempimento da parte del Responsabile ad uno degli obblighi stabiliti all'articolo 3 che precede nonché in caso di perdita da parte del Responsabile medesimo dei requisiti di cui all'art. 28 del GDPR, al Titolare è riconosciuta la facoltà di risolvere il Contratto, ai sensi dell'art. 1456 c.c., con revoca immediata della nomina in oggetto. Nelle ipotesi citate, la risoluzione si verifica di diritto, mediante comunicazione scritta con cui il Titolate dichiara al Responsabile che intende avvalersi della clausola risolutiva espressa, fatto salvo il diritto del Titolare medesimo alla manleva ed al risarcimento degli eventuali danni conseguenti all'inadempimento del Responsabile.

Articolo 10 — Durata della Nomina del Responsabile

La Nomina del Responsabile avrà la medesima durata del Contratto e, pertanto, cesserà al momento del completo adempimento o dello scioglimento del vincolo contrattuale, qualsiasi ne sia il motivo.

Articolo 11 — Cessazione del Trattamento

Il Responsabile, a seguito della cessazione del trattamento dei dati personali, sarà tenuto, a scelta del Titolare e sulla base delle istruzioni dallo stesso impartite, a:

(i) restituire al Titolare i dati personali trattati, oppure

(ii) provvedere alla loro integrale distruzione (eventuali copie comprese),

salvi solo i casi in cui la conservazione dei dati sia richiesta da norme di legge e/o altre finalità (contabili, fiscali, ecc.) o il caso in cui si verifichino circostanze autonome e ulteriori

che giustifichino la continuazione del trattamento dei dati da parte del Responsabile, con modalità limitate e per il periodo di tempo a ciò strettamente necessario. In tal caso il Responsabile dovrà indicare al Titolare i motivi ed i criteri di conservazione dei dati.

Articolo 12 – Compenso

Il presente Atto di nomina non comporta alcun diritto per il Responsabile a uno specifico compenso o indennità o rimborso per l'attività svolta, né ad un incremento del compenso spettante allo stesso in virtù delle relazioni contrattuali con il Titolare.

Articolo 13- Modifiche normativa privacy

Per quanto concerne i trattamenti che il Responsabile esegue per conto del Titolare in esecuzione del Contratto, il Titolare ha facoltà di rivedere le condizioni del presente Addendum, laddove la normativa subisse una significativa riforma. Nel caso di intervenute modifiche nella Legge Applicabile, le Parti si impegnano, sin d'ora, a prestare massima cooperazione per modificare o integrare il presente Addendum.

Articolo 14- Modalità sottoscrizione

Il presente Atto viene sottoscritto, in un unico originale, con firma digitale secondo le modalità previste dal D.lgs. n. 82/2005 e ss.mm.ii. "Codice dell'Amministrazione Digitale", relativamente all'invio di documenti in formato digitale attraverso l'utilizzo della casella PEC.

Articolo 15 - Legge applicabile e foro competente

Il presente Addendum e la sua interpretazione ed esecuzione sono regolate dalla Legge Italiana.

Qualsiasi controversia che dovesse sorgere in connessione o in relazione all'Addendum sarà devoluta alla cognizione esclusiva del Foro previsto nel Contratto.

Per tutto quanto non previsto dal presente Atto si rinvia alle disposizioni generali vigenti ed applicabili in materia di protezione dei dati personali.

Le Parti si danno reciprocamente atto che il presente Accordo e i relativi Allegati sono il risultato di una negoziazione e specifica condivisione tra di esse con riferimento ad ogni singola clausola e che, in considerazione di ciò, non trovano applicazione le disposizioni contenute all'articolo 1341 c.c.

Il Titolare del Trattamento	Il Responsabile del Trattamento
La Rettrice, prof. Giovanna Spatari	Maria Grazia Russo
Università degli Studi di Messina	Svelto! – Big Data Cleaning and Analytics Srl

ALLEGATO:

Elenco delle attività di trattamento dei dati personali effettuati dal Responsabile in favore del Titolare del Trattamento.

Denominazione del servizio: Piattaforma Criterium

https://criterium.svelto.tech, https://assistenza.criterium.svelto.tech

Categorie di Trattamenti Effettuati e Tipologie di Dati Trattati

I trattamenti sono finalizzati al calcolo di indicatori relativi alla produzione scientifica dei singoli e delle strutture di ricerca dell'Istituzione (dipartimenti, aree di valutazione, settori scientifico-disciplinari, settori concorsuali, o altri aggregati di soggetti individuati dall'Istituzione).

I modelli di valutazione implementati dal sistema sono quelli adottati dall'ANVUR nell'ambito delle procedure nazionali di valutazione della ricerca (nel seguito denominati "modelli di valutazione di riferimento"), come segue:

a. Modello di valutazione della VQR (Legge 11 dicembre 2016, n. 232) e successive evoluzioni.
b. Modello dell'Abilitazione Scientifica Nazionale (ASN) (Art. 16 della Legge 240/2010. Decreto del Presidente della Repubblica 04/04/2016 n. 95. Decreto Ministeriale 07/06/2016 n.120), e successive evoluzioni.

Il sistema produce il calcolo di indicatori relativi alla produzione scientifica dei singoli interessati, applicando le classificazioni previste dai suddetti modelli inclusa l'attribuzione di indicatori di posizionamento della produzione scientifica di ciascun interessato rispetto al complesso dei soggetti valutati dal sistema a livello nazionale, e la verifica del possesso dei requisiti per le qualifiche previste per l'Abilitazione Scientifica Nazionale (ASN)

I trattamenti effettuati e le categorie di dati trattati sono elencati di seguito:

- Acquisizione, conservazione ed elaborazione dei seguenti dati personali relativi agli utenti del sistema: nome, cognome, istituzione di appartenenza, qualifica, settore-scientifico disciplinare, settore concorsuale, struttura dipartimentale di appartenenza, indirizzo di posta elettronica, codice fiscale (allo scopo di anonimizzazione e conservazione di un hash crittografico).
- Se l'Istituzione adotta l'archivio istituzionale dei prodotti della ricerca IRIS acquisizione, conservazione ed elaborazione dei seguenti metadati dall'archivio istituzionale dell'Istituzione di appartenenza utilizzando le credenziali fornite dall'Istituzione:
    - metadati dei prodotti della ricerca dei soggetti valutati, acquisiti;

    - dati anagrafici (nome, cognome, istituzione di appartenenza, qualifica, settore-scientifico disciplinare, settore concorsuale, struttura dipartimentale di appartenenza, indirizzo di posta elettronica codice fiscale (allo scopo di anonimizzazione e conservazione di un hash crittografico) e del codice identificativo del soggetto (CRIS ID).
- Se l'Istituzione non adotta l'archivio istituzione dei prodotti della ricerca IRIS: acquisizione, conservazione ed elaborazione dei metadati dei prodotti della ricerca dei soggetti forniti dall'Istituzione in formato elettronico.
- Acquisizione, conservazione ed elaborazione dei dati bibliometrici (es: numero di citazioni ricevute) relativi ai prodotti della ricerca dei soggetti, acquisiti dai database Scopus (http://www.scopus.com) e WOS (http://app.webofknowledge.com), utilizzando credenziali di accesso fornite dall'Istituzione.
- Calcolo di indicatori relativi ai soggetti valutati sulla base dei modelli di valutazione di riferimento adottati dal sistema; ad esempio: per il modello VQR: classi dei prodotti, numero di prodotti, anche per classe e per tipologia; per il modello ASN: valori degli indicatori ASN per i settori bibliometrici e non bibliometrici, superamento o meno delle soglie per le qualifiche di associato, di ordinario e di commissario, scostamenti rispetto alle soglie; percentile degli indicatori ASN rispetto ai soggetti dello stesso settore concorsuale.
- Calcolo di indicatori aggregati relativi alle aggregazioni di soggetti dell'Istituzione – dipartimenti, aree, settori scientifico-disciplinari, settori concorsuali e combinazioni di questi, nonché aggregati arbitrari definiti dagli utenti – sulla base dei modelli di valutazione di riferimento; ad esempio: numero di prodotti, anche per classe e per tipologia, distribuzione dei prodotti rispetto alle classi di merito del modello della VQR, anche in relazione al complesso delle istituzioni che adottano il sistema.
- Calcolo di indicatori standardizzati di performance (ISP) relativi alle aggregazioni di soggetti dell'Istituzione – dipartimenti, aree, settori scientifico-disciplinari, settori concorsuali e combinazioni di questi.
- Generazione e conservazione di report relativi ai dati e agli indicatori delle strutture.
- Generazione e conservazione di report relativi alle acquisizioni dei metadati dei soggetti e dei prodotti, allo scopo di segnalare possibili anomalie e migliorare la qualità dei dati.
- Token tecnici di tipo JWT (JSON Web Tokens), utilizzati esclusivamente allo scopo di gestione delle sessioni applicative.
- Generazione e conservazione di log delle sessioni applicative, utilizzati esclusivamente per finalità tecniche (analisi della sicurezza e delle prestazioni del sistema).

In nessun caso gli interessati saranno sottoposti a decisioni basate unicamente sui trattamenti automatizzati condotti dal sistema che producano effetti giuridici che li riguardano o che incidano in modo analogo significativamente sulla loro persona.
Il periodo di conservazione dei dati personali è limitato alla durata di 1 anno.
Non è previsto il trattamento di dati personali appartenenti a categorie particolari (ad esempio dati genetici, dati biometrici, dati relativi alla salute, ecc.) o dati relativi a condanne penali e reati.

Politiche di Protezione dei Dati

La piattaforma Criterium è stata sviluppata da Svelto! con un approccio di tipo “privacy by design” e “privacy by default”, in modo da essere completamente allineata alle prescrizioni della normativa sul trattamento dei dati e da fornire al Titolare tutti gli strumenti per consentire la corretta implementazione delle politiche di privacy.

Provider di Servizi Cloud e Parametri Tecnici di Sicurezza

I dati e l’applicativo saranno ospitati su datacenter con sede in Europa della Google Cloud Platform (GCP), piattaforma certificata rispetto alla normativa vigente sulla privacy, ed in particolare rispetto al GDPR (https://cloud.google.com/privacy/gdpr).
La piattaforma Criterium è sviluppata utilizzando tecnologie “cloud native” e “container based” e quindi non fa uso di macchine virtuali tradizionali. Sulle eventuali macchine virtuali necessarie per il dispiegamento del servizio aggiuntivi (ad esempio il servizio di assistenza clienti) girerà un firewall sul quale sarà aperto il numero minimo di porte. L’accesso da remoto alle macchine sarà consentito solo attraverso l’utilizzo di crittografia a chiave pubblica.
Tutte le transazioni (scambio di dati tra i client e il server) relative all'applicativo avverranno utilizzando il protocollo di crittografia HTTPS.
Per l’accesso alle macchine virtuali e al DB verranno usate password con requisiti stringenti di robustezza.

Gestione degli Utenti, degli Accessi e delle Password

Tutte le password saranno salvate attraverso hash basati su crittografia forte.
Per tutti gli utenti sono imposti criteri minimi di robustezza in fase di scelta della password.
Per tutti gli utenti:

- Le password devono contenere almeno una lettera maiuscola, almeno una minuscola e almeno una cifra e contenere almeno 10 caratteri.
- La scadenza delle password è fissata a 90 giorni. Dopo quella data il sistema obbliga l’utente a cambiare la password prima di accedere.

- Viene mantenuta la storia (degli hash) delle ultime 10 password utilizzate, e viene impedito di riutilizzare una di queste.
- È disponibile un servizio per la notifica via e-mail dei login effettuati con l'utenza associata. Il servizio potrà essere abilitato o disabilitato accedendo alla pagina del proprio profilo. Sarà abilitato per default per gli amministratori delle istituzioni.

Il sistema adotterà un sistema di registrazione (logging) degli accessi, per intercettare eventuali tentativi di intrusione. L'account di un utente verrà bloccato nel caso in cui tenti senza successo di effettuare il login più di 10 volte nell'arco di 10 minuti. In questo caso, per riattivare l'account l'utente dovrà necessariamente effettuare la procedura di modifica della password.

Scambio dei File e Produzione dei Report

I dati relativi alle anagrafiche dei soggetti valutati, che contengono dati personali, tra cui i codici fiscali degli interessati, vengono forniti dagli Atenei. I codici fiscali vengono trattati per il tempo minimo indispensabile all'acquisizione ed eventuale pseudonimizzazione dei dati (trasformazione del codice fiscale nel suo hash crittografico).

Allo scopo di favorire il miglioramento della qualità dei dati, nel corso delle tornate di valutazione, dopo ciascuna acquisizione viene fornito agli Atenei un report delle anomalie riscontrate nei metadati acquisiti.

Il sistema genera report degli indicatori in formato Excel. Tutti i file Excel che contengono dati estratti dal sistema sono protetti con password robuste univocamente associate agli utenti che generano il report stesso.

I file contenenti le anagrafiche, i report delle anomalie e i report degli indicatori generati dal sistema vengono trattati per le finalità del sistema dagli incaricati dei trattamenti sui loro personal computer. Tutti gli incaricati utilizzano computer di ultima generazione configurati con crittografia del disco e password robuste per l'accesso.

Sicurezza della Piattaforma Cloud e Disaster Recovery

L'infrastruttura cloud utilizzata ha un livello di servizio garantito pari al 99,999% del tempo.

In aggiunta, verranno effettuati backup periodici del contenuto del database, salvati utilizzando servizi di memorizzazione cloud ad altissima affidabilità in formato crittografato.

Allo scopo di migliorare ulteriormente la sicurezza dei sistemi e dei dati, verranno messe in atto le seguenti misure:

- Adozione di un sistema di riconoscimento delle intrusioni ("intrusion detection system").
- Utilizzo di uno strumento di "vulnerability assessment".