Agreement _generale

Nomina di Responsabile del trattamento di dati personali
Ai sensi dell'art. 28 del GDPR - General Data Protection Regulation

L'ente ESU A.r.s.d.u. di Padova, con sede a Padova in Via San Francesco n.122, (di seguito anche la "**Amministrazione**" o il "**Titolare**"), in persona legale rappresentante *pro tempore*, in relazione al contratto sottoscritto con …… ……i CF: ……. (d'ora innanzi il "**Contratto**"), concernente lo svolgimento SERVIZIO DI RISTORAZIONE CONVENZIONATO PER GLI STUDENTI DELL'UNIVERSITÀ DI PADOVA. CIG: 95596508BC (di seguito l'"**Attività**"), con la presente lettera

(COMPILARE LE PARTI IN GIALLO)

Nomina

……. Partita IVA ……, con sede legale in via ……

RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI (di seguito il "**Responsabile**")

Le incombenze e le responsabilità oggetto della presente lettera di nomina vengono affidate al Responsabile sulla base delle dichiarazioni dallo stesso fornite alla Amministrazione (e della successiva verifica da parte della Amministrazione, per quanto ragionevolmente possibile, della loro rispondenza al vero) circa le caratteristiche di esperienza, capacità e affidabilità che vengono richieste dalla legge (artt. 28 GDPR) per chi esercita la funzione di Responsabile del trattamento. Con la sottoscrizione della presente lettera, il Responsabile si dichiara disponibile e competente per la piena attuazione di quanto ivi disposto, accetta la nomina, conferma la diretta ed approfondita conoscenza degli obblighi che assume in relazione al dettato del GDPR, conferma, altresì, di disporre di una propria organizzazione che dichiara idonea a consentire il trattamento dei dati nel pieno rispetto delle prescrizioni legislative, ivi compreso il profilo della sicurezza, e si impegna a procedere al trattamento dei dati personali attenendosi alle istruzioni impartite nel pieno rispetto di quanto imposto dall'art. 28, lettera a) del GDPR.

Onde consentire al Responsabile di espletare i compiti e le attribuzioni meglio specificati in seguito, con la presente lettera di nomina vengono fornite le specifiche istruzioni per l'assolvimento del compito assegnato.

1. <u>Definizioni</u>. I seguenti termini utilizzati nella presente Nomina avranno i seguenti significati:

a. "**Normativa applicabile**": indicano l'insieme delle norme rilevanti in materia di privacy alle quali il Titolare è soggetto incluso (i) il Regolamento europeo 2016/679 in materia di protezione dei dati personali (General Data Protection Regulation – di seguito "**GDPR**"); (ii) per quanto residualmente applicabile, il D.Lgs. 196/2003 – così come modificato dal D.Lgs 101/2018, di seguito il "**Codice**"; (iii) in ogni tempo, ogni linea guida, norma di legge, codice o provvedimento rilasciato o emesso dagli organi competenti o da altre autorità di controllo.

b. "**Titolare del trattamento**", "**responsabile del trattamento**", "**interessato**", "**dati personali**" e "**trattamento**" hanno il significato dato dalla Normativa applicabile.

c. **"Misure tecniche e organizzative di sicurezza":** sono le misure intese a proteggere i dati personali dalla distruzione accidentale o illegale o dalla perdita, alterazione, divulgazione o accesso non autorizzato, in particolare quando il trattamento comporta la trasmissione di dati su una rete, come previste dalla Normativa applicabile all'art.32 GDPR e tutte le ulteriori misure tecniche ed organizzative necessarie a garantire un livello di sicurezza adeguato al rischio, tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento posto in essere, come del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche. Queste misure dovranno includere:

-la pseudonimizzazione e la cifratura dei dati personali;

-la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

-la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

-una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

d. **"Data breach"**: si intende l'ipotesi in cui si verifica una violazione dei dati personali secondo l'art. 33 GDPR.

e. **"Garante"**: si intende l'autorità competente responsabile per la protezione dei dati.

f. **"Sub-responsabile/i":** si intende qualsiasi responsabile del trattamento incaricato dal (i) Responsabile o (ii) da qualsiasi altro "sub-responsabile" di trattare dati personali per conto del Responsabile, sempre in conformità alle istruzioni del Titolare.

2. Misure tecniche ed organizzative -Audit e diritti di verifica del Titolare del Trattamento

Il Responsabile del Trattamento si obbliga ad adottare ed implementare le Misure tecniche ed organizzative di sicurezza, oltre a quanto previsto dall'art. 4 con l'obbligo di documentarle se richiesto dal Titolare del Trattamento.

Il Titolare si riserva la facoltà di effettuare, nei modi ritenuti più opportuni, verifiche tese a vigilare sulla puntuale osservanza delle disposizioni di legge e delle presenti istruzioni.

In alternativa a quanto sopra precisato, il Responsabile può fornire al Titolare copie delle relative certificazioni esterne (es. ISO 27001: 2013, SSAE 16 ecc.), audit, report e/o altra documentazione sufficiente per il Titolare a verificare la conformità del Responsabile alle Misure tecniche e organizzative di sicurezza della presente Nomina.

3. Correzioni, cancellazione o blocco di dati

Il Responsabile può correggere, cancellare o bloccare il trattamento dei dati personali solo su richiesta del Titolare del Trattamento.

Alla scadenza dell'Accordo il Responsabile di obbliga a garantire la migrazione di tutti i dati in suo possesso al Titolare del Trattamento.

4. Istruzioni generali del Responsabile del Trattamento

Il Responsabile, sebbene non in via esaustiva, avrà i compiti e le attribuzioni di seguito elencate, oltre agli ulteriori obblighi previsti al successivo articolo 5, e dunque dovrà:

1. effettuare la ricognizione delle banche dati, degli archivi (cartacei e non) relativi ai trattamenti effettuati in esecuzione dell'Attività;

2. tenere un registro, come previsto dall'art. 30 del GDPR, in formato elettronico, di tutte le categorie di attività relative al trattamento svolte per conto della Amministrazione, contenente:

   - il nome e i dati di contatto del Responsabile e del Titolare e, laddove applicabile, del Responsabile della protezione dei dati;

   - le categorie dei trattamenti effettuati per conto del Titolare;

   - ove possibile, una descrizione generale delle misure di sicurezza tecniche ed organizzative adottate;

3. organizzare le strutture, gli uffici e le competenze necessarie e idonee a garantire il corretto espletamento dell'Attività;

4. astenersi dal trattare i dati per finalità diverse da quelle oggetto dell'Attività e non diffonderli a terzi ;

5. garantire l'affidabilità degli autorizzati al trattamento dei dati personali del Titolare ed assicurare, inoltre, che gli stessi abbiano ricevuto adeguate istruzioni e formazione con riferimento alla protezione e gestione dei dati personali;

6. tenere i dati personali trattati attraverso l'Attività e di cui è titolare la Amministrazione separati rispetto a quelli trattati per conto di altre terze parti, sulla base di un criterio di sicurezza di tipo logico;

7. **procedere alla nomina del proprio/i amministratore/i di sistema, in adempimento di quanto previsto dal provvedimento del Garante del 27.11.08, pubblicato in G.U. n. 300 del 24.12.2008, ove ne ricorrano i presupposti, comunicandolo prontamente al Titolare, curando, altresì, l'applicazione di tutte le ulteriori prescrizioni contenute nel suddetto provvedimento;**

8. assistere tempestivamente il Titolare con misure tecniche e organizzative adeguate, al fine di soddisfare l'obbligo del Titolare di procedere ad un DPIA (Valutazione di impatto sulla protezione dei dati) ex art. 35 e ss del GDPR, con obbligo di notifica quando venga a conoscenza di un trattamento di dati che possa comportare un rischio elevato;

9. assistere il Titolare nel garantire il rispetto degli obblighi di cui agli artt. 32-36 GDPR, tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile e garantire l'esercizio del diritto alla portabilità dei dati personali trattati attraverso l'Attività, ai sensi dell'art. 20 del GDPR, assicurando che gli stessi possano essere trasmessi in un formato strutturato, di uso comune e leggibile da qualsiasi dispositivo automatico;

10. notificare alla Amministrazione, senza ingiustificato ritardo e comunque non oltre le 24 ore da quando ne abbia avuto conoscenza, ai sensi dell'art.33 del GDPR, nel caso in cui si verifichi un *Data breach* anche presso i propri Sub-responsabili; la notifica deve contenere tutti i requisiti previsti dall'art. 33, 3° comma del GDPR (la natura delle violazioni, gli interessati coinvolti, le possibili conseguenze e le nuove misure di sicurezza implementate). Dovrà, inoltre, adottare, di concerto con la Amministrazione, nuove misure di sicurezza atte a circoscrivere gli effetti negativi dell'evento e a ripristinare la situazione precedente;

11. predisporre e aggiornare un registro che dettagli, in caso di eventuali *Data breach*, la natura delle violazioni, gli interessati coinvolti, le possibili conseguenze e le nuove misure di sicurezza implementate;

12. avvertire prontamente l'Amministrazione**,** entro tre (3) giorni lavorativi, in merito alle eventuali richieste degli interessati che dovessero pervenire al Responsabile inviando copia delle istanze ricevute all'indirizzo e-mail: esu@cert.esu.pd.it e collaborare al fine di garantire il pieno esercizio da parte degli interessati di tutti i diritti previsti dalla Normativa applicabile;

13. avvisare immediatamente, e comunque entro tre (3) giorni lavorativi, il Titolare del trattamento, di qualsiasi richiesta o comunicazione da parte dell'Autorità Garante o di quella Giudiziaria eventualmente ricevuta inviando copia delle istanze all'indirizzo e-mail: esu@cert.esu.pd.it (da verificare) per concordare congiuntamente il riscontro;

14. predisporre idonee procedure interne finalizzate alla verifica periodica della corretta applicazione e della congruità degli adempimenti posti in essere ai sensi della Normativa applicabile, attuate in accordo con il Titolare anche in applicazione delle Misure tecniche e organizzative di sicurezza;

15. mantenere un costante aggiornamento sulle prescrizioni di legge in materia di trattamento dei dati personali, nonché sull'evoluzione tecnologica di strumenti e dispositivi di sicurezza, modalità di utilizzo e relativi criteri organizzativi adottabili;

16. ottemperare tempestivamente alle richieste del Titolare;

17. inviare tutte le comunicazioni al Titolare previste nel presente atto all'indirizzo soprariportato o a quello diverso che verrà eventualmente comunicato;

5. Ulteriori obblighi del Responsabile

Il Responsabile del trattamento, compatibilmente con quanto previsto dalla presente Nomina ed in conformità con le previsioni dell'art.28 del GDPR, sarà altresì soggetto all' obbligo di riservatezza; a tal fine ogni persona che abbia accesso ai dati personali appartenenti al Titolare del trattamento, nell'ambito della presente Nomina, si impegna a mantenere la riservatezza.

6. Responsabilità

Il Responsabile tiene indenne e manlevato il Titolare (inclusi i dipendenti) da ogni perdita, costo, spesa, multa e/o sanzione, danno e da ogni responsabilità di qualsiasi natura (sia essa prevedibile, contingente o meno) derivante da o in connessione con una qualsiasi violazione da parte del Responsabile degli obblighi della Normativa applicabile o delle disposizioni contenute nella presente Nomina.

7. Miscellanea

I dati devono essere trattati ed utilizzati esclusivamente nel territorio di uno Stato Membro dell'Unione Europea (EU) o di altro firmatario della presente Nomina nell'Area Economica Europea (AEE).

8. Durata - Legge e foro competente

La Nomina decorre dalla data della sua sottoscrizione e rimarrà in vigore sino alla risoluzione del Contratto.

Le parti stabiliscono le seguenti **persone di contatto** per l'esecuzione della nomina:

Per il Titolare del Trattamento: dott. Marco Bonato

Per il Responsabile esterno del Trattamento: ……

Qualsiasi modifica relativa le sopramenzionate persone o la responsabilità delle persone di contatto deve essere immediatamente notificata all'altra parte.

***

Sottoscrivendo la presente Nomina per accettazione, il Responsabile dichiara di aver compiutamente e analiticamente esaminato i trattamenti gestiti dalla Amministrazione e di averli trovati non in contrasto con le disposizioni della Normativa applicabile.

Il Responsabile esterno	Il Titolare
……	Gabriele Verza
Firmato digitalmente	*Firmato Digitalmente*