

**Accordo di nomina a responsabile del trattamento
ex art. 28 del Regolamento generale sulla protezione dei dati (Reg. UE 2016/679)**

Questo accordo di nomina a responsabile del trattamento (di seguito, “**Nomina**”) fa riferimento al contratto
tra

La società Acadevmy srl, con sede legale in San Giovanni la Punta alla Via Alessandro Manzoni snc - 95037, P. IVA 05537900879 in persona del legale rappresentante *pro tempore* (di seguito, nei limiti della presente Nomina, il “Titolare”);

e

La società [...], con sede legale in _____, Via _____, rappresentata da _____ in qualità di _____ (di seguito, nei limiti della presente Nomina, o “il Responsabile”);

avente ad oggetto

la messa a disposizione di una piattaforma informatica per la raccolta di dati relativi ... del Titolare, stipulato in data _____ (di seguito “il Contratto Principale”).

(nei limiti di questa Nomina, il Titolare e il Responsabile sono congiuntamente definiti “le Parti”).

Premesso che

- A. la Titolare è titolare del trattamento di dati personali ai sensi del Regolamento generale sulla protezione dei dati (Reg. UE 2016/679), di seguito “RGPD”, e ritiene di avvalersi di un soggetto terzo che effettui per suo conto alcune operazioni di trattamento dei dati personali;
- B. il Responsabile è soggetto che dichiara di presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento del Titolare soddisfi i requisiti del RGPD e garantisca la tutela dei diritti degli interessati;

si conviene quanto segue:

1 Designazione

- 1.1 Con il presente accordo, di cui le premesse e gli allegati sono parte fondamentale, la Titolare nomina il Responsabile, che accetta, responsabile del trattamento dei dati personali ai sensi dell’art. 28 del RGPD.
- 1.2 Con il presente documento le Parti disciplinano i termini e le condizioni per la prestazione dei servizi relativi al trattamento cui, in relazione al Contratto Principale e in ottemperanza al RGPD, il Responsabile del Trattamento è tenuto, in maniera che quest’ultimo sia vincolato a rispettare le istruzioni impartite dal Titolare, in particolare in relazione alle finalità, alla natura e alle modalità del trattamento.

2 Definizioni

- 2.1 I termini utilizzati in questa Nomina hanno il significato precisato in questa Nomina.
- 2.2 Gli altri termini con iniziale maiuscola non definiti altrimenti hanno il significato ad essi attribuito dalle Parti nell'ambito del Contratto Principale.
- 2.3 Ai fini della presente Nomina, i termini e le espressioni di seguito indicati avranno il seguente significato:
 - “**Dati Personali Attinenti**” significa qualsiasi Dato Personale trattato dal Responsabile del Trattamento per conto del Titolare in esecuzione o comunque in relazione al Contratto Principale e a questa Nomina;
 - “**Normativa Applicabile**” significa Normativa Europea sulla Protezione dei Dati e, se applicabili, le normative nazionali sulla protezione dei dati in ogni Stato terzo coinvolto nel Trattamento dei Dati Personali Attinenti;
 - “**Normativa Europea sulla Protezione dei Dati**” significa il RGPD, la normativa di attuazione, armonizzazione o sostituzione del RGPD, nonché le disposizioni nazionali di ogni Stato Membro che abbiano recepito la Direttiva UE 95/46/CE e che non siano state abrogate a seguito dell'entrata in vigore del RGPD;
 - “**Violazione della sicurezza**” significa qualsiasi fatto o atto che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

3 Trattamento dei Dati Personali Attinenti

- 3.1 La Titolare rimane l'esclusivo Titolare del Trattamento dei Dati Personali Attinenti e in ragione del Contratto Principale determina i Dati Personali che dovranno essere trattati dal Responsabile del Trattamento, le relative finalità e modalità del trattamento da parte del Responsabile del Trattamento. Istruzioni di trattamento specifiche per il Responsabile del Trattamento sono contenute nell'Allegato 1 di questa Nomina.
- 3.2 Il Responsabile del Trattamento dovrà limitarsi a processare i Dati Personali Attinenti per conto e a beneficio della Titolare, in conformità con le istruzioni ricevute dalla stessa e non avrà alcun diritto indipendente in relazione ad essi.
- 3.3 Il Responsabile del Trattamento dovrà immediatamente informare la Titolare se, a suo giudizio, alcuna delle istruzioni ricevute violi la Normativa Applicabile.
- 3.4 Il Responsabile del Trattamento non dovrà processare i Dati Personali Attinenti per finalità diverse da quelle impartite dalla Titolare, salvo espressa autorizzazione scritta della stessa o salvo che un siffatto Trattamento sia richiesto dalla Normativa Applicabile alla quale il Responsabile del Trattamento è soggetto, caso in cui il Responsabile del Trattamento dovrà informare la Titolare, nei limiti di quanto permesso dalla Normativa Applicabile.
- 3.5 Qualora il Responsabile del Trattamento avesse nominato un Responsabile della Protezione dei Dati, il Responsabile del Trattamento dovrà comunicare alla Titolare il nome e i dati di contatto del suo

Responsabile della Protezione dei Dati. Qualora il Responsabile del Trattamento non abbia nominato un Responsabile della Protezione dei Dati, il Responsabile del Trattamento dovrà comunicare il nome e i dati di contatto di un soggetto delegato da cui possono essere ottenute maggiori informazioni sul Trattamento.

- 3.6 La Titolare potrà apportare in qualsiasi momento modifiche ragionevoli all'Allegato 1, dandone comunicazione scritta al Responsabile del Trattamento.

4 Incaricati del Responsabile del Trattamento

- 4.1 Il Responsabile del Trattamento dovrà adottare le misure necessarie per garantire l'affidabilità di tutti gli incaricati che per suo conto avranno accesso ai Dati Personali Attinenti, assicurando in ogni caso che l'accesso sia strettamente limitato a quei soggetti che debbano conoscere o avere accesso ai Dati Personali Attinenti e solo quando effettivamente necessario all'esecuzione delle attività relative al Contratto Principale, nel rispetto della Normativa Applicabile relativa ai doveri di chi agisce sotto l'autorità del Responsabile del Trattamento.
- 4.2 Il Responsabile del Trattamento dovrà assicurare che le persone autorizzate a trattare i Dati Personali Attinenti ai fini del Contratto Principale e ai sensi di questa Nomina, incluso il proprio personale, si siano impegnate alla riservatezza o siano a ciò tenuti in forza di un obbligo di legge.
- 4.3 Il Responsabile del Trattamento dovrà garantire che i suoi dipendenti o collaboratori rispettino la Normativa Applicabile e ricevano un'adeguata formazione relativamente alle loro obbligazioni in merito al trattamento dei Dati Personali Attinenti.
- 4.4 Il Responsabile del Trattamento dovrà tenere traccia, in registri in formato elettronico, delle attività utili a provare il rispetto delle obbligazioni stabilite in questo articolo.

5 Sub-Responsabili del Trattamento

- 5.1 Il Responsabile del Trattamento non potrà comunicare alcun Dato Personale Attinente a terzi se non dopo aver provveduto a nominarlo sub-responsabile del Trattamento, con il preventivo ed esplicito consenso scritto della Titolare.

6 Sicurezza del Trattamento

- 6.1 Il Responsabile del Trattamento garantisce l'adozione delle misure tecniche ed organizzative necessarie a proteggere i Dati Personali Attinenti dalla perdita e contro qualsiasi forma di trattamento illecito o non autorizzato dei dati. Tali misure dovranno garantire un appropriato livello di sicurezza così come previsto dall'Articolo 32 del RGPD.
- 6.2 Nel valutare l'adeguato livello di sicurezza, il Responsabile del Trattamento tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso non autorizzato, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

6.3 Le misure che il Responsabile del Trattamento dovrà adottare dovranno almeno rispettare le misure di sicurezza descritte all'Allegato 2 di questa Nomina.

7 Trasferimento dei Dati Personali Attinenti

7.1 Il Responsabile del Trattamento non dovrà trasferire o trattare alcun Dato Personale Attinente all'infuori dello Spazio Economico Europeo (SEE) senza previo ed esplicito consenso del Titolare.

8 Riscontro alle richieste degli interessati

8.1 Tenendo conto della natura del trattamento, il Responsabile del Trattamento dovrà assistere con misure tecniche e organizzative adeguate la Titolare al fine di adempiere agli obblighi giuridici di quest'ultima, in particolare quello di dare seguito alle eventuali richieste per l'esercizio dei diritti dell'interessato.

8.2 Il Responsabile del Trattamento dovrà:

- a) dare notizia al Titolare immediatamente, e comunque non oltre 24 ore dalla ricezione da parte del Responsabile del Trattamento Approvato, di qualsiasi richiesta da parte di un interessato relativamente al trattamento di Dati Personali Attinenti ai sensi di qualsiasi Normativa Applicabile;
- b) garantire piena collaborazione e assistenza in relazione a qualsiasi richiesta di un interessato relativamente al trattamento di Dati Personali Attinenti;
- c) assicurarsi che il Responsabile del Trattamento non risponda a tali richieste, salvo i casi in cui ciò sia imposto da istruzioni documentate del Titolare o dalla Normativa Applicabile, nel qual caso il Responsabile del Trattamento dovrà, nei limiti di quanto permesso dalla Normativa Applicabile, informare la Titolare di tale disposizione di legge prima di rispondere alla richiesta;
- d) mantenere, in registri in formato elettronico, traccia delle richieste degli interessati per l'esercizio dei loro diritti. Detti registri devono includere una copia della richiesta, i dettagli delle informazioni e delle attività svolte dal Responsabile del Trattamento per rispondere alle richieste, nonché traccia di eventuale corrispondenza o chiamate telefoniche svolte per dare seguito alle richieste.

9 Registri delle attività di trattamento

9.1 In aggiunta ai registri previsti in questa Nomina, il Responsabile del Trattamento terrà un registro in formato elettronico delle attività di trattamento dei Dati Personali Attinenti ai sensi dell'art. 30 del RGPD.

9.2 La Titolare si riserva il diritto di visionare e verificare, in qualsiasi momento, i registri che il Responsabile del Trattamento è tenuto a tenere ai sensi della presente Nomina e di chiederne l'aggiornamento o l'integrazione ove ciò possa essere ritenuto ragionevolmente utile, a discrezione della Titolare, al fine degli adempimenti richiesti dalla Normativa Applicabile.

10 Violazione della sicurezza

- 10.1 Il Responsabile del Trattamento deve informare la Titolare senza ingiustificato ritardo, e comunque entro 12 ore dalla scoperta, di qualsiasi Violazione della sicurezza attinente ai Dati Personali Attinenti.
- 10.2 Il Responsabile del Trattamento dovrà fornire alla Titolare informazioni sufficienti a permettere alla stessa di adempiere ai suoi obblighi di (i) notifica all'autorità di controllo competente ai sensi dell'art. 33 del RGPD o della Normativa Applicabile e, ove necessario, di (ii) informare gli interessati ai sensi dell'art. 34 del RGPD o della Normativa Applicabile. Il Responsabile del Trattamento dovrà utilizzare il modello di segnalazione della violazione indicato quale Allegato 3 di questa Nomina, compilando detto modulo nella maniera più completa possibile e, comunque, precisando sempre almeno quanto segue:
- l'identità e i recapiti del responsabile della protezione dei dati eventualmente nominato, o di altro delegato cui richiedere maggiori informazioni;
 - la natura della Violazione della sicurezza relativa ai Dati Personali Attinenti, compresi le categorie e un numero approssimativo di interessati e di dati personali coinvolti;
 - le possibili conseguenze della Violazione della sicurezza relativa ai Dati Personali Attinenti;
 - una descrizione delle misure che il Responsabile del Trattamento Approvato, la Titolare hanno adottato o potrebbero adottare per porre rimedio alla Violazione della sicurezza o attenuarne i possibili effetti negativi.
- 10.3 Qualora e nella misura in cui non sia possibile fornire tutte le informazioni di cui all'art. 10.2 o all'Allegato 3 contestualmente, il Responsabile del Trattamento può fornire le informazioni in fasi successive senza ingiustificato ulteriore ritardo.
- 10.4 Il Responsabile del Trattamento dovrà collaborare con la Titolare e adottare tutte le ragionevoli misure richieste dalla stessa per assisterlo nello svolgimento delle indagini, nell'attenuazione e nell'individuazione dei rimedi per ogni Violazione della sicurezza relativa ai Dati Personali Attinenti.

11 Valutazione di impatto sulla protezione dei dati

- 11.1 Il Responsabile del Trattamento dovrà fornire ragionevole collaborazione e assistenza alla Titolare nello svolgimento di eventuali valutazioni dell'impatto dei trattamenti previsti sulla protezione dei Dati Personali Attinenti, tenendo conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, in particolare quando è previsto l'uso di nuove tecnologie, come previsto dall'art. 35 RGPD. La collaborazione e assistenza cui è tenuto il Responsabile del Trattamento è dovuta anche nella eventuale fase di consultazione preventiva con l'autorità di controllo.
- 11.2 Il Responsabile del Trattamento dovrà fornire ragionevole assistenza nell'adozione delle misure previste per affrontare i rischi, in particolare delle misure di sicurezza e dei meccanismi per garantire la protezione dei Dati Personali Attinenti e dimostrare la conformità al RGPD, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

12 Diritto di ispezione e verifica

- 12.1 Il Responsabile del Trattamento dovrà rendere disponibili su richiesta della Titolare tutte le informazioni necessarie a dimostrare di aver adempiuto a quanto previsto in questa Nomina, e dovrà permettere e

collaborare alle attività di ispezioni e verifica che la Titolare potrà effettuare, direttamente o attraverso soggetti incaricati, in relazione al trattamento dei Dati Personali Attinenti.

12.2 I costi per le attività di cui all'art. 12.1 sono a carico della Titolare.

12.3 Inoltre, il Responsabile del Trattamento dovrà, almeno una volta l'anno, testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del Trattamento dei Dati Personali Attinenti, riferendo per iscritto alla Titolare l'esito di tali verifiche.

12.4 I costi per le attività di cui all'art. 12.3 sono a carico del Responsabile del Trattamento, così come i costi necessari a porre rimedio ad eventuali irregolarità o inefficienze che dovessero risultare dalle attività di test, verifica e valutazione.

13 Durata e cessazione dei servizi relativi al trattamento

13.1 Le Parti concordano che la prestazione dei servizi qui disciplinati verrà meno in caso di scioglimento del Contratto Principale, qualunque ne sia la ragione, o di revoca della presente Nomina.

13.2 Alla cessazione della Nomina, il Responsabile del Trattamento dovrà interrompere le attività di trattamento dei Dati Personali Attinenti immediatamente, o entro il diverso termine ragionevolmente indicato dalla Titolare o entro quello che sia comunque utile a garantire la sicurezza dei Dati Personali Attinenti. In nessun caso, infatti, il Responsabile del Trattamento potrà agire in maniera da pregiudicare la sicurezza degli stessi.

13.3 Su scelta della Titolare, il Responsabile del Trattamento dovrà cancellare o restituire i Dati Personali Attinenti, salvo che la Normativa Applicabile preveda la conservazione degli stessi, in questo caso il Responsabile del Trattamento dovrà garantire la riservatezza dei Dati Personali Attinenti per tutto il tempo di conservazione, senza porre in essere altre attività di trattamento.

13.4 All'atto della cessazione di questa Nomina, il Responsabile del Trattamento compilerà e consegnerà firmato l'Allegato 4 di questa Nomina.

14 Diffida ad adempiere e manleva

14.1 Le Parti riconoscono espressamente che qualora il Responsabile del Trattamento venisse meno agli impegni previsti dalla Normativa Applicabile o comunque assunti con la presente Nomina, la Titolare potrà risolvere la presente Nomina previa diffida ad adempiere ai sensi dell'art. 1454 c.c.

14.2 Il Responsabile del Trattamento terrà indenne la Titolare da qualsiasi danno, pregiudizio, sanzione, costo o spesa che derivi da un inadempimento del Responsabile del Trattamento agli obblighi previsti dalla Normativa Applicabile o comunque assunti con la presente Nomina.

Questa Nomina ha effetto dalla data della sua sottoscrizione.

Sono parte integrante della Nomina i seguenti allegati:

- Allegato 1 – Istruzioni di trattamento;
- Allegato 2 – Misure di sicurezza;
- Allegato 3 – Modulo di segnalazione di Violazione dei dati;
- Allegato 4 – Dichiarazione di eliminazione.

TITOLARE

[Titolare del Trattamento]

Data: _____

Firma: _____

RESPONSABILE

[Responsabile del Trattamento]

Data: _____

Firma: _____

ALLEGATO 1

Istruzioni specifiche del Trattamento

Questo Allegato 1 contiene i dettagli sul Trattamento dei Dati Personali Attinenti in ottemperanza a quanto richiesto dall'art. 28, co. 3 del RGPD.

Oggetto e durata del Trattamento dei Dati Personali Attinenti

Il Trattamento dei Dati Attinenti ha ad oggetto tutte le attività necessarie o utili ad eseguire il Contratto Principale.

La Nomina avrà termine con il Contratto Principale, salvo eventuali proroghe contrattuali.

Natura e scopo del Trattamento dei Dati Personali Attinenti

Il Trattamento è finalizzato a consentire l'erogazione dei servizi oggetto del Contratto Principale.

Quanto alla natura del Trattamento, si riportano di seguito le specifiche dello stesso:

1. Provenienza del dato

- TITOLARE
- Interessati
- Soggetti terzi

2. Attività consentite

Tipo di attività	Consentita	Non consentita
Raccolta diretta del dato		X
Ricezione del dato da TITOLARE	X	
Registrazione del dato nei propri sistemi informatici o cartacei	X	
Modifica e/o aggiornamento autonomo (se non consentito, eventuali correzioni o aggiornamenti devono essere previamente confermati dal Titolare)		X

Trasformazione e/o organizzazione del dato		X
Comunicazione del dato a un destinatario		X
Diffusione del dato ad un pubblico indistinto		X
Utilizzo del dato per altro trattamento proprio		X
Limitazione alla conservazione del dato: <input type="checkbox"/> conservazione consentita per un massimo di ___ mesi/anni <i>oppure</i> <input checked="" type="checkbox"/> conservazione consentita fino al termine della Nomina o a revoca della stessa	salvo espresse indicazioni da parte del Titolare	
Limitazione del trattamento del dato (ad esempio, per revoca del consenso degli interessati)		X (inoltrare al Titolare eventuali richieste)
Cancellazione del dato		X
Altro (specificare) _____ _____ _____		

Autorizzazione generale a nominare sub-responsabili Sì No

(se sì, il Responsabile si impegna ad informare il Titolare di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare l'opportunità di opporsi a tali modifiche)

I tipi di Dati Personali Attinenti da trattare

Categorie di interessati: (gruppi di persone fisiche a cui i dati si riferiscono: ad esempio, beneficiari del servizio, minori, dipendenti, collaboratori, disabili, etc.)

Clienti, dipendenti, collaboratori interni ed esterni, fornitori, utenti potenziali,

Categorie di dati personali:

- Dati generici (ad esempio dati anagrafici, indirizzi email, numeri di telefono, etc.)
- Dati di rilevanza economica (ad esempio, coordinate bancarie, numeri di carte di credito, etc.)
indirettamente, in quanto sono autorizzati ad accedere al portale solo i soggetti in regola con i pagamenti dovuti al Settore Tecnico TITOLARE
- Dati appartenenti a categorie particolari (ad esempio, dati sulla salute, dati su orientamenti religiosi, politici, appartenenza etnica, etc.)
- Altre categorie di dati la cui violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà degli interessati (ad esempio, credenziali di accesso, codici identificativi, furto di identità, etc.)

Gruppi di incaricati del Responsabile del Trattamento che hanno accesso ai Dati Personali Attinenti:

Indicare gli uffici, i dipartimenti o altre categorie di soggetti autorizzati al Trattamento

Il Titolare del Trattamento richiede che il Responsabile del Trattamento renda l' informativa agli interessati?

Sì No

Se sì, l' informativa è stata fornita al Responsabile del Trattamento in formato elettronico?

Sì No

ALLEGATO 2

Misure Tecniche ed Organizzative

DA COMPILARSI A CURA DEL RESPONSABILE DEL TRATTAMENTO

1. Il Trattamento dei Dati Personali Attinenti deve avvenire mediante sistemi di trattamento dei dati per i quali siano state adottate misure tecniche ed organizzative per la protezione dei dati. In questo contesto, il Responsabile del Trattamento assicura alla Titolare che adotterà tutte le misure richieste per il trattamento dei Dati Personali Attinenti tramite i suoi sistemi di trattamento dei dati in conformità con le misure indicate nella tabella seguente:

Oggetto della Misura di Sicurezza	Descrizione della misura adottata dal Responsabile del Trattamento
Pseudonimizzazione e cifratura dei dati personali: assicurare la pseudonimizzazione e la cifratura dei Dati Personali Attinenti	Criptazione sia a livello hardware che a livello del database. Dati identificabili e sensibili sono in tavole separate che impediscono la connessione.
Controllo sull'accesso all'apparecchiatura: impedire al personale non autorizzato l'accesso all'apparecchiatura utilizzata per il trattamento di dati personali	Il personale autorizzato può accedere alle apparecchiature solo con autenticazione a 2 fattori.
Controllo del supporto dati: prevenire operazioni di lettura, copia, modifica o rimozione di supporti dati non autorizzate	Protocollo (TLS) con la nuova generazione di cifrari per prevenire lo spoofing dei dati. 4 passaggi di sicurezza per accedere al database: i) non disponibile per l'accesso pubblico, ii) richiede l'autenticazione e iii) richiede la chiave del certificato, iv) richiede il privilegio per leggere la tabella utente. Attualmente il Responsabile non ammette processori di dati di terze parti. Tutti gli accessi ai dati sensibili devono essere autorizzati. Pertanto non vi sarà alcun accesso diretto ai dati personali.
Protezione dei supporti su cui sono conservati i dati: prevenire la distruzione, la manomissione o comunque l'alterazione dei supporti su cui sono conservati i dati	I dati sono archiviati nel cloud AWS, cui è mandata la responsabilità della protezione dell'hardware. Per affidabilità, il backup dei dati viene eseguito ogni 24 ore e archiviato per 7 giorni.

<p>Protezione delle aree e dei locali: Assicurare la protezione delle aree e dei locali in cui sono situati i dati personali od i supporti di conservazione dei dati personali</p>	<p>Il Responsabile è impostato in un su ... Cloud e i principali punti di ingresso come il server web e l'applicazione web si trovano all'interno della sottorete pubblica. Quindi accessibile da qualsiasi luogo. Ma il database si trova all'interno dello stesso con sottorete privata e non accessibile dall'esterno. Pertanto, solo una persona autorizzata può accedere con alcuni protocolli descritti in precedenza</p>
<p>Controllo della conservazione: prevenire l'inserimento non autorizzato di dati e l'ispezione, la modifica o la cancellazione non autorizzata dei dati personali conservati</p>	<p>L'accesso ai dati viene effettuato dal server delle applicazioni. E solo gli utenti autorizzati possono ispezionare i dati a loro trasmessi. Il resto delle operazioni sono vietate a livello aziendale e dai livelli di sicurezza impostati.</p>
<p>Controllo dell'utente: prevenire l'uso di sistemi automatizzati di trattamento dei dati da parte di personale non autorizzato ad utilizzare apparecchiature per la trasmissione dei dati</p>	<p>Solo personale autorizzato può usare i sistemi.</p>
<p>Controllo sull'accesso ai dati: assicurare che il personale autorizzato all'utilizzo di sistemi per il trattamento dei dati abbia accesso unicamente ai dati personali coperti dalle loro autorizzazioni di accesso</p>	<p>L'accesso ai dati viene effettuato dal server delle applicazioni. Solo gli utenti autorizzati possono ispezionare i dati a loro trasmessi secondo i livelli di autorizzazione impostati. IAM users.</p>
<p>Controllo sull'accesso alle credenziali: Assicurare che, nel caso in cui per l'accesso ai dati personali siano necessarie credenziali personali, queste rimangano sconosciute ed inaccessibili ai soggetti non autorizzati</p>	<p>Le password sono campi crittografati unidirezionali. Quando l'utente richiede l'accesso, il sistema esegue la codifica della password candidata e confronta 2 versioni codificate e restituisce l'errore in caso di errore. In caso di smarrimento della password, l'unico modo per recuperare l'accesso è reimpostare la password. E' attivo un sistema di autenticazione a due fattori.</p>
<p>Controllo della comunicazione: assicurare che sia possibile verificare e stabilire a quali individui possono essere trasmessi o resi disponibili i dati personali utilizzando apparecchiature per la trasmissione dei dati</p>	<p>È possibile accedere al server solo tramite TLS, quindi solo in forma autorizzata.</p>
<p>Controllo dell'inserimento: assicurare che sia successivamente possibile verificare e stabilire quali dati personali siano stati inseriti in sistemi</p>	<p>Il sistema è monitorato da logs.</p>

<p>automatizzati di trattamento dei dati e quando e da chi tale inserimento sia stato effettuato</p>	
<p>Controllo del trasporto: prevenire la lettura, la copia, la modifica o la cancellazione non autorizzata dei dati personali durante il trasferimento di tali dati o il trasferimento dei supporti dati</p>	<p>Dopo aver stabilito l'handshake SSL, i trasferimenti di dati vengono effettuati con token di sicurezza verificati per verificare e controllare l'autorizzazione dell'utente che ha creato la richiesta.</p>
<p>Ripristino: assicurare che i sistemi installati possano, in caso di interruzione, essere ripristinati</p>	<p>Cluster di database con più "repliche di lettura". Un cluster di database è una raccolta di database gestita da una singola istanza di un server di database in esecuzione. Ciò garantisce che ogni singola replica di lettura sia a tolleranza di errore. Inoltre, vengono eseguiti backup periodici per ripristinare i dati in situazioni fatali.</p>
<p>Integrità: assicurare che le funzionalità del sistema siano operative in ogni momento, che la comparsa di difetti nelle funzionalità sia segnalata (in maniera affidabile) e che i dati personali conservati non possano essere danneggiati da malfunzionamenti del sistema</p>	<p>Il livello dell'applicazione è separato dal livello dati. Pertanto, qualsiasi problema irreversibile nel livello dell'applicazione non influirà sui dati archiviati. In tali scenari, il nuovo server delle applicazioni può essere distribuito automaticamente per mitigare il problema di disponibilità</p>
<p>Protezione contro programmi informatici intrusivi: Assicurare che vi sia un'adeguata protezione contro la violazione dei dati effettuata tramite programmi informatici intrusivi (virus, spyware, ecc.)</p>	<p>Il Responsabile cerca sempre di tenere il passo con le versioni più recenti delle piattaforme e del software che utilizza. La pianificazione di aggiornamenti periodici alla generazione precedente di software per mitigare tali vulnerabilità può essere sfruttata da software dannoso. Pertanto la sicurezza si ottiene seguendo le migliori pratiche del settore.</p>

2. Il Responsabile del Trattamento fornirà alla Titolare, in conformità con le disposizioni di questa Nomina, un piano di protezione e sicurezza per il trattamento dei dati comprensivo e aggiornato il quale sarà condiviso con la Titolare non appena questa Nomina entrerà in vigore. La Titolare può altresì richiedere in ogni momento una copia del piano di sicurezza.
3. Nessuno dovrà essere preposto al trattamento dei dati personali dal Responsabile del Trattamento a meno che tale persona:
 - a) sia competente e qualificata per eseguire le specifiche mansioni ad essa assegnate;

- b) sia stata autorizzata dal Responsabile del Trattamento; e
 - c) sia stata pienamente informata dal Responsabile del Trattamento sulle procedure e le norme di legge rilevanti per l'adempimento delle obbligazioni del Responsabile del Trattamento ai sensi di questa Nomina.
4. È vietato fare copie di qualsiasi Dato Personale Attinente trasmesso dalla Titolare al Responsabile del Trattamento, fermo restando, in ogni caso, che il Responsabile del Trattamento può trattenere nei suoi server copie dei dati personali fornitigli ai sensi di un contratto correlato, per ragioni di backup e archiviazione, sino e non oltre il completo espletamento delle funzioni specificate in questa Nomina.

ALLEGATO 3

Modulo di segnalazione della violazione dei dati

Introduzione

Il RGPD impone l'obbligo di notifica delle violazioni dei dati personali alla pertinente autorità di controllo, e in alcuni casi agli Interessati, per tutti i soggetti che si occupano del trattamento di dati personali. Per violazione dei dati personali si intende una Violazione della Sicurezza e cioè un evento che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

In questi casi, i soggetti che si occupano del trattamento di dati personali possono notificare la violazione entro 72 ore dalla sua scoperta. La decisione di notificare la violazione sarà adottata dai competenti uffici della Titolare seguendo una procedura predeterminata. Per assicurarsi che siano adottate le misure necessarie, la Titolare necessita che ogni possibile violazione di dati venga tempestivamente segnalata. Questo modulo deve essere utilizzato per segnalare possibili violazioni dei dati alla persona indicata di seguito:

Il modulo compilato deve essere inviato a ...

Definizioni fondamentali:

Termine	Definizione
Violazione dei dati o della sicurezza	Un evento che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati
Dati personali	Qualsiasi informazione riguardante una persona fisica identificata o identificabile
Interessato	La persona fisica cui si riferiscono i dati personali
Responsabile del Trattamento	Il soggetto che tratta i dati personali per conto della Titolare

1. Dettagli della persona che segnala la violazione

Nome	
Indirizzo e-mail	
Numero di telefono	
Posizione aziendale	
Ufficio di appartenenza	

2. Dettagli della violazione dei dati

Sono state interessate informazioni che permettono l'identificazione di una persona?	<input type="checkbox"/> Si <input type="checkbox"/> No <input type="checkbox"/> Non lo so
Spiegare con parole proprie cosa è successo o cosa ha provocato l'incidente, descrivendo la sequenza di eventi che ha portato alla violazione (menzionare se sono presenti log consultabili). Ove possibile, specificare se le informazioni fornite sono confidenziali, complete, disponibili.	
La violazione riguarda un supporto o dispositivo della Titolare, del Responsabile del Trattamento o di soggetto terzo? In quest'ultimo caso, specificare il nome del soggetto e come si relaziona al trattamento.	
Specificare il nome del(le) applicazione(i)/sistema(i) coinvolti nella violazione, ovvero la fonte della violazione.	
Data in cui è iniziata la violazione dei dati (se conosciuta)	<input type="checkbox"/> Non conosco la data in cui la violazione dei dati è iniziata
Ora dell'incidente (su 24 ore)	<input type="checkbox"/> Non conosco l'ora in cui la violazione dei dati è iniziata
Data in cui la violazione di dati è cessata (se cessata)	<input type="checkbox"/> la violazione di dati non è ancora terminata
In quale stato è avvenuta la violazione di dati?	
La violazione ha coinvolto altri territori?	
A parere del segnalante, cosa ha causato la violazione dei dati?	<input type="checkbox"/> Non conosco le cause della violazione dei dati
Qual è il numero (stimato) di interessati che sono coinvolti / colpiti?	Min: Max: <input type="checkbox"/> Non conosco il numero di individui interessati / colpiti

<p>È possibile classificare il gruppo di individui colpiti dalla violazione? <i>Selezionare una o più categorie</i></p>	<input type="checkbox"/> Tesserati <input type="checkbox"/> Dipendenti <input type="checkbox"/> Fornitori o collaboratori <input type="checkbox"/> Sostenitori (iscritti a newsletter o consenso marketing) <input type="checkbox"/> Acquirenti di biglietteria e altri beni o servizi <input type="checkbox"/> Altro:
<p>È possibile classificare il tipo di dati personali interessati dall'incidente? <i>Selezionare una o più categorie</i></p>	<input type="checkbox"/> Nome e indirizzo <input type="checkbox"/> Recapiti (telefono, email, altro) <input type="checkbox"/> Data di nascita o età <input type="checkbox"/> Codice fiscale <input type="checkbox"/> Informazioni finanziarie (compensi, pagamenti, situazione patrimoniale, ecc) <input type="checkbox"/> Informazioni bancarie (conto corrente, carta di credito, ecc.) <input type="checkbox"/> Copie di documenti di identità <input type="checkbox"/> Documentazione medica <input type="checkbox"/> Username, password o altre informazioni d'accesso a quali servizi? <input type="checkbox"/> Dati relativi all'appartenenza a sindacati <input type="checkbox"/> Dati genetici <input type="checkbox"/> Dati relativi a condanne penali e/o reati <input type="checkbox"/> Altro, <i>specificare ogni altro tipo di dato personale non elencato sopra:</i>
<p>Quali sono le potenziali conseguenze per gli individui interessati? <i>Selezionare una o più categorie, se applicabile.</i></p>	<p>Ad esempio:</p> <input type="checkbox"/> Furto d'identità <input type="checkbox"/> Perdita economica <input type="checkbox"/> Uso non autorizzato di dati personali <input type="checkbox"/> Danno alla reputazione <input type="checkbox"/> Discriminazione <input type="checkbox"/> Altro, <i>specificare:</i>

3. Misure da adottare per affrontare la violazione dei dati

<p>La violazione è stata segnalata a qualcuno esterno alla Titolare? <i>Es. Interessati colpiti, autorità di controllo dei dati, altri soggetti?</i> Specificare se è stata data notifica alle autorità <i>Es. denuncia del furto di un laptop</i></p>	<input type="checkbox"/> No <input type="checkbox"/> Sì, <i>specificare:</i>
--	---

I dati personali colpiti sono stati recuperati?	<input type="checkbox"/> No <input type="checkbox"/> Si <input type="checkbox"/> Parzialmente, <i>specificare:</i>
Sono state adottate misure tecniche ed organizzative per attenuare le conseguenze?	<input type="checkbox"/> Non è stata adottata alcuna misura <input type="checkbox"/> Si, <i>specificare tutte le misure adottate:</i>
<i>Se applicabile:</i> i dati colpiti erano criptati?	<input type="checkbox"/> No <input type="checkbox"/> Si, specificare quale metodo di cifratura era stato utilizzato:

ALLEGATO 4

Dichiarazione di eliminazione in modo sicuro dei dati personali

1. Il Responsabile del Trattamento con la presente certifica di aver eliminato in modo sicuro ogni Dato Personale Attinente, compresi, tra gli altri, quelli conservati su supporto cartaceo, quelli conservati su supporti elettronici, conservati su server o nei back-up, in conformità con l'articolo 12 della Nomina.
2. Fintanto che il Responsabile del Trattamento è obbligato per legge alla conservazione dei Dati Personali Attinenti per un determinato periodo di tempo, il punto che precede è integrato dal seguente:

Il Responsabile del Trattamento ha trattenuto una copia dei Dati Personali Attinenti nel rispetto della Normativa Applicabile e conserverà i seguenti dati personali per il periodo di tempo determinato, dopo il quale il Responsabile del Trattamento garantisce che eliminerà in modo sicuro i Dati Personali Attinenti. Il Responsabile del Trattamento, una volta decorso il periodo di tempo determinato, si impegna a fornire alla Titolare la certificazione della distruzione dei dati suddetti.

Categorie di Interessati a	Categorie di dati personali	Termine per la cancellazione	Normativa che richiede la conservazione ulteriore
•	•	•	•