Cassa Dottori Commercialisti

SCHEMA

ATTO DI NOMINA A RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

(ai sensi dell'art. 28 del Regolamento (UE) 2016/679 – GDPR)

Servizio di tesoreria e prestazioni bancarie associate – CIG BC4F26FD30

La **Cassa Nazionale di Previdenza e Assistenza a favore dei Dottori Commercialisti**, con sede legale in Roma, via Mantova n. 1, codice fiscale 80021670585, in persona del Presidente e legale rappresentante *pro tempore* (di seguito "CNPADC" o "Cassa" o "Titolare")

e

[• denominazione dell'Aggiudicatario], con sede legale in [•], via [•], P. IVA / C.F. [•], iscritta all'Albo delle banche di cui all'art. 13 del D.Lgs. 385/1993 (TUB), in persona del legale rappresentante *pro tempore* (di seguito "Banca", "Aggiudicatario" o "Responsabile")

di seguito congiuntamente le "**Parti**" e ciascuna la "**Parte**".

PREMESSO CHE

A) la Cassa è persona giuridica di diritto privato ai sensi del D. Lgs. 30 giugno 1994, n. 509, e svolge funzioni di previdenza e assistenza obbligatoria a favore dei Dottori Commercialisti iscritti, nonché di gestione del proprio patrimonio;

B) all'esito della procedura di gara CIG BC4F26FD30 indetta ai sensi del D. Lgs. 31 marzo 2023, n. 36, per l'affidamento del servizio di tesoreria e prestazioni bancarie associate (il "Contratto"), la Cassa ha individuato quale aggiudicatario la Banca;

C) l'esecuzione del Contratto comporta, o può comportare, da parte della Banca il trattamento di dati personali di titolarità della Cassa ai sensi del Regolamento (UE) 2016/679 ("GDPR") e del D. Lgs. 30 giugno 2003, n. 196 e ss.mm.ii. ("Codice Privacy"), il cui pieno rispetto, ivi compresi i profili di sicurezza, deve essere garantito anche in attuazione dei provvedimenti dell'Autorità Garante per la protezione dei dati personali (di seguito il "Garante");

D) la Cassa, in qualità di Titolare del trattamento, ravvisa la necessità di nominare la Banca quale Responsabile del trattamento ai sensi e per gli effetti dell'art. 28 GDPR, in relazione ai soli trattamenti effettuati per suo conto nell'esecuzione del Contratto;

E) il Responsabile, ai sensi dell'art. 28, par. 1, GDPR, deve essere individuato tra soggetti che, per affidabilità, esperienza e capacità, presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, nel pieno rispetto della disciplina in materia di protezione dei dati e a tutela dei diritti degli interessati;

F) la Banca dichiara di possedere i requisiti di cui alla precedente lettera E), di disporre delle misure tecniche e organizzative descritte nell'Allegato 2 – da considerarsi parte integrante del presente atto – e ha manifestato la propria disponibilità ad assolvere l'incarico di Responsabile del trattamento;

G) le Parti intendono disciplinare con il presente atto (la "Nomina" o l'"Atto") il trattamento dei dati personali svolto dal Responsabile per conto del Titolare, in conformità all'art. 28, par. 3, GDPR.

TUTTO CIÒ PREMESSO, LE PARTI CONVENGONO E STIPULANO QUANTO SEGUE

Le premesse e gli allegati formano parte integrante e sostanziale del presente Atto.

Art. 1 Definizioni

I termini “dato personale”, “trattamento”, “interessato”, “titolare del trattamento”, “responsabile del trattamento”, “categorie particolari di dati”, “violazione dei dati personali”, “pseudonimizzazione” e ogni altro termine non diversamente definito hanno il significato loro attribuito dall’art. 4 e dalle ulteriori disposizioni del GDPR. Per “sub-responsabile” si intende l’altro responsabile di cui il Responsabile si avvale ai sensi dell’art. 28, parr. 2 e 4, GDPR.

Art. 2 Oggetto, finalità e perimetro del trattamento

2.1 Con il presente Atto il Titolare nomina la Banca quale Responsabile del trattamento dei dati personali gestiti per suo conto in ragione e nei limiti dell’esecuzione del Contratto, nonché delle ulteriori attività richieste per iscritto dal Titolare.

2.2 L’oggetto, la durata, la natura e le finalità del trattamento, la tipologia dei dati personali e le categorie di interessati sono dettagliati nell’Allegato 1.

2.3 Il Responsabile tratta i dati personali esclusivamente per le finalità connesse all’esecuzione del Contratto e non per finalità proprie, fatto salvo quanto previsto all’art. 4 (Titolarità autonoma della Banca). Il presente Atto non comporta il trasferimento al Responsabile della titolarità dei dati.

Art. 3 Durata della Nomina

3.1 La presente Nomina ha efficacia dalla data di sottoscrizione e per tutta la durata del Contratto, comprese le eventuali proroghe e il periodo necessario alle attività di subentro e migrazione dei dati.

3.2 Gli obblighi di riservatezza, di conservazione, di restituzione/cancellazione e ogni altro obbligo destinato per sua natura a permanere restano efficaci anche dopo la cessazione, per qualsiasi causa, del Contratto e della Nomina.

Art. 4 Qualificazione delle Parti e titolarità autonoma della Banca

4.1 In relazione ai trattamenti effettuati per conto del Titolare nell’esecuzione del Contratto, la Banca opera quale Responsabile del trattamento ai sensi dell’art. 28 GDPR.

4.2 Resta inteso che, per i trattamenti che la Banca effettua in adempimento di obblighi di legge propri dell’attività bancaria – tra cui, a titolo esemplificativo e non esaustivo, gli adempimenti in materia di antiriciclaggio e contrasto al finanziamento del terrorismo (D. Lgs. 231/2007), gli obblighi di adeguata verifica e conservazione, le segnalazioni e gli obblighi informativi verso la Banca d’Italia e le altre Autorità di vigilanza, la Centrale dei Rischi, gli obblighi fiscali e di conservazione documentale previsti dalla normativa bancaria, nonché la prevenzione delle frodi – la Banca agisce in qualità di **autonomo Titolare del trattamento**, assumendone i relativi obblighi e responsabilità. Tali trattamenti esulano dal perimetro della presente Nomina.

4.3 Qualora dall’esecuzione del Contratto dovessero derivare trattamenti riconducibili a una contitolarità ai sensi dell’art. 26 GDPR, le Parti ne disciplineranno gli aspetti con apposito accordo.

4.4 Resta inteso che, in relazione al servizio opzionale di autenticazione federata (Single Sign-On) di cui al Capitolo 10 delle Specifiche Tecniche, la Banca opera in qualità di Responsabile del Trattamento esclusivamente per la fase tecnica di transito dell'asserto di sicurezza. Dal momento in cui l'iscritto accede alle URL dedicate della Banca ed avvia l'istruttoria contrattuale per l'erogazione di servizi bancari o di finanziamento, la Banca assume la veste di Autonomo Titolare del Trattamento,

rispondendo in via esclusiva di ogni violazione e obbligandosi a tenere integralmente indenne la Cassa da qualunque pretesa o sanzione.

Art. 5 Istruzioni documentate del Titolare

5.1 Il Responsabile tratta i dati personali soltanto su istruzione documentata del Titolare, anche con riguardo all'eventuale trasferimento di dati verso Paesi terzi o organizzazioni internazionali, salvo che lo richieda il diritto dell'Unione o dello Stato membro cui è soggetto il Responsabile; in tal caso il Responsabile informa il Titolare prima del trattamento, salvo che il diritto applicabile lo vieti per rilevanti motivi di interesse pubblico.

5.2 Costituiscono istruzioni documentate il presente Atto e i suoi allegati, il Contratto, il Capitolato Tecnico Descrittivo e Prestazionale e i relativi allegati tecnici, nonché le ulteriori istruzioni scritte impartite dal Titolare anche in corso di esecuzione.

5.3 Il Responsabile informa immediatamente il Titolare qualora ritenga che un'istruzione violi il GDPR, il Codice Privacy o altre disposizioni, nazionali o dell'Unione, in materia di protezione dei dati personali.

Art. 6 Obblighi del Responsabile

Nell'accettare la presente Nomina, il Responsabile si impegna a effettuare il trattamento attenendosi alle istruzioni del Titolare e nel pieno rispetto della normativa applicabile, dichiarandosi edotto degli obblighi posti a suo carico. In particolare, il Responsabile si impegna a:

a) effettuare le operazioni di trattamento limitatamente a quanto necessario al perseguimento dell'oggetto del Contratto e a quanto ulteriormente delegato dal Titolare per iscritto, nel rispetto delle istruzioni documentate di cui all'art. 5;

b) garantire che le persone autorizzate al trattamento si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza, secondo quanto previsto all'art. 7;

c) adottare e mantenere le misure tecniche e organizzative adeguate ex artt. 25 e 32 GDPR, secondo quanto previsto all'art. 8 e nell'Allegato 2;

d) rispettare le condizioni per il ricorso a un sub-responsabile di cui all'art. 9;

e) assistere il Titolare, con misure tecniche e organizzative adeguate e nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo di dare seguito alle richieste per l'esercizio dei diritti degli interessati, secondo l'art. 11;

f) assistere il Titolare nel garantire il rispetto degli obblighi in materia di sicurezza del trattamento, notifica e comunicazione delle violazioni dei dati personali, valutazione d'impatto sulla protezione dei dati e consultazione preventiva (artt. 32-36 GDPR), secondo gli artt. 11 e 12;

g) su scelta del Titolare, cancellare o restituire tutti i dati personali al termine della prestazione dei servizi, secondo l'art. 16;

h) mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi a proprio carico e consentire e contribuire alle attività di revisione, comprese le ispezioni, secondo l'art. 15;

i) tenere il registro di tutte le categorie di attività relative al trattamento svolte per conto del Titolare ai sensi dell'art. 30, par. 2, GDPR;

j) individuare le modalità affinché la raccolta, il trattamento e la conservazione dei dati personali avvengano nel rispetto dei principi di cui all'art. 5 GDPR;

k) consentire al Titolare il controllo della sicurezza della strumentazione e dei programmi utilizzati nell'elaborazione dei dati personali;

l) qualora, considerata la propria competenza, ritenga le misure adottate non più adeguate, fornirne tempestiva comunicazione scritta al Titolare e porre in essere gli interventi provvisori essenziali e improcrastinabili, in attesa delle soluzioni definitive da concordare con il Titolare;

m) non adottare autonome decisioni in ordine alle finalità e alle modalità del trattamento; in caso di necessità e urgenza, informare al più presto il Titolare affinché questi possa assumere le opportune decisioni;

n) comunicare immediatamente al Titolare, e comunque non oltre le 24 ore successive al loro ricevimento, ogni richiesta, ordine o attività di controllo del Garante o dell'Autorità Giudiziaria relativi ai trattamenti svolti per conto del Titolare;

o) rispettare le istruzioni specifiche e ulteriori eventualmente impartite dal Titolare, integrandole nelle procedure già in essere, e informare tempestivamente il Titolare ai sensi dell'art. 5.3;

p) garantire la localizzazione dei dati nell'Unione Europea o nello Spazio Economico Europeo secondo l'art. 10;

q) realizzare quant'altro sia utile o necessario al fine di garantire l'adempimento degli obblighi previsti dalla normativa applicabile, nei limiti dei compiti affidati con il presente Atto.

Quanto sopra costituisce indicazione esemplificativa e non esaustiva dei compiti del Responsabile; ulteriori istruzioni potranno essere fornite, di volta in volta, dal Titolare.

Art. 7 Riservatezza, autorizzati al trattamento e amministratori di sistema

7.1 Il Responsabile garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza, anche per il periodo successivo alla cessazione del rapporto di lavoro o di collaborazione, in relazione alle operazioni eseguite per conto del Titolare.

7.2 Il Responsabile procede a designare e istruire il personale incaricato del trattamento ai sensi degli artt. 28 e 29 GDPR e dell'art. 2-quaterdecies del Codice Privacy, fornendo le istruzioni e le autorizzazioni necessarie a un trattamento corretto, lecito e sicuro e verificandone la puntuale applicazione.

7.3 Ove ricorrano i presupposti, il Responsabile applica il Provvedimento del Garante del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle funzioni di amministratore di sistema", come modificato dal Provvedimento del 25 giugno 2009. In particolare, individua e designa individualmente gli amministratori di sistema sulla base dei requisiti di esperienza, capacità e affidabilità; predispone, aggiorna e conserva l'elenco con gli estremi identificativi, fornendolo al Titolare su richiesta; svolge con cadenza almeno annuale i controlli sul loro operato; assicura la registrazione degli accessi (log) con caratteristiche di completezza e inalterabilità e conservazione per almeno sei mesi (cfr. Allegato 2).

Art. 8 Misure di sicurezza

8.1 Il Responsabile adotta e mantiene misure tecniche e organizzative adeguate ai sensi degli artt. 25 e 32 GDPR, di livello non inferiore a quelle descritte nell'Allegato 2 al presente Atto e a quelle previste dall'Art. 4 del Capitolato e dall'Allegato 1 – Specifiche tecniche, tenuto conto dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

8.2 In coerenza con il quadro di resilienza operativa digitale e cybersicurezza applicabile (Reg. (UE) 2022/2554 – DORA; Dir. (UE) 2022/2555 – NIS2, come recepita dal D. Lgs. 138/2024), le misure includono, tra l'altro: cifratura delle comunicazioni mediante TLS 1.3 o standard superiore e cifratura dei dati a riposo con algoritmi di forza pari o superiore ad AES-256; pseudonimizzazione ove compatibile con il servizio; autenticazione forte degli utenti e del personale; principi di minimo privilegio e segregazione dei ruoli; tracciabilità integrale delle operazioni mediante audit log immutabili; piani di continuità operativa e disaster recovery con test periodici.

8.3 Qualora ritenga le misure adottate non più adeguate, il Responsabile ne dà tempestiva comunicazione scritta al Titolare e adotta gli interventi provvisori essenziali ai sensi dell'art. 6, lett. l).

Art. 9 Sub-responsabili del trattamento

9.1 Il Responsabile non ricorre ad altro responsabile (sub-responsabile) senza previa autorizzazione scritta, specifica o generale, del Titolare.

9.2 Alla data di sottoscrizione, il Titolare autorizza i sub-responsabili indicati nell'Allegato 3, ivi comprese, ove pertinenti, le infrastrutture e i circuiti interbancari necessari all'erogazione del servizio (a titolo esemplificativo, il circuito CBI e il sistema pagoPA), i fornitori tecnologici, i servizi di conservazione a norma e gli eventuali soggetti del medesimo gruppo bancario impiegati nell'esecuzione del Contratto.

9.3 In caso di aggiunta o sostituzione di sub-responsabili, il Responsabile informa per iscritto il Titolare con un preavviso di almeno 30 (trenta) giorni, dando al Titolare la possibilità di opporsi per motivi legittimi. In caso di opposizione, le Parti ricercano in buona fede una soluzione; in mancanza di accordo, il Titolare ha facoltà di recedere, anche parzialmente, dalla porzione di servizio interessata, senza oneri a proprio carico.

9.4 Il Responsabile impone al sub-responsabile, mediante contratto o altro atto giuridico a norma del diritto dell'Unione o dello Stato membro, gli stessi obblighi di protezione dei dati contenuti nel presente Atto, in particolare la prestazione di garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate (art. 28, par. 4, GDPR).

9.5 Il Responsabile rimane pienamente responsabile nei confronti del Titolare dell'adempimento degli obblighi del sub-responsabile. Su richiesta, fornisce al Titolare copia delle clausole in materia di protezione dei dati contenute negli accordi con i sub-responsabili.

Art. 10 Trasferimenti verso Paesi terzi

10.1 Il Responsabile assicura la localizzazione dei dati personali all'interno dell'Unione Europea o dello Spazio Economico Europeo.

10.2 Eventuali trasferimenti verso Paesi terzi o organizzazioni internazionali sono ammessi soltanto su istruzione documentata del Titolare e nel rispetto del Capo V del GDPR (artt. 44-49), previa adozione delle garanzie adeguate previste (ivi comprese, ove applicabili, le decisioni di adeguatezza della Commissione o le clausole contrattuali tipo).

Art. 11 Assistenza al Titolare

11.1 Il Responsabile assiste il Titolare, con misure tecniche e organizzative adeguate, nel dare seguito alle richieste degli interessati per l'esercizio dei loro diritti (artt. 12-22 GDPR). Le istanze eventualmente ricevute direttamente dagli interessati sono trasmesse tempestivamente al Titolare e il Responsabile non vi dà autonomo riscontro, salvo istruzione del Titolare; coopera inoltre nel riscontro

ai sensi dell'art. 28, par. 3, lett. e), GDPR, fornendo tempestivamente le informazioni in proprio possesso.

11.2 Tenuto conto della natura del trattamento e delle informazioni a disposizione, il Responsabile assiste il Titolare nel garantire il rispetto degli obblighi in materia di sicurezza, di valutazione d'impatto sulla protezione dei dati e di consultazione preventiva (artt. 32, 35 e 36 GDPR).

Art. 12 Violazioni dei dati personali (data breach)

12.1 Il Responsabile informa il Titolare **immediatamente, per le vie brevi, e comunque mediante notifica formale entro e non oltre 2 (due) ore dal momento in cui è venuto a conoscenza** di una violazione dei dati personali, in conformità ai termini previsti dall'Allegato Specifiche tecniche al Capitolato (notifica iniziale entro 2 ore dalla classificazione dell'evento; informativa intermedia entro 24 ore; report finale entro 30 giorni), così da consentire al Titolare di adempiere ai propri obblighi di notifica al Garante entro 72 ore (art. 33) e di comunicazione agli interessati (art. 34).

12.2 La comunicazione di cui al comma precedente descrive almeno: la natura della violazione, comprese, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni interessate; i dati di contatto del DPO o di altro punto di contatto; le probabili conseguenze; le misure adottate o di cui si propone l'adozione per porvi rimedio o attenuarne gli effetti (art. 33, par. 3, GDPR).

12.3 Il Responsabile coopera con il Titolare e adotta ogni misura ragionevolmente necessaria per minimizzare gli effetti della violazione; mantiene un registro degli incidenti; non effettua alcuna notifica al Garante o comunicazione agli interessati in nome del Titolare, salvo specifica istruzione scritta.

Art. 13 Registro delle attività di trattamento

Il Responsabile tiene il registro di tutte le categorie di attività relative al trattamento svolte per conto del Titolare, con il contenuto prescritto dall'art. 30, par. 2, GDPR, e lo mette a disposizione del Garante e del Titolare su richiesta.

Art. 14 Responsabile della protezione dei dati

Il Responsabile designa un Responsabile della protezione dei dati (DPO) ove ne ricorrano i presupposti e, comunque, in coerenza con quanto previsto dall'Allegato 1 – Specifiche tecniche, comunicandone i recapiti al Titolare e mantenendoli aggiornati per l'intera durata del Contratto.

Art. 15 Audit e ispezioni

15.1 Il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 GDPR e al presente Atto.

15.2 Il Responsabile consente e contribuisce alle attività di revisione, comprese le ispezioni, realizzate dal Titolare o da un altro soggetto da questi incaricato e vincolato alla riservatezza, con preavviso ragionevole e con modalità tali da non compromettere la sicurezza e la riservatezza dei dati di terzi. Il Responsabile può dare evidenza della conformità anche mediante certificazioni o esiti di audit di terze parti (es. ISO 27001/22301), ferma restando la facoltà del Titolare di procedere ad audit diretti, in coordinamento con le previsioni del Capitolato.

Art. 16 Cancellazione o restituzione dei dati al termine

16.1 Al termine della prestazione dei servizi relativi al trattamento, ovvero in caso di anticipata cessazione del Contratto per qualsiasi causa, il Responsabile, su scelta del Titolare, cancella o restituisce

tutti i dati personali e cancella le copie esistenti, salvo che la conservazione sia richiesta dal diritto dell'Unione o dello Stato membro.

16.2 L'adempimento di cui al comma 16.1 è coordinato con l'obbligo, previsto dal Capitolato e dall'Allegato 1 – Specifiche tecniche (capitoli 5 e 9), di consegna alla Cassa, senza oneri aggiuntivi e in formato utilizzabile, di copia integrale e completa dell'archivio del materiale scambiato, su supporto informatico protetto (cifrato AES-256 o equivalente, con consegna delle chiavi secondo procedura di key escrow concordata, ovvero tramite canale telematico cifrato end-to-end), nonché con i termini di conservazione propri del servizio di tesoreria.

16.3 Ove la Banca sia tenuta a conservare determinati dati per adempiere a obblighi di legge propri (a titolo esemplificativo, gli obblighi di conservazione in materia di antiriciclaggio, gli obblighi fiscali e quelli previsti dalla normativa bancaria), essa li conserva limitatamente a quanto strettamente necessario e per il tempo prescritto, in qualità di autonomo Titolare ai sensi dell'art. 4, astenendosi da ogni ulteriore trattamento.

16.4 Su richiesta del Titolare, il Responsabile rilascia attestazione scritta dell'avvenuta cancellazione o restituzione dei dati.

Art. 17 Responsabilità e manleva

17.1 Ciascuna Parte risponde dei danni cagionati dal trattamento ai sensi dell'art. 82 GDPR. Il Responsabile risponde per i danni cagionati dal trattamento solo se non ha adempiuto agli obblighi del GDPR specificatamente diretti ai responsabili o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del Titolare.

17.2 Il Responsabile tiene indenne e manleva il Titolare da pretese, contestazioni, sanzioni e oneri derivanti dalla violazione, a sé imputabile, degli obblighi assunti con il presente Atto, fermo il diritto di regresso secondo l'art. 82, par. 5, GDPR.

17.3 Restano ferme le previsioni del Contratto in materia di responsabilità, penali e coperture assicurative.

Art. 18 Modifiche e cessazione

18.1 Eventuali modifiche al presente Atto sono concordate per iscritto tra le Parti. Le Parti adeguano la Nomina al mutato quadro normativo e ai provvedimenti del Garante che intervengano in corso di rapporto.

18.2 In caso di scioglimento o cessazione del Contratto per qualsiasi causa, la Nomina cessa e il Responsabile interrompe ogni operazione di trattamento, fatti salvi gli adempimenti di cui all'art. 16.

18.3 Il presente Atto non comporta alcun diritto del Responsabile a uno specifico compenso per l'attività svolta, intendendosi la stessa ricompresa nel corrispettivo del Contratto.

Art. 19 Disposizioni finali, legge applicabile e foro

19.1 In caso di contrasto tra il presente Atto e gli altri documenti contrattuali in materia di protezione dei dati personali, prevale la disposizione più favorevole alla tutela degli interessati e del Titolare.

19.2 Il presente Atto è regolato dalla legge italiana. Per ogni controversia è competente il foro indicato nel Contratto.

19.3 Con la sottoscrizione del presente Atto, il Responsabile accetta la Nomina e dichiara di impegnarsi a rispettare le istruzioni impartite dal Titolare e ad agire in conformità agli obblighi previsti dalla normativa applicabile in materia di protezione dei dati personali.

Luogo e data _____

Per il Titolare del trattamento	**Per il Responsabile del trattamento**
Il Presidente della Cassa	Il legale rappresentante
_____	_____

ALLEGATO 1
Descrizione del trattamento

Categorie di interessati. I dati personali oggetto di trattamento riguardano, in via esemplificativa e non esaustiva: iscritti e contribuenti della Cassa (Dottori Commercialisti); pensionati e titolari di trattamenti previdenziali; beneficiari di prestazioni assistenziali ed eventuali familiari/aventi diritto; dipendenti e collaboratori della Cassa; fornitori e relativi referenti; conduttori e locatari degli immobili dell'Ente; controparti di operazioni di investimento e di dismissione patrimoniale; ogni altro soggetto i cui dati siano trattati nell'ambito dei flussi di incasso e di pagamento gestiti nell'esecuzione del Contratto.

Tipologia di dati personali oggetto di trattamento. I dati oggetto di trattamento sono i seguenti:

Categoria di dati personali	Tipologia di dati personali
Dati personali comuni	Identificativi (nome, cognome, codice fiscale, documenti di identità); anagrafici (luogo e data di nascita); di contatto (residenza, domicilio, PEC, e-mail, telefono).
Dati bancari e finanziari	Coordinate di pagamento (IBAN), importi, causali, estremi di incasso e di pagamento; dati relativi alla posizione contributiva e ai trattamenti previdenziali e assistenziali erogati; dati relativi a operazioni patrimoniali.
Dati giudiziari e procedure esecutive (art. 10)	Dati relativi a condanne penali e reati o a connesse misure di sicurezza e procedure esecutive: Dati identificativi dei soggetti esecutati, importi precettati e codici di riferimento delle ordinanze di pignoramento presso terzi
Dati relativi a procedure esecutive	Dati identificativi e importi relativi a pignoramenti e ad altre procedure esecutive, ove trattati nell'ambito dei flussi.
Eventuali categorie particolari (art. 9)	Dati eventualmente idonei a rivelare lo stato di salute o altre categorie particolari, ove desumibili dalla natura o dalla causale di talune prestazioni assistenziali, trattati nei soli limiti strettamente necessari e con misure rafforzate. [Perimetro da confermare con il Titolare/DPO.] Categorie particolari di dati ex art. 9 GDPR: Dati idonei a rivelare lo stato di salute o condizioni di disabilità degli iscritti o dei loro aventi diritto, limitatamente alle causali dei mandati di pagamento per trattamenti assistenziali ordinati dall'Ente

Le tecniche di pseudonimizzazione e di cifratura sono applicate quali misure di sicurezza ove compatibili con le finalità e con le modalità operative del servizio.

Natura e finalità del trattamento. Il trattamento è effettuato per conto del Titolare e in ragione dell'esecuzione del servizio di tesoreria e prestazioni bancarie associate, con particolare riguardo a: gestione degli incassi (deleghe SDD, MAV, avvisi pagoPA, F24, bonifici); esecuzione dei pagamenti (trattamenti previdenziali e assistenziali, emolumenti al personale, fornitori, tributi); riconciliazione e rendicontazione; conservazione e gestione documentale; assistenza e ogni ulteriore attività richiesta per iscritto dal Titolare. Il trattamento ha natura necessaria all'esecuzione del Contratto.

Operazioni di trattamento. Raccolta, registrazione, organizzazione, strutturazione, conservazione, consultazione, elaborazione, comunicazione nei limiti strettamente necessari all'esecuzione del

Contratto, trasmissione mediante i canali tecnici previsti (SFTP cifrato, API/web service, PEC, procedura OIL) e cancellazione.

Durata del trattamento. Il trattamento è effettuato per tutta la durata del Contratto e delle eventuali proroghe, fatti salvi gli obblighi e i termini di conservazione di cui all'art. 16.

Modalità di trattamento. Il trattamento avviene mediante strumenti manuali ed elettronici e modalità automatizzate, con logiche strettamente correlate alle finalità e, comunque, con modalità tali da garantire la sicurezza e la riservatezza dei dati, nel rispetto degli obblighi sanciti dalla legge.

ALLEGATO 2

Misure tecniche e organizzative adottate dal Responsabile e dagli eventuali Sub-responsabili

Il Responsabile e gli eventuali Sub-responsabili si impegnano a garantire un livello di sicurezza non inferiore a quello descritto dalle misure tecniche e organizzative di seguito riportate, in coerenza con gli artt. 25 e 32 GDPR, con l'Art. 4 del Capitolato e con l'Allegato 1 – Specifiche tecniche.

1. Amministratori di sistema

Rispetto del Provvedimento del Garante del 27 novembre 2008 e ss.mm.ii. in materia di amministratori di sistema.

Designazione. Redazione di una lettera di designazione individuale per ciascun amministratore di sistema, previa valutazione di esperienza, capacità e affidabilità, con elencazione analitica degli ambiti di operatività.

Revisione dell'operato. Revisione, con cadenza almeno annuale, dell'operato degli amministratori di sistema.

Lista. Produzione, su richiesta del Titolare, dell'elenco del personale designato quale amministratore di sistema, con le funzioni attribuite.

Logging. Implementazione di un software che produca log di accesso ai sistemi su cui operano gli amministratori, completi e inalterabili, verificabili in integrità e conservati per almeno sei mesi.

2. Autenticazione

Credenziali. Password alfanumerica di almeno 8 caratteri con maiuscole/minuscole e caratteri speciali; in alternativa token o, per trattamenti di particolare rilevanza, caratteristiche biometriche; su richiesta del Titolare, autenticazione a più fattori. Applicazione dei criteri su tutti i sistemi e applicazioni.

Modifica periodica. Cambio password automatizzato almeno ogni 90 giorni e cambio forzato al primo accesso per i nuovi utenti.

Credenziali individuali. Assegnazione di credenziali esclusivamente individuali, in particolare per le utenze con permessi elevati.

Inattività e disattivazione. Segnalazione come inattive e scadenza automatica delle credenziali (salvo utenze tecniche) decorsi sei mesi, o aggiornamento al cambio di mansione.

Non disclosure. Procedure documentate per l'accesso ai dati in caso di assenza prolungata dell'incaricato, senza disclosure delle password.

3. Salvaguardia di dati e dispositivi

Protezione delle credenziali e dei dispositivi. Policy con istruzioni sulle cautele per la segretezza delle credenziali e la custodia dei dispositivi, anche a protezione da danni e furti.

Protezione delle sessioni. Lock screen/screensaver con reinserimento delle credenziali, attivazione automatica dopo meno di 5 minuti di inattività.

4. Autorizzazione

Profili autorizzativi. Sistema centralizzato di autenticazione e autorizzazione; censimento dei permessi prima dell'assegnazione.

Minimizzazione dei permessi. Principi di least privilege e need to know, con attribuzione dei permessi minimi su sistemi e applicativi.

Revisione dei profili. Verifica almeno annuale della coerenza e della presenza dei profili autorizzativi, con verbalizzazione.

5. Difesa

Aggiornamenti. Gestione centralizzata e/o automatizzata degli aggiornamenti, con particolare riguardo a quelli di sicurezza.

Sistemi non supportati. Segregazione delle macchine non più supportate.

Data protection by design. Adozione di linee guida di data protection by design coerenti con i sistemi sviluppati internamente.

Programmi di protezione. Antivirus (preferibilmente a gestione centralizzata), firewall con moduli IDS/IPS e antispam, mantenuti aggiornati.

6. Disponibilità dei dati

Backup. Sistema e piano di backup documentati in apposita policy e procedura.

Piani di ripristino. Test di ripristino verbalizzati, con documentazione delle procedure e dei tempi.

7. Protezione dei dati

Cifratura e confinamento. Cifratura a tutti i livelli (full disk encryption, transparent data encryption sui database, file-level encryption per file contenenti credenziali) con standard crittografici non deprecati.

Pseudonimizzazione. Pseudonimizzazione dei dati personali eventualmente presenti nei database.

Cifratura in transito. Implementazione e documentazione delle tecnologie di cifratura in transito.

8. Dispositivi rimovibili

Regolamentazione. Disciplina dell'utilizzo e della protezione dei supporti rimovibili.

Sanitizzazione. Procedure per distruzione, cifratura e/o formattazione dei dispositivi rimovibili e aziendali in uso.

9. Ruoli di sicurezza

Individuazione della funzione aziendale responsabile della cybersecurity (es. CISO/CSO), reperibile per la gestione degli incidenti e nota a tutto il personale.

10. Terze parti

Contratti. Inclusione nei contratti con outsourcer e fornitori dei requisiti di sicurezza pertinenti.

Audit di secondo livello. Verifica periodica della coerenza con i requisiti di sicurezza contrattualizzati tramite audit calendarizzati.

11. Asset management

Rimozione tempestiva di asset e credenziali del personale non più in forza o che abbia cambiato mansione, con verifica periodica dell'effettiva rimozione.

12. Sicurezza fisica del Centro Elaborazione Dati (CED)

Misure di sicurezza fisica. Procedure formali di accesso al CED; controllo accessi con scheda elettronica e allarmi collegati a SOC; registrazione e analisi dei tentativi non autorizzati; porte tagliafuoco con allarme; CCTV interno ed esterno operativo 24/7 con registrazioni conservate per almeno 7 giorni.

Visitatori. Autenticazione, accompagnamento e registrazione dei visitatori, previa approvazione delle aree e identificazione in loco.

Condizioni del CED. Monitoraggio costante di temperatura, raffreddamento, polvere e umidità, con verifica periodica dei sensori.

13. Controllo degli accessi

Credenziali individuali. Credenziali individuali per ciascun incaricato, con istruzioni a non condividerle.

Profili autorizzativi. Creazione di profili autorizzativi a cui assegnare le utenze.

Network access control e segmentazione. Valutazione di soluzioni NAC e segmentazione della rete in VLAN separate.

Sessioni e rate limiting. Numero massimo di sessioni concorrenti per utente e di tentativi di login falliti prima del blocco.

14. Integrità dei sistemi

Sanitizzazione degli input. Processi di sanitizzazione degli input per prevenire attacchi noti (es. SQL Injection).

Gestione di password e chiavi. Soluzioni per la gestione di password e chiavi di cifratura.

Misure non disattivabili. Impossibilità, per gli incaricati non preposti a funzioni di sicurezza, di disattivare le misure di protezione.

15. Vulnerability assessment e penetration testing

Periodicità. Sessioni di vulnerability assessment e penetration testing con periodicità almeno annuale.

Automatizzazione. Impiego di tool automatizzati, a integrazione e non in sostituzione di quelli tradizionali.

16. Gestione degli incidenti e delle violazioni

Procedure di incident handling. Prassi, protocolli e procedure formalizzate con ruoli prestabiliti.

Formazione. Personale reso edotto delle procedure di incident handling.

Alert e registro. Adozione, ove adeguato, di un SIEM o soluzioni equivalenti; registro degli incidenti con informazioni su scoperta, analisi, contenimento, mitigazione e recupero.

Comunicazione al Titolare. Comunicazione tempestiva degli incidenti, nei termini di cui all'art. 12 del presente Atto.

17. Business continuity e disaster recovery

Business continuity. Garanzia della continuità operativa dei servizi offerti al Titolare, anche tramite Business Continuity Plan.

Disaster recovery. Strategia di disaster recovery con policy per la conservazione sicura e il ripristino dei backup.

Cifratura e custodia. Cifratura dei backup e procedure sicure di custodia.

18. Formazione, registrazione delle operazioni e sviluppo software

Formazione. Training periodici di security awareness per tutto il personale.

Registrazione delle operazioni. Software di operational intelligence che produca log inalterabili, completi e verificabili sui sistemi su cui sono trattati i dati del Titolare.

Sviluppo e ambienti. Linee guida di codice sicuro; separazione degli ambienti di test, sviluppo e produzione; procedure formalizzate di rilascio; testing prima della messa in produzione; gestione delle patch; protezione dei dati di test mediante offuscamento o cifratura.

ALLEGATO 3

Elenco dei sub-responsabili autorizzati

Il presente elenco riporta i sub-responsabili autorizzati dal Titolare alla data di sottoscrizione, ai sensi dell'art. 9. Eventuali aggiornamenti seguono la procedura ivi prevista. [Da compilare a cura dell'Aggiudicatario.]

Denominazione	Sede / Paese	Attività / servizio affidato	Ubicazione del trattamento
			(UE/SEE)
			(UE/SEE)
			(UE/SEE)