Allegato e) al Capitolato Tecnico

SCHEMA

Accordo sul trattamento e nomina a Responsabile del trattamento dei dati personali ("DPA")

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

VISTO il contratto (di seguito anche "**Contratto**") contraddistinto dal n. CIG n. _____, sottoscritto dalla PagoPA S.p.A. (di seguito anche "**Committente**" o "**Titolare**") in data _____, per l'affidamento a _____ (CF. e P.IVA _____) (di seguito anche "**Fornitore**" o "Responsabile") dei servizi _____ ("**Servizi**") così come dettagliati nel predetto Contratto e nell'offerta proposta dal Fornitore e accettata dalla Committente;

CONSIDERATO che le attività oggetto del Contratto comportano o possono comportare il trattamento di dati personali, ai sensi del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (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);

VISTO, in particolare, l'art. 4, paragrafo 1, n. 7) del Regolamento, che 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 visto altresì l'art. 4, paragrafo 1, n. 8) del Regolamento, che 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*";

VISTO l'art. 28, paragrafo 1 del Regolamento, secondo cui "*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*";

CONSIDERATA l'idoneità, alla luce dell'attività istruttoria già svolta, di _____ rispetto alle garanzie richieste dalla normativa regolamentare europea con riferimento all'adeguatezza delle misure tecniche e organizzative per la tutela dei diritti dell'interessato;

PagoPA S.p.A. con sede legale in Roma, piazza Colonna, 370 - C.F. 15376371009 - in persona di **Giuseppe Virgone**

DESIGNA

_____ (CF. e P.IVA 06409201008), in persona del ..... Dott....., con sede legale in ..... (...), ... n. ..... - che accetta - quale **Responsabile del trattamento dei dati personali**, ai sensi e per gli effetti dell'art. 28 del Regolamento, con riferimento alle attività di cui al Contratto CIG _____, che qui si intente integralmente richiamato .

Per le attività per le quali la Committente agisce a sua volta come responsabile del trattamento, la presente nomina deve intendersi quale nomina a sub-responsabile del trattamento ai sensi dell'art. 28 co. 4 del Regolamento.

Il Fornitore effettua, per conto del Titolare, il trattamento dei dati personali necessario per lo svolgimento delle attività disciplinate dal Contratto.

A tal fine si conviene quanto segue.

1. Il Fornitore s'impegna a garantire la massima riservatezza e a non divulgare a terzi informazioni, dati etc., anche relativi alla Committente, di cui verrà a conoscenza nell'ambito dello svolgimento delle attività oggetto del Contratto.
2. Il Fornitore si impegna affinché tutte le informazioni, concetti, idee, procedimenti, metodi e/o dati tecnici di cui il personale utilizzato verrà a conoscenza nello svolgimento del servizio debbano essere considerati riservati. In tal senso Il Fornitore si obbliga ad adottare con i propri dipendenti e consulenti tutte le cautele necessarie a tutelare la riservatezza di tali informazioni e/o documentazione.
3. Il Fornitore è nominato Responsabile del trattamento ai sensi dell'art. 28 del Regolamento UE n. 2016/679 sulla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (nel seguito anche "Regolamento UE"), per tutta la durata del contratto. A tal fine il Fornitore è autorizzato a trattare i dati personali necessari per l'esecuzione delle attività oggetto del Contratto, escluso espressamente il trattamento dei dati personali per finalità proprie del Fornitore, e si impegna ad effettuare, per conto della Committente, le sole operazioni necessarie per fornire il servizio oggetto del contratto, nei limiti delle finalità ivi specificate, nel rispetto del d.lgs. n. 196/2003 e ss. mm.e del Regolamento UE (nel seguito anche "Normativa in tema di trattamento dei dati personali") e delle istruzioni nel seguito fornite.
4. Il Fornitore si impegna a presentare, su richiesta della Committente, garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse per l'adozione di misure tecniche ed organizzative adeguate volte ad

assicurare che il trattamento sia conforme alle prescrizioni della normativa in tema di trattamento dei dati personali.

5. Le finalità del trattamento sono: esecuzione del Contratto.
6. Il tipo di dati personali trattati in ragione delle attività oggetto del Contratto sono:
    a. dati comuni (a titolo esemplificativo e non esaustivo, dati identificativi, dati anagrafici e di contatto);
    b. dati relativi a prodotti o servizi erogati agli utenti finali dei prodotti e servizi gestiti dalla Committente;
    c. dati relativi all'attività d'impresa, d'arte o professione, dati relativi all'attività scolastica e accademica;
    d. dati fiscali e contabili, anche compresi o comunque collegati alle categorie precedenti, inclusi quelli relativi alla fatturazione;
    e. dati bancari e dati relativi a strumenti e operazioni di pagamento (es. IBAN, dati relativi a conti correnti e conti di moneta elettronica, estremi identificativi di strumenti di pagamento, dati relativi a transazioni di pagamento);
    f. eventuali categorie particolari di dati, ove volontariamente forniti dagli interessati;
    g. dati comunicati spontaneamente dagli interessati, anche compresi nelle categorie precedenti.
7. Le categorie di interessati sono:
    a. dipendenti e collaboratori della Committente;
    b. utenti finali dei prodotti e servizi gestiti dalla Committente.
8. Nell'esecuzione del Contratto, il Fornitore si impegna a:
    a. rispettare la normativa vigente in materia di trattamento dei dati personali, ivi comprese le norme che saranno emanate nel corso della durata del Contratto;
    b. trattare i dati personali per le sole finalità specificate e nei limiti dell'esecuzione delle prestazioni contrattuali;
    c. trattare i dati conformemente alle istruzioni impartite dalla Committente, che il Fornitore si impegna a far osservare anche alle persone da questi autorizzate ad effettuare il trattamento dei dati personali oggetto del Contratto, d'ora in poi "persone autorizzate"; nel caso in cui ritenga che un'istruzione costituisca una violazione del Regolamento UE sulla protezione dei dati o delle altre disposizioni di legge relative alla protezione dei dati personali, il Fornitore deve informare immediatamente la Committente;
    d. garantire la riservatezza dei dati personali trattati nell'ambito del contratto e verificare che le persone autorizzate a trattare i dati personali in virtù del Contratto:
    e. si impegnino a rispettare la riservatezza o siano sottoposti ad un obbligo legale appropriato di segretezza;
    f. ricevano la formazione necessaria in materia di protezione dei dati personali;

g. trattino i dati personali osservando le istruzioni impartite dal Titolare per il trattamento dei dati personali ;
h. adottare politiche interne e attuare misure che soddisfino i principi della protezione dei dati personali fin dalla progettazione di tali misure (privacy by design), nonché adottare misure tecniche ed organizzative adeguate per garantire che i dati personali siano trattati, in ossequio al principio di necessità ovvero che siano trattati solamente per le finalità previste e per il periodo strettamente necessario al raggiungimento delle stesse (privacy by default);
i. adottare tutte le misure tecniche ed organizzative che soddisfino i requisiti del Regolamento UE anche al fine di assicurare un adeguato livello di sicurezza dei trattamenti, in modo tale da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, modifica, divulgazione non autorizzata, nonchè di accesso non autorizzato, anche accidentale o illegale, o di trattamento non consentito o non conforme alle finalità della raccolta;
j. su eventuale richiesta della Committente assistere quest'ultima nello svolgimento della valutazione d'impatto sulla protezione dei dati, conformemente all'articolo 35 del Regolamento UE e nella eventuale consultazione del Garante per la protezione dei dati personali, prevista dall'articolo 36 del medesimo Regolamento UE;
k. ai sensi dell'art. 30 del Regolamento UE, tenere un Registro delle attività di trattamento effettuate sotto la propria responsabilità e cooperare con la Committente e con l'Autorità Garante per la protezione dei dati personali, mettendo il predetto Registro a disposizione della Committente e dell'Autorità, laddove ne venga fatta richiesta ai sensi dell'art. 30 comma 4 del Regolamento UE;

9. Tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, il Fornitore fornisce e aggiorna nel tempo un piano di misure di sicurezza rimesse all'approvazione della Committente medesima, che saranno concordate al fine di mettere in atto misure tecniche ed organizzative idonee per garantire un livello di sicurezza adeguato al rischio e per garantire il rispetto degli obblighi di cui all'art. 32 del Regolamento. Tali misure comprendono tra le altre, se del caso:
    a. la pseudonimizzazione e la cifratura dei dati personali;
    b. la capacità di assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi che trattano i dati personali;
    c. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
    d. una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
10. Il Fornitore deve mettere a disposizione della Committente e tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al

Regolamento UE, oltre a contribuire e consentire alla Committente - anche tramite soggetti terzi dal medesimo autorizzati, dandogli piena collaborazione - verifiche periodiche, ispezioni e audit circa l'adeguatezza e l'efficacia delle misure di sicurezza adottate ed il pieno e scrupoloso rispetto delle norme in materia di trattamento dei dati personali. A tal fine, la Committente informa preventivamente il Fornitore con un preavviso minimo di quattro giorni lavorativi.

11. Nel caso in cui all'esito di tali verifiche periodiche, ispezioni e audit le misure di sicurezza dovessero risultare inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione del Regolamento, o risulti che il Fornitore agisca in modo difforme o contrario alle istruzioni fornite dalla Committente, quest'ultima diffiderà il Fornitore ad adottare tutte le misure più opportune o a tenere una condotta conforme alle istruzioni entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a seguito della diffida, resa anche ai sensi dell'art. 1454 cc, la Committente potrà, in ragione della gravità della condotta del Fornitore e fatta salva la possibilità di fissare un ulteriore termine per l'adempimento, risolvere il contratto ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.
12. In alternativa alle verifiche di cui sopra, la Committente potrà richiedere al Fornitore di fornire annualmente o comunque su richiesta della Committente una relazione sull'andamento della gestione dei dati personali e sull'applicazione delle misure di sicurezza approvate.
13. Il Fornitore può avvalersi di ulteriori sub-Responsabili per delegargli attività specifiche, previa autorizzazione scritta della Committente.
14. Il sub-Responsabile del trattamento deve rispettare obblighi analoghi a quelli forniti dalla Committente al Fornitore o, riportate in uno specifico contratto o atto di nomina. Spetta al Fornitore assicurare che il sub-Responsabile del trattamento presenti garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per l'adozione di misure tecniche ed organizzative appropriate di modo che il trattamento risponda ai principi e alle esigenze del Regolamento.
15. In caso di violazione da parte del sub-Responsabile del trattamento o degli obblighi in materia di protezione dei dati, il Fornitore del trattamento è interamente responsabile nei confronti della Committente di tali inadempimenti. La Committente potrà in qualsiasi momento verificare le garanzie e le misure tecniche ed organizzative del sub-Responsabile, tramite audit verifiche e ispezioni anche avvalendosi di soggetti terzi. A tal fine, La Committente informa preventivamente il Fornitore con un preavviso minimo di 4 (quattro) giorni lavorativi.
16. Ove tali misure dovessero risultare inapplicate o inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione del Regolamento, o risulti che il Sub responsabile/terzo autorizzato agisca in modo difforme o contrario alle istruzioni fornite dalla Committente, quest'ultima diffiderà il Fornitore a far adottare al sub-Responsabile tutte le

misure più opportune o a tenere una condotta conforme alle istruzioni entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a tale diffida, resa anche ai sensi dell'art. 1454 cc, la Committente potrà, in ragione della gravità della condotta del sub-Responsabile e fatta salva la possibilità di fissare un ulteriore termine per l'adempimento, risolvere il contratto con il Fornitore ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.

17. In alternativa alle verifiche di cui sopra, la Committente potrà richiedere al Fornitore di fornire annualmente o comunque su richiesta una relazione sull'andamento della gestione dei dati personali e sull'applicazione delle misure di sicurezza approvate da parte del sub-Responsabile.
18. Il Fornitore manleverà e terrà indenne la Committente da ogni perdita, contestazione, responsabilità, spese sostenute nonché dei costi subiti (anche in termini di danno reputazionale) in relazione anche ad una sola violazione della normativa in materia di Trattamento dei Dati Personali e/o del Contratto (inclusi gli Allegati) derivata dalla condotta (attiva e/o omissiva) sua e/o dei suoi agenti e/o subappaltatori e/o sub-contraenti.
19. Il Fornitore deve assistere la Committente al fine di dare seguito alle richieste per l'esercizio dei diritti degli interessati; qualora gli interessati esercitino tale diritto presso il Fornitore, quest'ultimo è tenuto ad assistere la Committente, nei tempi stabiliti dal Contratto e con le modalità concordate, al fine di fornire adeguato riscontro agli interessati nei termini prescritti.
20. Il Fornitore informa tempestivamente e, in ogni caso senza ingiustificato ritardo dall'avvenuta conoscenza, la Committente di ogni violazione di dati personali (cd. data breach); tale notifica è accompagnata da ogni documentazione utile, ai sensi degli artt. 33 e 34 del Regolamento UE, per permettere al Titolare del trattamento, ove ritenuto necessario, di notificare questa violazione all'Autorità Garante per la protezione dei dati personali, entro il termine di 72 ore da quanto il Titolare ne viene a conoscenza; nel caso in cui il Titolare debba fornire informazioni aggiuntive all'Autorità di controllo, il Fornitore si impegna a supportare la Committente o , se diverso, il Titolare nell'ambito di tale attività.
21. Il Fornitore deve avvisare tempestivamente e senza ingiustificato ritardo la Committente in caso di ispezioni, di richiesta di informazioni e di documentazione da parte dell'Autorità Garante per la protezione dei dati personali; inoltre, deve assistere la Committente nel caso di richieste formulate dall'Autorità Garante in merito al trattamento dei dati personali effettuate in ragione del contratto.
22. Il Fornitore deve comunicare alla Committente il nome ed i dati del proprio "Responsabile della protezione dei dati" e il Referente Privacy di cui al Contratto, comunicando tempestivamente alla Committente qualsiasi variazione; il Responsabile della protezione dei dati personali del Fornitore, anche tramite il Referente Privacy, collabora e si tiene in costante contatto con il Responsabile della protezione dei dati della Committente.

23. Il Fornitore ha stipulato e mantiene per la durata del Contratto adeguata polizza assicurativa con primaria compagnia di assicurazione, per i rischi correlati alla c.d. Cyber liability, con i massimali di cui al Contratto.
24. Al termine della prestazione dei servizi oggetto del contratto, il Fornitore su richiesta della Committente, si impegna a:
    a. restituire alla Committente i supporti rimovibili eventualmente utilizzati su cui sono memorizzati i dati;
    b. distruggere tutte le informazioni registrate su supporto fisso, documentando per iscritto l'adempimento di tale operazione.
25. Il Fornitore informa preventivamente la Committente se a individuare e a designare per iscritto gli amministratori di sistema mettendo a disposizione della Committente l'elenco aggiornato delle nomine e i log di accesso, che devono comprendere i riferimenti temporali e la descrizione dell'evento che ne ha determinato la generazione (per es. query).
26. Il Fornitore si impegna ad operare adottando tutte le misure tecniche e organizzative, le attività di formazione, informazione e aggiornamento ragionevolmente necessarie per garantire che i Dati Personali trattati in esecuzione del contratto, siano precisi, corretti e aggiornati nel corso della durata del trattamento - anche qualora il trattamento consista nella mera custodia o attività di controllo dei dati - eseguito dal Fornitore, o da un sub-Responsabile.
27. Il Fornitore non può trasferire i dati personali verso un paese terzo o un'organizzazione internazionale, salvo che non abbia preventivamente ottenuto l'autorizzazione scritta da parte della Committente. In tal caso il Fornitore si obbliga a stipulare le Clausole Contrattuali Standard della Commissione Europea e gli obblighi aggiuntivi contenuti nell'Appendice 1 del presente DPA. In ogni caso, il Fornitore assicura il rispetto delle misure di garanzie previste dal Regolamento e, a richiesta, ne fornisce prova alla Committente senza ritardo.
28. Sarà obbligo della Committente vigilare durante tutta la durata del trattamento, sul rispetto degli obblighi previsti dalle presenti istruzioni e dal Regolamento sulla protezione dei dati da parte del Fornitore, nonché a supervisionare l'attività di trattamento dei dati personali effettuando audit, ispezioni e verifiche periodiche sull'attività posta in essere dal Fornitore.
29. Durante l'esecuzione del Contratto, nell'eventualità di qualsivoglia modifica della normativa in materia di Trattamento dei Dati Personali che generi nuovi requisiti (ivi incluse nuove misure di natura fisica, logica, tecnica, organizzativa, in materia di sicurezza o trattamento dei dati personali), il Fornitore si impegna a collaborare - nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse - con la Committente e affinché siano sviluppate, adottate e implementate misure correttive di adeguamento ai nuovi requisiti.

PagoPA S.p.A.
Giuseppe VIRGONE
f.to digitalmente

PER ACCETTAZIONE
Il Fornitore
f.to digitalmente

Appendice 1 al DPA

APPENDIX 3

ADDITIONAL SAFEGUARDS TO STANDARD CONTRACTUAL CLAUSES

1. The data importer will assess whether the laws applicable to it provide adequate protection under European Union ("**EU**") data protection law. If and to the extent that it determines that any such laws are likely to have a substantial adverse effect on the level of data protection offered by the Standard Contractual Clauses and required under European data protection law, it undertakes to comply with the safeguards set out in paragraphs 2 to 4 below.

2. The data importer undertakes to adopt supplementary measures to protect the personal data received under the Standard Contractual Clauses from the data exporter ("SCC Personal Data") in accordance with the requirements of EU data protection law, including by implementing appropriate technical and organizational safeguards, such as encryption or similar technologies, access controls or other compensating controls, to protect personal data against any interference that goes beyond what is necessary in a democratic society to safeguard national security, defence and public security[u1] .

3. In the event that the data importer receives a legally binding request for access to the SCC Personal Data by a public authority, it will promptly notify the data exporter of such request to enable the data exporter to intervene and seek relief from such disclosure, unless the data importer is otherwise prohibited from providing such notice, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. If the data importer is so prohibited:

(a) It will use its reasonable best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible, and be able to demonstrate that it did so.

(b) In the event that, despite having used its reasonable best efforts, the data importer is not permitted to notify the data exporter, it will make available on an annual basis general information on the requests it received to the data exporter and/or the competent supervisory authority of the data exporter.

(c) Oppose any such request for access and contest its legal validity to the extent legally permitted under applicable law.

4. In the event of any request for access to the SCC Personal Data by a public authority, the data importer will:

(a) comply with a Data Disclosure Policy, to be provided at request;

(b) not make any disclosures of the SCC Personal Data to any public authority that are determined to be massive, disproportionate and indiscriminate in a manner that it would go beyond what is necessary in a democratic society; and

(c) upon request from the data exporter, provide general information on the requests from public authorities it received in the preceding 12 month period relating to SCC Personal Data.