

## Atto di designazione del Responsabile del trattamento dei dati personali

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

**VISTO** il contratto (di seguito anche "Contratto") relativo alla procedura contraddistinta dal n. CIG n. **8284797ECO**, sottoscritto dalla PagoPA S.p.A. (di seguito anche "**Società**") in data 16 giugno 2020, per l'affidamento a Fabrick S.p.A. (C.F. e iscrizione al Registro delle Imprese di Biella n. 02654890025, P.I. 02675650028) (di seguito anche "**Fornitore**") dell'implementazione *della Soluzione tecnologica Check-iban e dei Servizi evolutivi*, così come dettagliati nel predetto Contratto e nell'Offerta (come definita nel Contratto) proposta dal Fornitore e accettata dalla Società;

**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 Fabrick S.p.A. 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 dell'Amministratore Unico **Giuseppe Virgone**

## DESIGNA

Fabrick S.p.A. (C.F. e iscrizione al Registro delle Imprese di Biella n. 02654890025, P.I. 02675650028), in persona del suo Legale Rappresentante, l'Amministratore Delegato Paolo Zaccardi, con sede legale in Biella, Piazza Gaudenzio Sella, n. 1 - 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 **8284797EC0**, che qui si intende integralmente richiamato.

Per le attività per le quali la Società 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 precisa quanto segue.

Il Fornitore s'impegna a garantire la massima riservatezza e a non divulgare a terzi informazioni, dati etc., anche relativi alla Società, di cui verrà a conoscenza nell'ambito dello svolgimento delle attività oggetto del Contratto.

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.

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 e si impegna ad effettuare, per conto della Società, 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 in conformità alle istruzioni nel seguito fornite.

Il Fornitore si impegna a presentare, su richiesta della Società, 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.

Le finalità del trattamento sono: esecuzione del contratto.

Il tipo di dati personali trattati in ragione delle attività oggetto del contratto sono:

- dati comuni (es. dati anagrafici e di contatto, dati bancari compreso il codice IBAN);
- eventuali categorie particolari di dati, ad esclusione dei dati giudiziari;

Le categorie di interessati sono: personale in forze (dipendente e non dipendente) alla Società/personale incaricato dagli enti; utenti e fruitori dei prodotti digitali curati e gestiti dalla Società; utenti di servizi e prodotti offerti da enti terzi che si rivolgono alla Società per la fornitura di servizi.

Nell'esercizio delle proprie funzioni, il Fornitore si impegna 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;
- trattare i Dati Personali per le sole finalità specificate e nei limiti dell'esecuzione delle prestazioni contrattuali;
- trattare i dati conformemente alle istruzioni impartite dalla Società, 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 Società;

- 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:
  - si impegnino a rispettare la riservatezza o siano sottoposti ad un obbligo legale appropriato di segretezza;
  - ricevano la formazione necessaria in materia di protezione dei dati personali;
  - trattino i Dati Personali osservando le istruzioni impartite dal Titolare per il trattamento dei dati personali;
- 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);
- 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, nonché di accesso non autorizzato, anche accidentale o illegale, o di trattamento non consentito o non conforme alle finalità della raccolta;
- su eventuale richiesta della Società 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;
- ai sensi dell'art. 30 del Regolamento UE, tenere un Registro delle attività di trattamento effettuate sotto la propria responsabilità e cooperare con la Società e con l'Autorità Garante per la protezione dei dati personali, mettendo il predetto Registro a disposizione della Società e dell'Autorità, laddove ne venga fatta richiesta ai sensi dell'art. 30 comma 4 del Regolamento UE;

Tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, il Fornitore si impegna, su richiesta della Società, a fornirle un piano di misure di sicurezza rimesse all'approvazione della Società 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 UE. Tali misure comprendono tra le altre, se del caso:

- la pseudonimizzazione e la cifratura dei Dati Personali;
- la capacità di assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi che trattano i Dati Personali;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Il Fornitore deve mettere a disposizione della Società e tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al Regolamento UE, oltre a contribuire e consentire alla Società - 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 Società informa preventivamente il Fornitore con un preavviso minimo di quattro giorni lavorativi.

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 Società, 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 Società 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 nei limiti previsti dal presente Contratto.

In alternativa alle verifiche di cui sopra, la Società potrà richiedere al Fornitore di fornire annualmente o comunque su richiesta della Società una relazione sull'andamento della gestione dei Dati Personali e sull'applicazione delle misure di sicurezza approvate.

Il Fornitore può avvalersi di ulteriori sub-Responsabili per delegargli attività specifiche, previa autorizzazione scritta della Società .

Il sub-Responsabile del trattamento nominato dal Fornitore deve rispettare obblighi analoghi a quelli forniti dalla Società 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 UE.

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 Società di tali inadempimenti. La Società 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 Società informa preventivamente il Fornitore con un preavviso minimo di quattro giorni lavorativi.

Ove tali misure dovessero risultare inapplicate o inadeguate rispetto al rischio del trattamento o, comunque, inadeguate ad assicurare l'applicazione del Regolamento, o risulti che il Sub responsabile/terzo autorizzato agisca in modo difforme o contrario alle istruzioni fornite dalla Società, 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 Società 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 nei limiti previsti dal presente Contratto.

In alternativa alle verifiche di cui sopra, la Società 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.

Il Fornitore nei limiti previsti dal presente Contratto manleverà e terrà indenne la Società 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 e la documentazione correlata, ove presente) derivata dalla condotta (attiva e/o omissiva) sua e/o dei suoi agenti e/o subappaltatori e/o sub-contraenti.

Il Fornitore deve assistere la Società 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 inoltrare tempestivamente, e comunque nel più breve tempo possibile, le istanze alla Società supportando quest'ultimo al fine di fornire adeguato riscontro agli interessati nei termini prescritti.

Il Fornitore informa tempestivamente e, in ogni caso senza ingiustificato ritardo dall'avvenuta conoscenza, la Società di ogni violazione dei 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 quando 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 Società o, se diverso, il Titolare nell'ambito di tale attività.

Il Fornitore deve avvisare tempestivamente e senza ingiustificato ritardo la Società 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 Società nel caso di richieste formulate dall'Autorità Garante in merito al trattamento dei dati personali effettuate in ragione del Contratto.

Il Fornitore deve comunicare alla Società il nome e i recapiti del proprio Responsabile della protezione dei dati (di seguito "**DPO**"), nonché il nome e i recapiti di un referente dedicato (di seguito "**Referente Privacy**"), avente una seniority di almeno 4 anni su tematiche privacy e appartenente all'ufficio del DPO del Fornitore; il DPO del Fornitore collabora e si tiene in costante contatto, anche tramite il Referente Privacy, con il DPO e l'eventuale referente privacy della Società. Senza pregiudizio dell'obbligo di informare la Società tempestivamente e senza ritardo rispetto a qualsiasi violazione dei Dati Personali, in caso di richiesta di assistenza su tematiche privacy, il Referente Privacy deve fornire un primo riscontro alla Società, con conferma di presa in carico entro 24 ore, 7 giorni su 7, e con immediata fornitura di tempistiche certe di riscontro/attuazione/output. Il Referente Privacy deve assicurare la produzione della documentazione richiesta senza ingiustificato ritardo e comunque entro e non oltre 7 (sette) giorni lavorativi dal riscontro della predetta richiesta di assistenza, salvo diverso termine concordato con la Società.

Al termine della prestazione dei servizi oggetto del Contratto, ovvero alla cessazione per qualsiasi causa del Contratto, il Fornitore su richiesta della Società, si obbliga a:

- a) restituire alla Società copia di tutte le informazioni relative al Contratto e ai Dati Personali, in conformità ai tracciati, ai modelli e alle modalità concordate con la Società;
- b) restituire alla Società i supporti rimovibili eventualmente utilizzati per la memorizzazione dei Dati Personali;
- c) distruggere tutte le informazioni relative al Contratto e ai Dati Personali, comunque memorizzate o altrimenti incorporate su qualunque supporto, fornendo per iscritto prova dell'adempimento di tale operazione, senza pregiudizio degli obblighi di conservazione previsti dalla normativa vigente, compresa la normativa in tema di trattamento dei dati personali.

Il Fornitore si impegna a individuare e a designare per iscritto gli amministratori di sistema mettendo a disposizione della Società l'elenco aggiornato delle nomine.

Il Fornitore si impegna a comunicare tempestivamente alla Società qualunque variazione in merito ai nominativi e ai recapiti del proprio DPO, del Referente Privacy e degli amministratori di sistema.

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 Personali - eseguito dal Fornitore o da un sub-Responsabile.

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 Società. In tal caso il Fornitore assicura il rispetto delle misure di garanzie previste dal Regolamento EU e, a richiesta, ne fornisce prova alla Società senza ritardo.

Sarà obbligo della Società vigilare durante tutta la durata del trattamento, sul rispetto degli obblighi previsti dalle presenti istruzioni e dal Regolamento UE 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.

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 Società affinché siano sviluppate, adottate e implementate misure correttive di adeguamento ai nuovi requisiti.

Oltre agli obblighi di cui sopra, il Fornitore si impegna altresì al rispetto degli obblighi e delle eventuali istruzioni sul trattamento indicati nella DPIA consegnata alla Committente e da quest'ultima approvata, i quali saranno controfirmati dal Fornitore per presa visione e si riterranno vincolanti per lo stesso ai sensi dell'art. 28 GDPR.

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

**PER ACCETTAZIONE**  
**Il Fornitore**  
***f.to digitalmente***