ALLEGATO C

Palermo, _____

Oggetto: Accordo di designazione tra il Titolare del Trattamento e il Responsabile del Trattamento

Ente/Azienda: Comune di Palermo
con sede legale in: Piazza Pretoria 1
CAP: 90133, CITTÀ: Palermo,
Partita Iva n. 80016350821

in qualità di Titolare del Trattamento (di seguito anche Titolare) ha deciso di avvalersi di soggetti esterni nell'attività di trattamento di dati personali, affidando ad essi determinate attività che restano nella sfera della sua titolarità e che non comportano decisioni sulle finalità e sulle modalità di utilizzazione dei dati. Pertanto, il Titolare

DESIGNA

Azienda/Ente ……..
con sede legale in: ……
CAP: ……, CITTÀ: ……
Partita Iva/CF: ……

a Responsabile del Trattamento (di seguito anche Responsabile o Fornitore) ai sensi dell'Articolo 28 del Regolamento UE 2016/679 (di seguito anche GDPR)
Il Responsabile presenta adeguata e documentata esperienza, capacità ed affidabilità in relazione ai compiti ad esso affidati dal Titolare nonché idonea organizzazione tecnica, organizzativa e di risorse atte ad eseguirla. Il Responsabile, accettando la presente designazione, conferma e garantisce il rispetto delle vigenti disposizioni in materia di trattamento di dati personali, anche con riferimento al profilo relativo alla sicurezza (attraverso l'adozione di misure tecniche e organizzative adeguate ai sensi dell'art. 32 del Regolamento UE 2016/679) e al rispetto dei diritti dell'interessato.

1. Premessa dell'accordo sul trattamento dei dati

Il presente Accordo sul trattamento dei dati stabilisce i diritti e gli obblighi che si applicano al trattamento dei dati personali da parte del Responsabile del trattamento per conto del Titolare.
Il presente accordo è stato progettato per garantire la conformità delle parti all'articolo 28 del *Regolamento UE 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla tutela delle persone fisiche con riguardo al trattamento dei dati personali e sulla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (GDPR)*, che stabilisce requisiti specifici per il contenuto degli accordi sul trattamento dei dati.

Il trattamento dei dati personali da parte del Responsabile del trattamento ha luogo ai fini dell'adempimento del "Contratto generale" stipulato dalle Parti. **Convenzione finalizzata all'erogazione di buoni servizio a sostegno delle famiglie finanziati con fondi extra comunali.**

Il Contratto sul trattamento dei dati e il "Contratto principale" devono essere interdipendenti e non possono essere risolti separatamente. Tuttavia, l'accordo sul trattamento dei dati può - senza la risoluzione del "Contratto principale" - essere sostituito da un accordo alternativo valido per il trattamento dei dati.

Il presente Accordo ha la priorità su qualsiasi disposizione analoga contenuta in altri accordi tra le Parti, incluso il "Contratto generale".

Quattro appendici sono allegate al presente Accordo sul trattamento dei dati. Le appendici formano parte integrante del presente Accordo sul trattamento dei dati.

Appendice A. del presente Accordo contiene i dettagli del trattamento, nonché lo scopo e la natura del trattamento, il tipo di dati personali, le categorie di soggetti e la durata del trattamento.

Appendice B. del presente Accordo contiene i termini e le condizioni che si applicano all'uso dei sub-responsabili da parte del Responsabile del trattamento e, se del caso, un elenco di sub-responsabili approvati dal Titolare del trattamento.

Appendice C. del presente Accordo contiene le istruzioni impartite dal Titolare del trattamento al fine di eseguire il trattamento, le misure di sicurezza da attuare e il modo in cui gli Audit sul Responsabile o sui Sub-Responsabili devono essere eseguiti.

Appendice D. del presente Accordo contiene le disposizioni che non sono coperte dalle clausole contrattuali.

Il contratto di elaborazione dei dati e le relative appendici sono conservati per iscritto e per via elettronica da entrambe le parti.

Il presente Accordo sul trattamento dei dati non esonera il Responsabile del trattamento da alcun vincolo a cui il Responsabile del trattamento è soggetto in base al Regolamento generale sulla protezione dei dati o ad altre normative comunitarie o nazionali.

2. I diritti e gli obblighi del Titolare

Il Titolare del trattamento è responsabile nei confronti degli interessati e deve garantire che il trattamento dei dati personali avvenga nell'ambito del Regolamento generale sulla protezione dei dati e del Codice in materia di protezione dei dati d.lgs. 196/2003

Il Titolare del trattamento deve pertanto avere sia il diritto che l'obbligo di prendere decisioni in merito alle finalità e ai mezzi di trattamento dei dati personali.

Il Titolare del trattamento ha la responsabilità di garantire che il trattamento di cui è incaricato il Responsabile del Trattamento sia conforme alle norme di legge.

3. Il Responsabile del Trattamento dei dati agisce secondo le istruzioni

Il Responsabile del trattamento dei dati è autorizzato a trattare i dati personali solo su istruzioni documentate del Titolare del trattamento a meno che il trattamento non sia richiesto dalla legislazione europea o nazionale a cui è soggetto il Responsabile del trattamento; in tal caso, il Responsabile del trattamento dei dati informa il Titolare del trattamento di questo requisito legale prima del trattamento, a meno che la legge non vieti tali informazioni per importanti motivi di interesse pubblico, cfr. Articolo 28, sottosezione 3, comma a. Tali istruzioni sono specificate nelle appendici A e C. Ulteriori istruzioni possono essere fornite anche dal Titolare per tutta la durata del trattamento dei dati personali, ma tali istruzioni devono sempre essere documentate e conservate in forma scritta, anche in formato elettronico.

Il Responsabile del trattamento informa immediatamente il Titolare del trattamento se, a suo parere, alcune istruzioni contravvengono al regolamento generale sulla protezione dei dati o ad altre disposizioni contenute in altre normative comunitarie o nazionali.

4. Riservatezza

Il Responsabile del trattamento dei dati garantisce che solo le persone che sono espressamente e formalmente autorizzate possano accedere ai dati personali trattati per conto del Titolare. L'accesso ai dati dovrebbe pertanto essere negato senza indugio se tale autorizzazione viene rimossa o scade.

Sono considerate autorizzate le persone che richiedono l'accesso ai dati personali per adempiere all'obbligo del Responsabile del trattamento nei confronti del Titolare del trattamento.

Il Responsabile del trattamento garantisce al Titolare che gli Addetti al trattamento dei dati personali da lui designati sono vincolati al più stretto riserbo sulla base di atti negoziali (es. codici di condotta interni, accordi di riservatezza specifici, ecc.) o disposizioni normative previste dal diritto dell'Unione o dal diritto nazionale cui il Responsabile e gli Addetti al trattamento dei dati personali sono soggetti, inoltre hanno accesso solo ai dati che hanno necessità di conoscere.

Il Responsabile del trattamento dei dati deve, su richiesta del Titolare, essere in grado di dimostrare che i dipendenti interessati sono soggetti alla riservatezza di cui al punto precedente.

5. Sicurezza del trattamento

Il responsabile del trattamento dei dati adotta tutte le misure richieste ai sensi dell'articolo 32 del regolamento generale sulla protezione dei dati, che stabilisce che, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio

Il suddetto art. 32 pone in capo al Responsabile l'obbligo di eseguire una valutazione del rischio e, a seguito, l'implementazione di misure tali da contrastare il rischio identificato. Se del caso, le misure possono comprendere quanto segue:

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 di trattamento;
c. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali 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.

Il Responsabile del trattamento garantisce quanto sopra in tutti i casi e, comunque, deve attenersi a quanto specificato nell'Appendice C del presente Accordo.
Se nella valutazione del responsabile del trattamento, la mitigazione dei rischi individuati richiedono ulteriori misure da attuare da parte del Titolare del trattamento, rispetto a quelli già esistenti, è necessario specificare tali misure supplementari nell'Appendice C.

6. Utilizzo di sub-responsabili del trattamento

Il responsabile del trattamento deve soddisfare i requisiti di cui all'articolo 28, sottosezioni 2 e 4, del regolamento generale sulla protezione dei dati al fine di utilizzare un altro responsabile del trattamento (sub-responsabile).

L'incarico conferito dovrà essere disciplinato da un atto di designazione a responsabile del trattamento conforme a quanto previsto dall'Articolo 28, comma 2 e 4, del Regolamento UE 679/2016. In caso di autorizzazione scritta generale, il Responsabile del trattamento dovrà informare il Titolare di eventuali designazioni o sostituzioni dei sub-responsabili del trattamento, il Titolare del trattamento si riserva la facoltà di opporvisi, per giusta causa nel termine di 30 giorni dal momento in cui viene informato della circostanza da parte del Responsabile.

In caso di consenso scritto generale, il Responsabile del trattamento dei dati informa il Titolare del trattamento di eventuali modifiche pianificate rispetto alle aggiunte o alla sostituzione di altri responsabili del trattamento dei dati e offre quindi al Titolare del trattamento la possibilità di opporsi a tali modifiche.

Il Responsabile del trattamento, salvo il diritto di rivalersi nei di loro confronti, risponde dei danni causati nel corso delle operazioni di trattamento dall'operato dei soggetti autorizzati dal Responsabile e dei sub-responsabili.

I requisiti del Titolare del trattamento per l'utilizzo da parte del Responsabile del trattamento di sub-responsabili sono descritti nell'Appendice B al presente Accordo.

Quando il Titolare ha autorizzato un sub-Responsabile, il Responsabile del trattamento deve garantire che i trattamenti svolti dal Sub-Responsabile siano soggetti alle stesse garanzie di protezione dei dati specificate nel presente Accordo sul trattamento dei dati sulla base di un contratto o altro documento legale ai sensi del diritto dell'UE o del diritto nazionale degli Stati membri, in particolare fornendo le garanzie necessarie affinché il sub-responsabile attui le misure tecniche e organizzative appropriate in modo tale che il trattamento soddisfi i requisiti del regolamento generale sulla protezione dei dati.

Il Responsabile del trattamento dei dati è incaricato - sulla base di un accordo - di richiedere che il sub-responsabile ottemperi almeno agli obblighi a cui è soggetto il Responsabile del trattamento in conformità con i requisiti del Regolamento generale sulla protezione dei dati e a questo Accordo e relative appendici.

Una copia di tale accordo di sub-responsabile e successive modifiche deve - su richiesta del Titolare del trattamento - essere presentata al Responsabile del trattamento che avrà così l'opportunità di garantire che sia stato stipulato un accordo valido tra il Responsabile del trattamento e il sub-responsabile. I termini e le condizioni commerciali, come i prezzi, che non influiscono sul contenuto legale di protezione dei dati non sono richiesti.

Il Responsabile del trattamento dei dati, nel suo accordo con il Sub-Responsabile, include il Titolare del trattamento come terza parte. In caso di fallimento o chiusura del rapporto del Responsabile del trattamento dei dati questo deve consentire al Titolare del trattamento di assumere diritti sul sub-responsabile in modo da poter richiedere al Sub-Responsabile di eseguire la cancellazione o la restituzione dei dati.

7. Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Il Responsabile del trattamento è autorizzato a trattare i dati personali solo su istruzioni documentate del Titolare del trattamento, anche per quanto riguarda il trasferimento (cessione, divulgazione e uso interno) di dati personali a paesi terzi o organizzazioni internazionali, a meno che il trattamento non sia richiesto ai sensi dell'UE o degli Stati membri, legislazione alla quale è soggetto il Responsabile del trattamento; in tal caso, il Responsabile del trattamento informa il Titolare, di tali requisiti legali, prima del trattamento, a meno che tale legge non vieti la divulgazione di informazioni per importanti motivi di interesse pubblico, cfr. Articolo 28, sottosezione 3, comma a.

Pertanto, senza le istruzioni o l'approvazione del Titolare, il Responsabile del trattamento - nell'ambito del presente Accordo sul trattamento dei dati non deve:

a) divulgare i dati personali a un responsabile del trattamento in un paese terzo o in un'organizzazione internazionale;
b) assegnare il trattamento di dati personali a un sub-responsabile in un paese terzo;
c) far elaborare i dati in un'altra delle società del Responsabile del trattamento che si trova in un paese terzo.

Le istruzioni del responsabile del trattamento dei dati personali per il trasferimento verso un paese terzo, se applicabile, sono stabilite nell'Appendice C al presente Accordo.

8. Assistenza al Titolare del trattamento

Il Responsabile, tenuto conto della natura del trattamento, assiste, per quanto possibile, il Titolare con adeguate misure tecniche e organizzative, nell'adempimento dell'obbligo del Titolare di rispondere alle richieste di esercizio delle persone interessate "diritti" di cui al capitolo 3 del regolamento generale sulla protezione dei dati.
Ciò implica che il Responsabile del trattamento dovrebbe, per quanto possibile, assistere il Titolare nelle seguenti attività:

a) Informare gli interessati, ai sensi dell'art. 13 del GDPR, prima della raccolta di dati personali;
b) Informare gli interessati, ai sensi dell'art. 14 del GDPR, se i dati personali non sono stati ottenuti direttamente dall'interessato;
c) Gestire le richieste degli interessati sul:
    a. diritto di accesso;
    b. diritto alla rettifica
    c. diritto alla cancellazione ("il diritto all'oblio")
    d. diritto di limitare l'elaborazione
    e. diritto alla portabilità dei dati
    f. diritto di opposizione
    g. diritto di opporsi al risultato di processi decisionali individuali automatizzati, compresa la profilazione
d) Informare l'interessato in merito alla rettifica o alla cancellazione dei dati personali o alla limitazione del trattamento.

Il Responsabile del trattamento assiste il Titolare nel garantire il rispetto degli obblighi ai sensi degli articoli 32-36 del Regolamento generale sulla protezione dei dati, tenendo conto della natura del trattamento e dei dati resi disponibili al Responsabile del trattamento, cfr. Articolo 28, sottosezione 3, comma f.

Ciò implica che il Responsabile del trattamento dei dati dovrebbe, per quanto possibile, tenendo conto della natura del trattamento, assistere il Titolare nelle seguenti attività:

a) Attuare adeguate misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio associato al trattamento;
b) Denunciare le violazioni dei dati personali all'autorità di controllo (Autorità Garante per la protezione dei dati) senza indebito ritardo e, se possibile, entro 72 ore dal momento in cui il Titolare rileva tale violazione a meno che, sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche;
c) Informare l'interessato - senza indebito ritardo -della violazione dei dati personali quando è probabile che tale violazione comporti un rischio elevato per i diritti e le libertà delle persone fisiche;
d) Svolgere una valutazione d' impatto sulla protezione dei dati, se un tipo di trattamento può comportare un rischio elevato per i diritti e le libertà delle persone fisiche;
    e) Consultare l'autorità di controllo (Autorità Garante per la protezione dei dati) prima dell'elaborazione, se la valutazione d'impatto sulla protezione dei dati mostra che il trattamento comporterà un rischio elevato e in mancanza di misure idonee a limitare il rischio.

Le parti definiscono nell'Appendice C le misure tecniche e organizzative adeguate con cui il responsabile del trattamento è tenuto ad assistere il titolare del trattamento, nonché la portata e l'entità dell'assistenza necessaria.

9. Notifica di violazione dei dati personali

In caso di identificazione di una violazione di dati personali presso le strutture del Responsabile del trattamento dei dati o di un sub-responsabile, il Responsabile informa il Titolare con prontezza fornendo le opportune informazioni (secondo le informazioni richieste dall'Autorità Garante al momento dell'indicente).

La notifica del Responsabile del trattamento al Titolare deve, se possibile, avvenire entro al massimo 48 h dopo che il Responsabile del trattamento ha individuato la violazione per consentire al Titolare di adempiere al proprio obbligo, se applicabile, di denunciare la violazione all'Autorità Garante entro 72 ore.

Secondo la clausola 8 del presente Accordo, il Responsabile del trattamento dei dati, tenendo conto della natura del trattamento e dei dati disponibili, assiste il Titolare nel segnalare la violazione all'autorità di controllo. Ciò può significare che il Responsabile del trattamento dei dati è tenuto a fornire assistenza per ottenere le informazioni che, in conformità con l'articolo 33, sottosezione 3 del Regolamento generale sulla protezione dei dati, devono essere dichiarate nella relazione del Titolare del trattamento all'autorità di controllo (e almeno):

a) La natura della violazione dei dati personali, inclusi, se possibile, le categorie e il numero approssimativo di interessati e le categorie e il numero approssimativo di record di dati personali interessati;
a) Probabili conseguenze di una violazione dei dati personali;
b) Misure adottate o proposte per gestire la violazione dei dati personali, comprese, se del caso, misure per limitare il suo possibile danno.

Le parti definiscono nell'Appendice D tutti gli elementi che devono essere forniti dal Responsabile, quando assiste il titolare del trattamento nella notifica di una violazione dei dati personali alle autorità di vigilanza competenti.

10. Cancellazione e restituzione dei dati

Alla cessazione del servizio, il Responsabile del trattamento è tenuto, a discrezione del Titolare, a cancellare o restituire tutti i dati personali in suo possesso a meno che il diritto dell'UE o il diritto nazionale non richiedano la conservazione obbligatoria.

11. Ispezioni e Audit

Il Titolare del trattamento si riserva la facoltà di effettuare visite di controllo, direttamente o per il tramite di suoi incaricati eventualmente esterni al Titolare stesso, presso il Responsabile. Il Titolare si impegna a dare preventiva comunicazione delle visite di controllo e, qualora svolte da parte di incaricati esterni al Titolare, di indicarne i riferimenti e nominativi delle persone coinvolte e l'ambito di verifica ad essi conferito nell'incarico.

Il Responsabile del trattamento mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare la conformità con l'articolo 28 del Regolamento generale sulla protezione e del presente Accordo e per consentire e contribuire agli audit, comprese le ispezioni eseguite dal Titolare o da altri revisori inviati dal Titolare.

Le procedure applicabili all'ispezione del Responsabile del trattamento da parte del Titolare del trattamento sono specificate nell'Appendice C al presente Accordo sul trattamento dei dati.

L'ispezione dei sub-processori da parte del Titolare del trattamento, se applicabile, deve di norma essere eseguita tramite il Responsabile del trattamento. Le procedure per tale ispezione sono specificate nell'appendice C al presente Accordo sul trattamento dei dati.

Il Responsabile del trattamento è tenuto a fornire alle autorità di controllo, che hanno accesso alle strutture del Titolare e del Responsabile del trattamento, o ai rappresentanti che agiscono per conto di tali autorità di controllo, l'accesso alle strutture fisiche del Responsabile.

12. Entrata in vigore

Il presente Accordo sul trattamento dei dati entrerà in vigore alla data della firma da entrambe le Parti.

Entrambe le Parti hanno il diritto di richiedere la rinegoziazione del presente Accordo sul trattamento dei dati qualora le modifiche alla legge o l'inesattezza delle disposizioni contenute nel presente documento comportino tale rinegoziazione.

Il presente Accordo sul trattamento dei dati può essere risolto in conformità con i termini e le condizioni di risoluzione definite nel Contratto generale.

Il presente Accordo sul trattamento dei dati si applica fino a quando il trattamento è eseguito. Indipendentemente dalla risoluzione del "Contratto principale" e / o del presente Accordo, il Contratto sul trattamento dei dati rimarrà in vigore fino al termine del trattamento e alla cancellazione dei dati da parte del Responsabile del trattamento e di eventuali sub-responsabili.

Il Titolare può revocare l'incarico in caso di svolgimento delle funzioni non conforme alle istruzioni fornite, nonché per la sopravvenuta perdita dei requisiti di cui all'art. 28 del GDPR o per esigenze di interesse pubblico.

13. Responsabilità

Il Responsabile risponde ai sensi degli artt. 2043 e 2049 c.c. per qualsiasi danno cagionato al Titolare o a terzi derivante da atti, fatti o omissioni posti in essere in violazione delle disposizioni del GDPR e delle altre disposizioni in materia di protezione dei dati personali, anche da parte delle persone autorizzate e dagli amministratori di sistema. In particolare, il Responsabile risponde per i danni derivanti dal trattamento qualora abbia agito in modo difforme o contrario alle legittime istruzioni del Titolare.

14. Richieste degli interessati

Su espressa richiesta del Titolare, nella misura in cui ciò sia possibile, il Responsabile fornisce riscontro alle eventuali istanze degli interessati nei termini previsti dal GDPR. Il Responsabile prima di provvedere sottopone al Titolare la risposta da fornire in merito al trattamento dei dati

15. Corrispettivo e spese

L'esecuzione delle attività e dei compiti di cui al presente atto non genera il diritto ad alcun compenso a favore del nominato Responsabile, in quanto le già menzionate attività e compiti sono svolti nell'ambito del Capitolato Speciale d'appalto nei quali è già stata definita l'intera valutazione economica del rapporto tra le Parti.

16. Punti di contatto del titolare del trattamento e del responsabile del trattamento

Le parti possono contattarsi reciprocamente utilizzando i seguenti contatti / punti di contatto:
Nome e Cognome: ……
posizione: ……
Numero di Telefono: ……..
E-mail: ……..

Nome e Cognome: ……..

posizione: ……..

Numero di Telefono: ……

E-mail: ……

Le Parti saranno costantemente obbligate a informarsi reciprocamente delle modifiche al contratto.

Per accettazione dell'incarico
Il Responsabile del trattamento
per ……..

_____
(firma)

Il titolare del trattamento

_____
(firma)

Appendice A Informazioni sul trattamento

Lo scopo del trattamento dei dati personali da parte del Responsabile del trattamento per conto del Titolare del trattamento è la gestione dei buoni servizio a sostegno delle famiglie:

Il trattamento dei dati personali da parte del Responsabile del trattamento per conto del Titolare del trattamento riguarda principalmente dati relativi ai beneficiari dei buoni servizi

Il trattamento comprende i seguenti tipi di dati personali relativi agli interessati:

X Dati anagrafici/indirizzo e recapito/residenza

X Dati sulle abitudini di vita e sul lavoro

X Origine razziale ed etnica

X Convinzioni religiose

☐ Opinioni politiche

☐ Adesioni a partiti, sindacati o associazioni

☐ Dati di carattere filosofico

X Salute

☐ Vita sessuale

X Geolocalizzazione

X Dati giudiziari

X Dati genetici o biometrici

X Dati pseudo-sensibili (stato di bisogno o di disagio, finanziari)

Il trattamento comprende le seguenti categorie di interessati:

X Cittadini

X Cittadini residenti all'estero

X Dipendenti/collaboratori

X Minori

X Amministratori

☐ Altro.

Il trattamento dei dati personali da parte del Responsabile del trattamento per conto del Titolare del trattamento può essere eseguito solo dopo la firma del presente Accordo. L'elaborazione ha la seguente durata:

- Durata della Convenzione sottoscritta con l'A.C.

Appendice B. Termini di utilizzo dei sub-responsabili da parte del Responsabile del trattamento dei dati ed elenco dei sub-processori approvati

B1. Termini di utilizzo dei sub-responsabili da parte del Responsabile del trattamento dei dati, se applicabili

- Il Responsabile del trattamento dei potrà fruire di sub-responsabili solo previo esplicito consenso scritto del Titolare. La richiesta del Responsabile del trattamento dovrà essere inoltrata al Titolare del trattamento un minimo di 30 giorni prima dell'inizio del trattamento da parte dei sub-responsabili. Il Titolare del trattamento rifiuta il consenso solo se ci sono motivi ragionevoli e specifici per tale rifiuto.

Appendice C. Istruzioni relative all'utilizzo dei dati personali

C.1 Sicurezza del trattamento
Il livello di sicurezza dovrebbe riflettere:

Livelli Essenziali di Sicurezza.

☐ Tale trattamento comporta un ampio volume di dati personali che è soggetto all'articolo 9 del regolamento generale sulla protezione dei dati "categorie particolari di dati personali", motivo per cui è necessario un livello di sicurezza elevato.

Il Responsabile del trattamento dei dati avrà successivamente il diritto e l'obbligo di prendere decisioni in merito alle misure di sicurezza tecniche e organizzative da applicare per creare il livello necessario (e concordato) di sicurezza dei dati.

Tuttavia, il Responsabile del trattamento deve, almeno e in ogni caso, implementare le seguenti misure indicative e non esaustive, concordate con il Titolare del trattamento (sulla base della valutazione del rischio effettuata dal Titolare) e per i trattamenti definiti nell'Appendice A:

☐ **Protezione da malware.** Devono essere attuati controlli di individuazione, di prevenzione e di ripristino relativamente al malware, congiuntamente ad un'appropriata consapevolezza degli utenti. Il software antivirus è necessario per prevenire l'infezione da internet (e-mail o web-sourced), e per evitare che i virus che possono anche essere introdotti da dispositivi portatili. E 'essenziale che tale software venga aggiornato su base regolare. Devono essere previste politiche sulla vigilanza delle potenziali minacce.

Quando esiste una connettività esterna è necessario che siano presenti firewall configurati secondo le migliori best practies.

☐ **Formazione del personale.** Il Responsabile deve disporre di programmi di formazione strutturati e regolari per il personale, compresi i programmi specifici (relativi alla protezione dei dati personali) per l'inserimento dei nuovi arrivati.

☐ **Sviluppo di applicazioni software mobile.** In ogni caso lo sviluppo del codice sorgente dovrà essere conforme alle linee guida per lo sviluppo del software sicuro nella pubblica amministrazione pubblicate da AGID[1] e alle Guideline di Enisa su Smartphone Scure Development di Dicembre 2016[2].

☐ **Sviluppo di applicazioni software**. In ogni caso lo sviluppo del codice sorgente dovrà essere conforme alle linee guida per lo sviluppo del software sicuro nella pubblica amministrazione pubblicate da AGID[3].

[1] https://www.agid.gov.it/it/sicurezza/cert-pa/linee-guida-sviluppo-del-software-sicuro
[2] https://www.enisa.europa.eu/publications/smartphone-secure-development-guidelines-2016
[3] https://www.agid.gov.it/it/sicurezza/cert-pa/linee-guida-sviluppo-del-software-sicuro

☐ **Sistemi di geolocalizzazione.** In presenza della necessità di prevedere dispositivi di lettura di TAG e dispositivi di geolocalizzazione, occorre conformare la disciplina di tale funzionalità ai principi di necessità e proporzionalità in relazione alle finalità perseguite (v. art. 5, par. 1, lett. c), Regolamento), e di minimizzazione dei dati, fermo restando, se applicabile, il preventivo accordo sindacale (che costituisce condizione di liceità del trattamento), e ferma restando la preliminare informativa, chiara e completa, da fornire ai soggetti interessati dal trattamento.

Detto altrimenti, la disciplina della funzionalità di lettura di TAG e di geolocalizzazione deve prevedere al fine di rispettare i principi di necessità e proporzionalità:

- l'attivazione della funzionalità solo previa comunicazione ai soggetti interessati;
- la limitazione temporale ove applicabile;
- Tecniche di psudonimizzazione o criptazione per la conservazione dei dati di geolocalizzazione in riferimento ad un soggetto interessato, se necessario.
- la necessità di individuare modalità di trattamento dei dati raccolti conformi ai richiamati principi di protezione dei dati, compresi i tempi di conservazione, limitando la memorizzazione ai dati strettamente necessari per il raggiungimento della finalità perseguita (v. art. 5, par. 1, lett. c) ed e), del Regolamento)
- la necessità di individuare una tipologia di dispositivo che, anche per le sue caratteristiche esteriori, non sia lesiva, o comunque non risulti tale nella percezione degli interessati, della dignità degli interessati;

E' necessario predisporre una politica, prima del trattamento dei dati personali, dove deve essere data indicazione precisa dei tempi di conservazione dell'associazione della posizione del veicolo con il mezzo geolocalizzato, così da poter adottare misure organizzative preordinate all'effettiva e definitiva cancellazione dei dati contenuti nelle tabelle in questione entro e non oltre il breve periodo temporale stabilito.

Frequenza della rilevazione: occorre osservare che il Garante ha già precisato che i principi di necessità e proporzionalità non consentono, di regola, una rilevazione costante e continuativa della posizione del veicolo (già, "Gruppo articolo 29", parere n. 13, 16 maggio 2011, sui servizi di geolocalizzazione su dispositivi mobili intelligenti, WP 185, p. 15: "il datore di lavoro deve […] evitare il monitoraggio costante […e che i] dispositivi di tracciamento dei veicoli non sono dispositivi di tracciamento del personale, bensì la loro funzione consiste nel rintracciare o monitorare l'ubicazione dei veicoli sui quali sono installati. I datori di lavoro non dovrebbero considerarli come strumenti per seguire o monitorare il comportamento o gli spostamenti di autisti o di altro personale […]"). Il sistema deve quindi essere configurato in modo da consentire la rilevazione del punto geografico con una periodizzazione temporale strettamente aderente ai principi di pertinenza e non eccedenza in relazione alle finalità perseguite. Per cui si prevede che la frequenza temporale stimata sia ogni ogni 5 minuti.

Si rende necessario configurare il sistema, inserendo la previsione nell'apposito regolamento di cui al punto superiore in modo tale da consentire l'accesso ai dati trattati al solo personale autorizzato:

- tramite l'assegnazione di credenziali di autenticazione differenziate;
- individuando profili autorizzativi personalizzati;
- limitando quanto più possibile l'assegnazione di profili con funzionalità di modifica ed estrazione dei dati (cfr. provvedimento garante della privacy 19.10.2017, doc. web n. 7321142, par. 4).

- Infine, è necessario predisporre misure al fine di garantire agli interessati l'esercizio dei diritti previsti dagli articoli 15 e seguenti del Regolamento.

È necessario inoltre, configurare il sistema, affinché permetta:

l'indicazione di un'icona che indichi che la funzionalità di localizzazione è attiva:

- (solo per il personale dipendente) la configurazione del sistema consenta la disattivazione della funzionalità di localizzazione durante le pause consentite dell'attività lavorativa;
- (solo per il personale dipendente) la configurazione del sistema permetta di oscurare la visibilità della posizione geografica decorso un periodo determinato di inattività dell'operatore sul monitor presente nella centrale operativa relativamente a tale funzionalità.
- Alle suddette misure tecniche il Garante ha affiancato anche le seguenti misure organizzative:
- l'individuazione di profili differenziati di autorizzazione relativi alle diverse tipologie di dati e di operazioni eseguibili;
- l'individuazione di tempi di conservazione dei dati in concreto trattati tenendo conto delle finalità perseguite;
- la predisposizione di periodiche verifiche di test sulla funzionalità e l'affidabilità dei parametri adottati, in vista della valutazione di eventuali falsi positivi o negativi effettuati dal sistema e la conseguente predisposizione di correttivi a tutela della qualità dei dati trattati.

Requisiti minimi per la pseudonimizzazione e la crittografia dei dati personali

☐ **Crittografia.** La crittografia del disco completo dovrebbe essere abilitata su tutte le unità disco. È considerato una misura di sicurezza fondamentale quando i dati personali sono memorizzati su un dispositivo portatile o trasmessi attraverso una rete pubblica. La chiave per decifrare i dati deve essere custodita al sicuro. La chiave deve soddisfare i requisiti di complessità richiesto per le password.

☐ **Pseudonimizzazione**. I dati sensibili devono essere conservati separatamente dai dati personali.

Requisiti minimi per garantire la riservatezza, l'integrità, la disponibilità e la resilienza continua dei sistemi e dei servizi di elaborazione.

☐ **Trasferimento dei dati.**Non deve essere consentito il trasferimento di dati personali da workstation a dispositivi di archiviazione esterni (ad esempio USB, DVD, dischi rigidi esterni). Le workstation utilizzate per il trattamento dei dati personali dovrebbero non essere collegate a Internet a meno che non siano in atto misure di sicurezza per impedire l'elaborazione, la copia e il trasferimento non autorizzati dei dati personali archiviati.

☐ **Backup.** Devono essere effettuate copie di backup delle informazioni, del software e delle immagini dei sistemi e quindi sottoposte a test periodici secondo una politica di backup concordata.

☐ **Cifratura dei backup.** Le copie di backup devono essere crittografate e archiviate in modo sicuro offline.

☐ **Disaster recovery.** Le strutture per l'elaborazione delle informazioni devono essere realizzate con una ridondanza sufficiente a soddisfare i requisiti di disponibilità. Disaster recovery (non solo informatico).

☐ **File temporanei.** E' necessario creare politiche, procedure e linee guida che definiscano, termini e limitazioni dei documenti temporanei prodotti nei vari trattamenti o da procedure informatiche, queste devono includere anche i dispositivi mobili o il telelavoro. Il Responsabile del trattamento si deve uniformare alle politiche definite dal titolare.

☐ **Protezione dei dati.** Utilizzare sul perimetro della rete strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale, sul traffico uscente dalla propria rete, l'impiego di crittografia non autorizzata o l'accesso a siti che consentano lo scambio e la potenziale esfiltrazione di informazioni

Requisiti minimi per la capacità di ripristinare la disponibilità e l'accesso ai dati personali in modo tempestivo in caso di incidente fisico o tecnico.

☐ **Data Breach.** Un piano di risposta degli incidenti dovrebbe essere documentato, compreso un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli e condiviso con il Titolare del trattamento su richiesta di quest'ultimo.

Requisiti minimi per i processi di test, valutazione periodica dell'efficacia delle misure tecniche e organizzative per garantire la sicurezza del trattamento.

☐ **Logging.** È necessario definire procedure e politiche per essere in grado di identificare accesso a risorse. Un registro delle modifiche, insieme con l'autore / chi modifica, dovrebbe essere presente. Un IDS dovrebbe implementato e attivato.

☐ **Patching.** Le patch sono gli ultimi aggiornamenti dallo sviluppatore del software del sistema operativo o software applicativo. Di solito contengono correzioni a potenziali problemi di sicurezza e può essere uno strumento importante per prevenire gli attacchi di hacker o malware. L'organizzazione deve assicurarsi di avere procedure di gestione delle patch regolari, coerenti e completi.

☐ **Gestione delle vulnerabilità tecniche.** Le informazioni sulle vulnerabilità tecniche dei sistemi informativi utilizzati devono essere ottenute in modo tempestivo, l'esposizione a tali vulnerabilità deve essere valutata e appropriate misure devono essere intraprese per affrontare i rischi relativi.

☐ **Penetration Test**. I sistemi informativi devono essere regolarmente riesaminati per conformità con le politiche e con le norme per la sicurezza. La scansione automatizzata delle vulnerabilità della rete, i controlli sulle versioni e i penetrati on test possono fornire flussi regolari di informazioni, insieme a revisioni e / o audit.

Requisiti minimi per l'accesso ai dati.

☐ **Controllo accessi.** Deve essere attuato un processo formale di registrazione e deregistrazione per abilitare l'assegnazione dei diritti di accesso. L'uso di account generici (non personali) deve essere evitato. Nei casi in cui ciò è necessario, è necessario garantire che tutti gli utenti che usano l'account generico abbiano gli stessi ruoli e responsabilità. Limitazioni di accesso maggiori per dati particolari.

☐ **Controllo accessi.** Deve essere progettata e applicata la sicurezza fisica agli uffici, ai locali ed agli impianti.

☐ **Autenticazione.** Una politica specifica per la password dovrebbe essere definita e documentata. La politica deve includere almeno la lunghezza della password, la complessità, il periodo di validità e il numero di tentativi di accesso non riusciti accettabili. Le password degli utenti devono essere archiviate con criptazione sicura.

☐ **Autenticazione a due fattori.** Le modalità di autenticazione (es. autenticazione a fattore singolo o multiplo) per gli utenti, i dispositivi e altri asset sono commisurate al rischio della transazione (es. rischi legati alla sicurezza e privacy degli individui). L'autenticazione a due fattori dovrebbe essere implementata e utilizzata.

Requisiti minimi per la protezione dei dati durante la trasmissione.

☐ **Protezioni adeguate delle comunicazioni.** Devono essere redatte politiche, procedure e controlli formali a protezione del trasferimento delle informazioni attraverso l'uso di tutte le tipologie di strutture di comunicazione.

È necessario:

- protezione dei messaggi dall'accesso non autorizzato, dalla modifica o dal denial of service in modo commisurato allo schema di classificazione adottato
- assicurare un corretto indirizzamento e trasporto del messaggio;
- affidabilità e disponibilità del servizio;
- ottenimento di un'approvazione preventiva per l'uso di servizi pubblici esterni quali la messaggistica istantanea, i social network o la condivisione di file;
- livelli di autenticazione più elevati per il controllo degli accessi da reti pubblicamente accessibili.

☐ **Crittografia.** Devono essere utilizzati strumenti di cifratura per la trasmissione dei dati.

Requisiti minimi per la sicurezza fisica dei luoghi in cui vengono trattati i dati personali.

☐ **Sospensione mediante screen saver dopo un periodo di inattività.** E' necessario abilitare la sospensione dei sistemi mediante screensaver dopo un certo periodo di inattività di un computer, richiedendo nuovamente la password per l'accesso. Questo non vale solo per i computer in aree pubbliche, ma a tutti i computer.

Requisiti minimi per l'uso del telelavoro e del lavoro a distanza.

☐ **Accesso da remoto.** Qualora venga autorizzato un membro del personale/fornitore ad accedere alla rete da una postazione remota, tale accesso crea un potenziale debolezza del sistema. Per questo motivo questa tipologia di accessi dovrebbe essere adeguatamente valutata e concordata con il Titolare del trattamento. L'accesso deve essere limitato a specifici indirizzi IP.

Requisiti minimi di memorizzazione e conservazione.

☐ **Dispositivi portatili.** Devono essere previste misure di sicurezza per gli asset all'esterno delle sedi, considerando i diversi rischi derivanti dall'operare all'esterno dei locali dell'organizzazione stessa.

È necessario creare meccanismi per essere in grado di cancellare da remoto i dati personali su un dispositivo mobile compromesso. I dispositivi mobili devono essere fisicamente protetti contro il furto quando non sono in uso.

☐ **Backup**. Devono essere effettuate copie di backup delle informazioni, del software e delle immagini dei sistemi e quindi sottoposte a test periodici secondo una politica di backup concordata. Le copie di backup devono essere crittografate e archiviate in modo sicuro offline. Periodicamente il responsabile dovrà fornire al Titolare del trattamento le copie di backup dei dati e delle informazioni di cui è titolare.

☐ **Dismissione dei supporti.** La dismissione dei supporti non più necessari deve avvenire in modo sicuro, attraverso l'utilizzo di procedure formali.

☐ **Sistemi di geolocalizzazione.** Tempi di conservazione: con riferimento ai tempi di conservazione, il Garante ha ritenuto congruo un tempo di conservazione dei dati commisurato in 30 giorni, specificando che ciò avvenga allo scopo di rendicontazione delle spese del servizio, salva la conservazione in presenza di eventuali obblighi di legge gravanti sul titolare del trattamento (art. 5, comma 1. lett. e), del Regolamento).

C.2Periodo di conservazione / procedure di cancellazione

I dati personali devono essere cancellati dal Responsabile del trattamento alla scadenza del presente contratto.

C.3 Luogo di elaborazione

Il trattamento dei dati personali, ai sensi del presente Accordo, non può essere eseguito in luoghi diversi dai seguenti senza il previo consenso scritto del Titolare. l'elaborazione avviene presso la sede amministrativa della cooperativa

C.4Istruzioni e/o approvazione del trasferimento di dati personali verso paesi terzi

Il responsabile del trattamento non ha diritto di trasferire i dati verso paesi terzi.

C.5 Procedure per l'ispezione da parte del Titolare del trattamento

Il Titolare del trattamento, inoltre, previa richiesta formulata con congruo preavviso e comunque non prima di 5 giorni lavorativi, si riserva il diritto di eseguire controlli, attraverso ispezioni o attività di audit, sull'effettivo svolgimento delle attività e dei compiti affidati, purché quest'ultimi avvengano in forme compatibili con il normale svolgimento delle attività del Responsabile; il titolare previa richiesta formulata con congruo preavviso e comunque non prima di 5 giorni lavorativi, verificherà periodicamente la sussistenza dei caratteri di esperienza, capacità ed affidabilità in capo al responsabile e il rispetto da parte dello stesso di tutte le disposizioni normative in materia di sicurezza dei dati. A tal fine il Titolare del trattamento potrà richiedere allo stesso di essere relazionato per iscritto attraverso regolari report

Appendice D. Disposizioni che non sono coperte dalle clausole contrattuali.