

Allegato

ACCORDO SUL TRATTAMENTO DEI DATI PERSONALI

tra

il **CLIENTE**, ossia il soggetto che, ai sensi dei Termini e Condizioni dei Servizi (le “**Condizioni**”), usufruisce dell/i servizio/i fornito/i, in persona del suo legale rappresentante *pro tempore* (il “**Cliente**” o il “**Titolare del Trattamento**”)

e

OMSIC S.R.L., C.F./P.IVA 10058120154 con sede in Cinisello Balsamo (MI), via F.lli Gracchi n. 27, in persona del legale rappresentante *pro tempore* (il “**Responsabile del Trattamento**”),

anche definite singolarmente “**Parte**” e, congiuntamente, “**Parti**”

PREMESSE

- a) Il Cliente ha sottoscritto in data odierna le Condizioni in forza delle quali ha assunto il diritto di utilizzare il/i Servizio/i come indicati nelle condizioni speciali di servizio/assistenza e/o nel relativo modulo d’ordine (il “**Servizio**” o i “**Servizi**”);
- b) l’esecuzione del/i Servizio/i comporta inevitabilmente il trattamento, da parte del Fornitore per conto del Cliente, di dati personali di cui il Cliente, ai sensi della Normativa privacy, è Titolare, meglio dettagliati nell’Allegato 1) del presente DPA (i “**Dati Personali**”);
- c) con il presente accordo, ritenuto che OMSIC presenti garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento (UE) 679/2016 (il “**Regolamento**” o il “**GDPR**”) e della normativa *privacy* e garantisca la tutela dei diritti dell’interessato nonché in considerazione della sua esperienza, capacità ed affidabilità, il Titolare, come sopra individuato e legalmente rappresentato dal sottoscrittore in calce, ai sensi dell’art. 28 GDPR intende nominare OMSIC quale Responsabile Esterno del Trattamento dei Dati Personali a cui ha accesso nello svolgimento del/i Servizio/i e disciplinare gli specifici obblighi a suo carico (“**Nomina**” o “**DPA**”);
- d) per i trattamenti concernenti dati personali che esulano dall’ambito del presente DPA, le Parti si danno atto e convengono che ciascuna di esse agisce in qualità di autonomo Titolare e sotto la propria distinta responsabilità e terrà l’altra Parte completamente manlevata e indenne da qualsiasi costo, spesa, responsabilità, esborso - ivi incluso per spese legali o sanzioni -, pretesa di terzi e qualsivoglia altro onere che debba sostenere a causa della violazione da parte dell’altra Parte degli obblighi su di essa gravanti in qualità di autonomo Titolare del trattamento.

Tutto ciò premesso, le Parti convengono quanto segue

1. Premesse

- 1.1 Le premesse e l’Allegato 1) costituiscono parte integrante e sostanziale del presente DPA.

2. Obblighi e Responsabilità del Titolare del Trattamento

- 2.1 Fatti salvi gli altri obblighi previsti dalle disposizioni di legge e regolamentari applicabili, il Titolare del Trattamento dichiara e garantisce:

- 2.1.1 di aver raccolto e di trattare i Dati Personali nel pieno rispetto della normativa nazionale e sovranazionale applicabile;

- 2.1.2 di aver fornito agli interessati adeguata informativa relativa al trattamento dei Dati Personali, anche in relazione alle finalità di cui al presente DPA, e di aver raccolto, ove necessario, il relativo consenso;
 - 2.1.3 che detterà al Responsabile del Trattamento istruzioni aderenti alle informazioni rese agli interessati, che potranno essere integrate e/o modificate in coerenza alle evoluzioni normative e tecniche in materia;
 - 2.1.4 che tutte le attività di trattamento dei Dati Personali rilevanti ai sensi del presente DPA sono svolte sulla base di almeno una delle condizioni di cui all'articolo 6 del Regolamento (UE) 679/2016 (il "**Regolamento**") e
 - 2.1.5 di conservare la titolarità dei Dati Personali.
- 2.2 Il Titolare si obbliga a fornire tutta la collaborazione e l'assistenza necessaria affinché il Responsabile del trattamento possa svolgere i compiti di "Responsabile".

3. Obblighi del Responsabile del Trattamento

- 3.1 Fatti salvi gli altri obblighi previsti dalle disposizioni di legge e regolamentari applicabili, il Responsabile del Trattamento dichiara e garantisce che:
- 3.1.1 tratterà - anche per mezzo di propri incaricati del trattamento e/o amministratori di sistema e/o Sub-Responsabili - i Dati Personali esclusivamente per conto del Titolare per le sole finalità connesse all'esecuzione del/i Servizio/i e all'utilizzo, Manutenzione Ordinaria e/o Manutenzione Straordinaria e server dedicati e/o richieste dalla normativa applicabile, nel rispetto della normativa vigente e secondo le istruzioni contenute nel presente DPA o comunque impartite per iscritto dal Titolare del Trattamento;
 - 3.1.2 curerà la conservazione dei Dati Personali in conformità a quanto previsto dall'art. 5 GDPR e, in generale, nel rispetto dei tempi e delle modalità previsti dal Contratto, adottati dal Titolare in relazione alle finalità di trattamento per cui sono stati raccolti ed imposti dalla Normativa Privacy vigente;
 - 3.1.3 ove una o più istruzioni dettate dal Titolare del Trattamento si pongano in contrasto con la normativa nazionale e/o sovranazionale vigente, comunicherà immediatamente per iscritto al Titolare del Trattamento tale contrasto indicandone le relative motivazioni;
 - 3.1.4 salva l'eventuale designazione di sub-responsabili a norma del presente DPA, non comunicherà a terzi o diffonderà in tutto od in parte i Dati senza la preventiva autorizzazione scritta del Titolare del Trattamento, a meno che la comunicazione degli stessi non sia necessaria per eseguire il/i Servizio/i e/o per garantire la corretta operatività, impegnandosi a comunicare la minor quantità possibile di dati personali necessaria per conformarsi alla legge. Tale obbligo continuerà a sussistere anche al termine del rapporto contrattuale in essere tra le Parti, per qualsiasi ragione intervenuto;
 - 3.1.5 assicurerà che nessuno dei Dati Personali venga trasferito o divulgato verso Paesi Terzi (extra SEE) o organizzazioni internazionali senza la preventiva autorizzazione scritta del Titolare, salvo che tale trasferimento sia necessario per l'esecuzione del/i Servizio/i e/o per garantire la corretta operatività o sia previsto da specifica disposizione di legge e, in tal caso, che lo stesso avverrà con applicazione di almeno uno dei meccanismi di salvaguardia previsti dagli articoli 44 e seguenti del Regolamento;
 - 3.1.6 provvederà ad individuare per iscritto al proprio interno le persone autorizzate al trattamento dei Dati Personali e/o gli amministratori di sistema impartendo agli stessi le istruzioni riguardo il rispetto delle misure di sicurezza adottate e consentendo l'accesso dei medesimi ai soli Dati

Personali la cui conoscenza sia strettamente necessaria per adempiere alle mansioni loro assegnate inerenti al/i Servizio/i, nonché a vigilare su tali aspetti;

- 3.1.7 provvederà alla formazione delle persone autorizzate e garantisce che le stesse si impegnino alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- 3.1.8 si impegnerà periodicamente a verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione degli incaricati e/o responsabili del trattamento e/o amministratori di sistema nominati;
- 3.1.9 si impegnerà a collaborare con il Titolare del Trattamento nel rispondere alle richieste del Garante per la Protezione dei Dati Personali e di ogni altra autorità competente in materia in caso di effettuazione di controlli ed accertamenti, prestando piena e sollecita cooperazione al fine di rispondere tempestivamente ed in modo esauriente a eventuali richieste di informazioni e documenti;
- 3.1.10 notificherà al Titolare del Trattamento qualsiasi violazione delle misure di sicurezza adottate per la protezione dei dati e delle informazioni che comporti anche accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali e alle informazioni trasmesse, memorizzate o comunque trattate.
- 3.1.11 In particolare, il Responsabile si impegna a:
 - 3.1.11.1 informare tempestivamente il Titolare, in ogni caso entro e non oltre 24 ore dalla scoperta dell'evento, di ogni violazione dei dati personali trattati presso le proprie sedi o per mezzo di propri Sub-Responsabili per conto del Titolare che presenti un rischio per i diritti e le libertà delle persone fisiche;
 - 3.1.11.2 fornire al Titolare tutti i dettagli completi della violazione subita: in particolare, la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione, le probabili conseguenze della violazione dei dati personali, le misure adottate o di cui si propone l'adozione da parte del Titolare per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi;
 - 3.1.11.3 fornire assistenza e supportare il Titolare per far fronte alla violazione e alle sue conseguenze, al fine di mitigare gli effetti delle violazioni e valutare le misure correttive più idonee;
 - 3.1.11.4 collaborare con il Titolare, limitatamente ai trattamenti compiuti in qualità di Responsabile ai sensi della presente nomina, nell'assolvimento degli obblighi di notifica delle violazioni di dati all'Autorità Garante per la protezione dei dati personali ad altre autorità di controllo competenti e, laddove richiesto in ragione dell'elevato livello di rischio per i diritti e le libertà degli interessati, anche a questi ultimi nonché, in tutti i casi in cui ciò sia necessario, di idonea valutazione di impatto sulla protezione dei dati (privacy impact assessment), oltre che nello svolgimento di eventuali procedure di consultazione preventiva con il Garante o le altre autorità competenti;
- 3.1.12 assicurerà misure tecniche ed organizzative che, anche in considerazione della natura dei trattamenti svolti per conto e nell'interesse del Titolare, consentano al Fornitore di assistere il Cliente nell'adempimento del proprio obbligo di fornire adeguato riscontro alle richieste di esercizio dei diritti avanzate da parte degli interessati, con particolare riferimento alle istanze di portabilità, di limitazione del trattamento e di cancellazione ("oblio") dei dati;
- 3.1.13 fermo l'obbligo di collaborazione di cui sopra, metterà il Cliente al corrente di qualsiasi richiesta di esercizio di diritti inviata da parte degli interessati, entro un termine massimo di 5 giorni dal ricevimento della stessa.

4. Adozione di misure di sicurezza

- 4.1 Il Responsabile si impegna ad implementare misure e processi che garantiscano l'attuazione dei principi di privacy-by-design e privacy-by-default e, più in generale, la minimizzazione e la sicurezza dei trattamenti nonché ad adottare le misure necessarie a prevenire, o quantomeno minimizzare, ogni rischio ragionevolmente prevedibile connesso alla distruzione, alla perdita, alla modifica, alla divulgazione non autorizzata o all'accesso, in modo accidentale o illegale, ai Dati;
- 4.2 In particolare, egli, tenendo conto anche delle best practices di settore, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità delle operazioni trattamento connesse all'adempimento del Contratto, oltre che dei rischi che tali trattamenti possono determinare per i diritti e le libertà degli interessati, misure tecniche e organizzative adeguate a garantire un idoneo livello di sicurezza dei Dati, si obbliga ad individuare, adottare ed impartire le misure di sicurezza adeguate previste dagli artt. 32-35 GDPR e dalla normativa privacy applicabile per ridurre al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità del trattamento stesso dei Dati Personali, e a titolo indicativo e non esaustivo:
- 4.2.1 adottare un sistema di autenticazione informatica, permettendo l'accesso solo agli incaricati e/o ai responsabili interni e/o ai sub-responsabili esterni del trattamento e/o agli amministratori di sistema all'uopo muniti di credenziali di autenticazione;
- 4.2.2 adottare procedure di gestione delle credenziali di autenticazione, nonché di disattivazione/cancellazione delle stesse se non utilizzate o in caso di perdita della qualità che consente l'accesso ai Dati Personali;
- 4.2.3 impartire istruzioni per regolare le modalità per assicurare la disponibilità dei Dati Personali in caso di prolungata assenza o impedimento di un incaricato che renda indispensabile e indifferibile intervenire per necessità di operatività e sicurezza;
- 4.2.4 utilizzare un sistema di autorizzazione per gli incaricati, i responsabili interni e gli amministratori di sistema e aggiornare periodicamente l'ambito del trattamento consentito a detti soggetti;
- 4.2.5 redigere e aggiornare la lista degli incaricati, dei responsabili interni e degli amministratori di sistema;
- 4.2.6 proteggere gli strumenti elettronici e i Dati Personali rispetto a trattamenti illeciti e ad accessi non consentiti, adottando antivirus e software volti a prevenire la vulnerabilità di strumenti elettronici, da aggiornare con cadenza almeno semestrale;
- 4.2.7 adottare procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei Dati Personali e dei sistemi, che prevedano il salvataggio dei Dati Personali con frequenza almeno settimanale;
- 4.2.8 dare istruzione ai propri incaricati, responsabili interni, sub-responsabili esterni e amministratori di sistema di mantenere come confidenziale ogni Dati Personale portato a loro conoscenza nel corso del Servizio, allo stesso modo dei relativi trattamenti, evitando che le credenziali restino incustodite o il terminale accessibile durante una sessione di trattamenti;
- 4.2.9 adottare le misure volte ad assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi, nonché la disponibilità e l'accesso dei Dati Personali in caso di incidente fisico o tecnico;
- 4.2.10 adottare misure e procedure per testare, verificare e valutare l'efficacia delle misure adottate;
- 4.2.11 impostare i propri sistemi secondo i principi di *privacy by design e by default*;
- 4.2.12 formare adeguatamente dipendenti e collaboratori;

- 4.2.13 redigere e implementare appropriate policy, processi e strumenti per assicurare e incrementare la *compliance* con il GDPR;
- 4.2.14 istituire e mantenere il registro delle attività di trattamento ai sensi dell'art. 30 del GDPR e metterlo a disposizione del Titolare ogniqualvolta richiesto;
- 4.2.15 comunicare al Titolare, previa espressa richiesta scritta, i recapiti di contatto del proprio Responsabile della Protezione dei Dati, ove designato ai sensi degli artt. 37 e ss. del GDPR;
- 4.2.16 assistere il Titolare relativamente ai Dati Personali oggetto di trattamento, nel garantire – ove applicabili - il rispetto degli obblighi relativi alla sicurezza del trattamento, alla valutazione d'impatto sulla protezione dei Dati Personali ai sensi dell'art. 35 del GDPR, alla consultazione preventiva ai sensi dell'art. 36 del GDPR.

4.3 Il Titolare riconosce sin d'ora l'efficacia e l'adeguatezza delle misure di sicurezza qui indicate.

5. Designazione di Sub-responsabili

5.1 Il Titolare del Trattamento fornisce la propria autorizzazione generale a che il Responsabile del Trattamento, ai sensi dell'articolo 28, paragrafo 2, del Regolamento, possa ricorrere ad uno o più Sub-responsabili del trattamento, al fine di poter adempiere agli obblighi discendenti dalle Condizioni e dal presente DPA.

5.2 Il Responsabile del Trattamento nell'instaurare il proprio rapporto contrattuale con i Sub-responsabili dovrà attenersi alle seguenti condizioni:

5.2.1 il Responsabile del Trattamento è tenuto a scegliere diligentemente il Sub-responsabile prestando particolare attenzione alla reputazione e all'esperienza nonché all'adeguatezza delle misure tecniche e organizzative adottate dallo stesso. Il Responsabile del Trattamento è tenuto a stipulare un accordo scritto con qualsiasi eventuale Sub-responsabile il quale deve: (i) prevedere nei confronti del Sub-responsabile gli stessi obblighi previsti dal DPA in capo al Responsabile del Trattamento, nonché provvedere alla comunicazione nei confronti del Sub-Responsabile di qualsivoglia ulteriore e specifica istruzione sul trattamento che dovesse provenire dal Titolare, anche successivamente alla sottoscrizione della presente Nomina (ii) descrivere i trattamenti oggetto dell'eventuale accordo e (iii) dettagliare le misure tecniche e organizzative che il Sub-responsabile è tenuto ad implementare ai sensi del presente DPA e della normativa applicabile;

5.2.2 qualora gli eventuali sub-responsabili esterni del trattamento siano situati in un paese extra-UE, il Responsabile si impegna ad assicurare un livello di protezione dei Dati Personali equivalente all'Unione Europea, stipulando con i sub-responsabili esterni le *Standard Contractual Clauses* (SCC) adottate dalla Commissione Europea.

6. Potere di controllo del Titolare

6.1 Il Titolare potrà vigilare periodicamente sulla puntuale osservanza delle istruzioni impartite al Responsabile e verificare il perdurare dei requisiti di esperienza, capacità ed affidabilità che hanno influito sulla designazione del Responsabile.

6.2 Il Responsabile consente al Titolare - o a soggetto da questi incaricato, vincolato da obblighi di riservatezza - di eseguire verifiche e ispezioni al fine di accertare l'adempimento di detti obblighi e contribuisce alle relative attività. Il Titolare, ove intenda procedere a tale attività di verifica, dovrà comunicarlo per iscritto al Responsabile, con almeno 15 giorni lavorativi di preavviso. Rimane salva la possibilità per le parti di concordare che tali verifiche vengano condotte al di fuori dell'orario lavorativo. Il Responsabile si impegna a offrire ogni supporto necessario a tali attività di verifica, rispondendo alle richieste di informazioni e chiarimenti e fornendo la documentazione eventualmente richiesta. In nessun caso, tuttavia, il Responsabile darà accesso ai propri sistemi informativi al Titolare in modalità autenticata o permetterà accessi alle reti private dei propri sistemi informativi.

7. Inadempimento

- 7.1 Il Responsabile si obbliga a manlevare e a tenere indenne il Titolare da qualsiasi danno, pregiudizio, costo, spesa (incluse le spese legali), sanzione o qualsivoglia altro onere derivanti da pretese o azioni giudiziarie, arbitrali o amministrative da parte di qualsiasi terzo, nonché da condotta illecita o non diligente dei propri incaricati del trattamento e/o amministratori di sistema e/o Sub-Responsabili per effetto di violazioni della presente Nomina e, in generale, del GDPR e/o della Normativa *Privacy* per tempo applicabile, nei limiti di quanto previsto dalle Condizioni.
- 7.2 Il Titolare si obbliga a manlevare e a tenere indenne il Responsabile da qualsiasi danno materiale o immateriale, pregiudizio, costo, spesa (incluse le spese legali), sanzione o qualsivoglia altro onere derivanti da pretese o azioni giudiziarie, arbitrali o amministrative da parte da parte di qualsiasi terzo, per effetto dell'inadempimento, condotta illecita e/o non diligente da parte del medesimo Titolare e dei suoi incaricati del trattamento e/o referenti interni del trattamento e/o amministratori di sistema e/o responsabili esterni del trattamento (ulteriori rispetto al Responsabile) per violazione degli obblighi di cui al GDPR e/o alla Normativa *Privacy* per tempo applicabile in materia di protezione dei dati specificatamente diretti ai titolari del trattamento o della presente Nomina ovvero che derivi dall'attuazione da parte del Responsabile delle istruzioni date dal Titolare per il trattamento dei Dati Personali in relazione alla fornitura dei Servizi.

8. Durata e cessazione del trattamento

- 8.1 Il presente DPA è causalmente collegato alle Condizioni, pertanto esso avrà validità dalla data della loro sottoscrizione fino al termine di durata delle Condizioni e cesserà automaticamente alla cessazione di queste ultime per qualsiasi causa o sino alla cessazione del/i Servizio/i e/o delle operazioni di trattamento dei Dati Personali di cui sopra.
- 8.2 I Dati dovranno essere conservati dal Responsabile del Trattamento per il tempo strettamente necessario all'esecuzione delle Condizioni, delle previsioni del DPA e nel rispetto dei termini obbligatori previsti dalla legge, dal Regolamento e/o da provvedimenti del Garante per la protezione di dati personali e, in ogni caso, nel rispetto dei termini comunicati dal Titolare del Trattamento.
- 8.3 In caso di cessazione, per qualsiasi causa, del presente DPA il Responsabile del Trattamento si impegna sin d'ora:
- 8.3.1 a cessare o far cessare le operazioni di trattamento affidate e
 - 8.3.2 su istruzione del Titolare del Trattamento, a restituire al Titolare del Trattamento i Dati Personali oggetto delle operazioni di trattamento, oppure provvedere alla loro integrale distruzione, entro il termine di 90 giorni dalla data della richiesta.

9. Incarico di Amministratore di sistema

- 9.1 Ove applicabile, il Fornitore si impegna a conformarsi al Provvedimento generale del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", così come modificato dal Provvedimento del Garante del 25 giugno 2009 "Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento", così come eventualmente modificato o sostituito dallo stesso Garante, e ad ogni altro pertinente provvedimento dell'Autorità.
- 9.2 Il Fornitore si impegna, in particolare, a:

- 9.2.1 designare quali amministratori di sistema le figure professionali dedicate alla gestione e alla manutenzione di impianti di elaborazione o di loro componenti con cui vengono effettuati trattamenti di dati personali;

- 9.2.2 predisporre e conservare l'elenco contenente gli estremi identificativi delle persone fisiche qualificate quali amministratori di sistema e le funzioni ad essi attribuite;
- 9.2.3 comunicare ove richiesto dal Titolare l'elenco aggiornato degli amministratori dei sistemi;
- 9.2.4 verificare annualmente l'operato degli amministratori di sistema;
- 9.2.5 mantenere i file di log previsti in conformità a quanto previsto nel suddetto provvedimento.

10. Varie

- 10.1 Il presente DPA non prevede alcun compenso aggiuntivo a favore del Responsabile rispetto a quello già pattuito nelle Condizioni.
- 10.2 Per quanto non espressamente ivi previsto, si rinvia alle Condizioni ed alle disposizioni generali vigenti in materia di protezione di dati personali.
- 10.3 Il presente accordo è regolato dalla legge italiana e ogni controversia relativa alla sua validità, efficacia e interpretazione è devoluta alla competenza esclusiva del Foro di Milano.

ALLEGATO 1) all'ACCORDO SUL TRATTAMENTO DEI DATI PERSONALI

TIPOLOGIA DI DATI TRATTATI

In esecuzione delle Condizioni e del DPA il Responsabile del trattamento tratterà le seguenti tipologie di Dati Personali:

X nome e cognome autisti;

X numero e riferimenti patente di guida autisti;

X nome e cognome, indirizzo, codice fiscale dei soggetti fiscali;

CATEGORIE DI INTERESSATI

I Dati trattati dal Responsabile del Trattamento in esecuzione delle Condizioni e del DPA sono relativi alle seguenti categorie di interessati:

X autisti del Cliente;

X dipendenti/collaboratori del Cliente;

X soggetti fiscali quali depositi /raffinerie, proprietari e destinatari di merce;

OPERAZIONI DI TRATTAMENTO

X conservazione,

X estrazione,

X consultazione,

X comunicazione mediante trasmissione,

X cancellazione,

X distruzione,
