DPA (Data Processing Agreement) - Accordo sul trattamento dei dati personali ai sensi dell'art. 28 del Regolamento (UE) 2016/679 ("GDPR")

Ultimo aggiornamento: 01/04/2026 - versione 1.0

Versione pubblicata online e accettata per via elettronica

Il presente Accordo sul trattamento dei dati personali ("**DPA**") costituisce parte integrante e sostanziale dei **Termini e Condizioni** e/o dell'**Ordine di acquisto** relativi al servizio software SaaS **SmartGarage.biz**.

Il presente DPA si intende concluso e vincolante tra:

Maxisoft® s.r.l., con sede in Via Dorsale, 13 – 54100 Massa (MS) – Italia, Partita IVA / Codice Fiscale / Registro Imprese Massa Carrara n. IT00667410450, REA MS 100489, in persona del legale rappresentante pro tempore, di seguito "**Maxisoft®**" o "**Responsabile del trattamento**";

e

il soggetto, persona fisica o giuridica, che acquista, sottoscrive o utilizza il servizio SmartGarage.biz quale cliente, come identificato nell'Ordine, nel checkout, nell'account cliente o nei dati di fatturazione, di seguito "**Cliente**" o "**Titolare del trattamento**",

congiuntamente, le "**Parti**".

L'accettazione del presente DPA avviene mediante separata accettazione elettronica nel flusso di acquisto, nell'attivazione dell'account o nel rinnovo del servizio, oppure mediante sua espressa incorporazione nell'Ordine, nel checkout o nel Contratto principale, in conformità all'art. 28, par. 9 GDPR. Il mero utilizzo della piattaforma, in assenza di tale forma scritta o elettronica, non costituisce di per sé autonoma modalità di conclusione del presente DPA.

1. Premesse e rapporto con il Contratto principale

1.1 Le premesse costituiscono parte integrante del presente DPA.

1.2 Il presente DPA disciplina i trattamenti di dati personali effettuati da Maxisoft® **per conto del Cliente** nell'ambito dell'erogazione del servizio SaaS SmartGarage.biz, ai sensi dell'art. 28 GDPR.

1.3 Il presente DPA integra i Termini e Condizioni del servizio, l'Ordine di acquisto e ogni altro accordo contrattuale avente ad oggetto SmartGarage.biz (congiuntamente, il "**Contratto principale**").

1.4 In caso di contrasto tra il presente DPA e il Contratto principale in materia di protezione dei dati personali, prevale il presente DPA.

1.5 Il presente DPA non disciplina i trattamenti di dati personali effettuati da Maxisoft® in qualità di autonomo Titolare per finalità proprie, quali, a titolo esemplificativo: la gestione del rapporto commerciale e contrattuale con il Cliente, la fatturazione, gli adempimenti amministrativi, fiscali e contabili, la gestione dell'account contrattuale, i dati di pagamento, le comunicazioni di servizio rivolte al Cliente e i trattamenti strettamente necessari alla sicurezza della piattaforma, alla prevenzione di abusi e alla tutela dei diritti di Maxisoft®. Tali trattamenti sono disciplinati dalla specifica informativa "Privacy Area Clienti e Piattaforma SmartGarage.biz".

2. Definizioni

Ai fini del presente DPA:

a) "**GDPR**" indica il Regolamento (UE) 2016/679;
b) "**Codice Privacy**" indica il D.Lgs. 196/2003 come armonizzato dal D.Lgs. 101/2018 e successive modifiche e integrazioni.
c) "**Dati personali del Cliente**" indica i dati personali trattati da Maxisoft® per conto del Cliente nell'ambito dell'erogazione del servizio SmartGarage.biz;
d) "**Interessato**" indica la persona fisica cui si riferiscono i dati personali;
e) "**Violazione dei dati personali**" indica una violazione di sicurezza che comporta accidentalmente o in modo illecito distruzione, perdita, modifica, divulgazione non autorizzata o accesso ai dati personali;
f) "**Sub-responsabile**" indica il soggetto terzo nominato da Maxisoft® per svolgere specifiche attività di trattamento per conto del Cliente;
g) "**Servizio**" indica la piattaforma software SaaS SmartGarage.biz e i relativi servizi accessori, funzionali o connessi.

Per quanto non espressamente definito nel presente DPA, valgono le definizioni contenute nel GDPR.

3. Oggetto della nomina

3.1 Con il presente DPA, il Cliente nomina Maxisoft® quale **Responsabile del trattamento** ai sensi dell'art. 28 GDPR, limitatamente ai trattamenti di dati personali che Maxisoft® effettua **per conto del Cliente** e sulla base delle sue istruzioni documentate, al fine di consentire l'erogazione del Servizio.

3.2 Maxisoft® accetta tale nomina e si impegna a trattare i Dati personali del Cliente nel rispetto del presente DPA, del GDPR e della normativa applicabile.

3.3 Le caratteristiche essenziali del trattamento affidato sono descritte nell'**Allegato 1** al presente DPA.

4. Durata

4.1 Il presente DPA entra in vigore alla data di accettazione elettronica da parte del Cliente e resta efficace per tutta la durata del Contratto principale.

4.2 Alla cessazione, per qualsiasi causa, del Contratto principale, il presente DPA resterà efficace per il tempo strettamente necessario all'esecuzione delle attività di restituzione, esportazione, cancellazione, conservazione tecnica residuale, backup, disattivazione e/o adempimento di obblighi di legge.

5. Natura e finalità del trattamento

5.1 Maxisoft® tratta i Dati personali del Cliente esclusivamente per consentire al Cliente di utilizzare il Servizio, comprese, a titolo esemplificativo:

a) hosting applicativo e messa a disposizione della piattaforma;
b) memorizzazione, organizzazione, consultazione ed elaborazione dei dati immessi dal Cliente;
c) gestione tecnica delle utenze, dei profili, dei permessi e delle configurazioni;
d) backup, ripristino, business continuity e misure di resilienza tecnica;
e) assistenza tecnica, manutenzione correttiva, manutenzione evolutiva e supporto operativo;
f) sicurezza logica, monitoraggio tecnico, prevenzione di incidenti e protezione dell'infrastruttura;

g) ogni ulteriore attività strettamente necessaria all'esecuzione del Contratto principale e conforme alle istruzioni documentate del Cliente.

5.2 Maxisoft® non utilizza i Dati personali del Cliente per finalità proprie incompatibili con il ruolo di Responsabile del trattamento.

5.3 Qualora Maxisoft® utilizzi, nell'ambito dell'erogazione del Servizio o del supporto tecnico, sistemi di Intelligenza Artificiale o automazione assistita, tali sistemi saranno impiegati esclusivamente nei limiti delle istruzioni documentate del Cliente, delle funzionalità del Servizio e della normativa applicabile. Salvo diversa specifica informativa o diversa configurazione richiesta dal Cliente, tali strumenti non sono utilizzati da Maxisoft® per assumere decisioni unicamente automatizzate che producano effetti giuridici o analogamente significativi sugli interessati ai sensi dell'art. 22 GDPR. Maxisoft® garantisce che i sistemi AI siano chiaramente identificabili come artificiali ai sensi dell'art. 50 del Regolamento (UE) 2024/1689 (AI Act) e mantiene supervisione umana sui processi critici. Il Cliente ha in ogni momento il diritto di richiedere l'escalation a un operatore umano.

5.4 Trattamento dati per funzionalità di comunicazione elettronica

5.4.1 Qualora il Servizio SmartGarage.biz includa funzionalità di invio comunicazioni elettroniche verso destinatari individuati dal Cliente (es. SMS per appuntamenti, email per preventivi, notifiche push per promozioni), Maxisoft® tratta i relativi dati personali (numeri di telefono, indirizzi email, contenuti dei messaggi) esclusivamente quale Responsabile del trattamento per conto del Cliente e nei limiti delle istruzioni documentate da quest'ultimo.

5.4.2 Responsabilità del Cliente (Titolare)

Il Cliente, quale Titolare del trattamento, è l'unico responsabile:

- della liceità delle comunicazioni inviate tramite il Servizio;
- della corretta individuazione della base giuridica applicabile (consenso, contratto, legittimo interesse);
- dell'adempimento degli obblighi informativi verso i destinatari ai sensi dell'art. 13 GDPR;
- del rispetto della disciplina in materia di comunicazioni elettroniche indesiderate (art. 130 D.Lgs. 196/2003, GDPR art. 21, Registro Pubblico delle Opposizioni);
- della verifica che i destinatari non siano iscritti al Registro Pubblico delle Opposizioni (RPO) istituito dal D.P.R. 178/2010, ove applicabile;
- della gestione delle richieste di opposizione (opt-out) da parte dei destinatari.

5.4.3 Ruolo di Maxisoft® (Responsabile)

Maxisoft® si limita a:

- fornire l'infrastruttura tecnica per l'invio delle comunicazioni;
- eseguire materialmente l'invio su istruzione del Cliente;
- utilizzare sub-responsabili tecnici per l'erogazione del servizio (es. provider SMS gateway, email delivery service) come indicato nell'Allegato 3.

Maxisoft® non esegue alcun controllo preventivo sulla liceità delle liste di contatti, sulla validità dei consensi o sulla conformità dei contenuti alla normativa applicabile. Tali verifiche sono esclusiva responsabilità del Cliente.

5.4.4 Limitazioni d'uso

Il Cliente si impegna a non utilizzare le funzionalità di comunicazione del Servizio per:

- invii massivi non autorizzati (spam);
- comunicazioni verso soggetti iscritti al RPO senza valida eccezione di legge;
- contenuti illeciti, diffamatori, ingannevoli o contrari all'ordine pubblico;
- pratiche commerciali aggressive o ingannevoli ai sensi del Codice del Consumo.

5.4.5 Manleva

Il Cliente si impegna a manlevare e tenere indenne Maxisoft® da qualsiasi contestazione, sanzione, danno o pretesa derivante da invii non autorizzati, violazioni del GDPR, del D.Lgs. 196/2003, del D.P.R. 178/2010 (RPO) o di altra normativa applicabile alle comunicazioni elettroniche, incluse eventuali spese legali sostenute da Maxisoft® per la difesa.

6. Istruzioni documentate del Cliente

6.1 Maxisoft® tratta i Dati personali del Cliente esclusivamente su istruzione documentata del Cliente, salvo che il trattamento sia richiesto dal diritto dell'Unione o dello Stato membro cui Maxisoft® è soggetta; in tal caso Maxisoft® informerà il Cliente di tale obbligo giuridico prima del trattamento, salvo che la legge vieti tale informazione per rilevanti motivi di interesse pubblico.

6.2 Il presente DPA, il Contratto principale, le configurazioni del Servizio selezionate dal Cliente, le richieste di assistenza, i ticket, le autorizzazioni impartite tramite console amministrativa, nonché le ulteriori indicazioni scritte o elettroniche trasmesse dal Cliente, costituiscono istruzioni documentate ai fini del presente articolo.

6.3 Qualora Maxisoft® ritenga che un'istruzione del Cliente violi il GDPR o altra normativa applicabile in materia di protezione dei dati personali, ne informerà senza ingiustificato ritardo il Cliente.

6.4 Il Cliente è responsabile della liceità delle istruzioni impartite, della correttezza dei presupposti di trattamento e dell'esistenza di una valida base giuridica per i trattamenti effettuati tramite il Servizio.

7. Obblighi del Cliente quale Titolare del trattamento

7.1 Il Cliente dichiara e garantisce di essere il Titolare del trattamento, oppure di essere legittimato a impartire istruzioni a Maxisoft®, con riferimento ai Dati personali del Cliente trattati mediante il Servizio.

7.2 Il Cliente si impegna a:

a) trattare i dati personali nel rispetto del GDPR e della normativa applicabile;
b) fornire agli interessati le informative richieste;
c) raccogliere, ove necessario, validi consensi o fondare il trattamento su altra idonea base giuridica;
d) determinare le finalità e i mezzi essenziali del trattamento svolto tramite il Servizio;
e) verificare che le categorie di dati trattati mediante il Servizio siano adeguate, pertinenti e non eccedenti;
f) non utilizzare il Servizio per trattamenti illeciti o vietati;
g) configurare correttamente ruoli, permessi, utenti autorizzati e politiche interne di accesso.

7.3 Il Cliente resta l'unico responsabile, nei confronti degli interessati e delle autorità competenti, del contenuto dei dati immessi nella piattaforma, delle finalità perseguite, della correttezza delle istruzioni impartite e della legittimità complessiva del trattamento.

8. Riservatezza e persone autorizzate

8.1 Maxisoft® garantisce che le persone autorizzate a trattare i Dati personali del Cliente si siano impegnate alla riservatezza o siano soggette a un adeguato obbligo legale di riservatezza.

8.2 Maxisoft® assicura che l'accesso ai Dati personali del Cliente sia consentito esclusivamente a personale autorizzato che abbia necessità di conoscerli ai fini dell'esecuzione del Servizio e che abbia ricevuto adeguate istruzioni in materia di protezione dei dati personali.

9. Misure tecniche e organizzative di sicurezza

9.1 Maxisoft® adotta misure tecniche e organizzative adeguate ai sensi dell'art. 32 GDPR, tenendo conto dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.

9.2 Tali misure includono, ove applicabili e in misura proporzionata:

a) controllo degli accessi logici e autenticazione degli utenti;
b) gestione profilata di ruoli e permessi;
c) separazione logica dei dati e protezione dell'ambiente applicativo;
d) cifratura o altre misure equivalenti di protezione dei dati in transito e, ove opportuno, a riposo;
e) registrazione e monitoraggio degli eventi di sicurezza;
f) sistemi di backup, ripristino, continuità operativa e resilienza;
g) procedure di gestione degli incidenti;
h) test, verifiche e valutazioni periodiche dell'efficacia delle misure adottate;
i) misure organizzative interne di autorizzazione, riservatezza e formazione del personale.

9.3 Le misure di sicurezza attualmente adottate sono descritte nell'Allegato 2, che può essere aggiornato da Maxisoft® in modo da mantenere o migliorare il livello di sicurezza, senza ridurne sostanzialmente l'efficacia.

9.4 Utilizzo dati del Cliente per addestramento sistemi di Intelligenza Artificiale

9.4.1 Divieto di utilizzo dei dati
Maxisoft® si impegna a non utilizzare in alcun modo i dati personali del Cliente trattati ai sensi del presente DPA per l'addestramento, il fine-tuning, il miglioramento o lo sviluppo di modelli di intelligenza artificiale, machine learning o sistemi automatizzati, né di proprietà di Maxisoft® né di terze parti, salvo previo consenso scritto esplicito del Cliente o previa anonimizzazione irreversibile certificata ai sensi dei commi successivi. Tale divieto è assoluto e non ammette eccezioni implicite.

9.4.2 Eccezioni con consenso esplicito
Maxisoft® potrà utilizzare i dati personali del Cliente per finalità di addestramento AI esclusivamente nei seguenti casi:

a) previo consenso scritto esplicito del Cliente, che dovrà specificare:

- le categorie precise di dati che saranno utilizzate;
- le finalità specifiche dell'addestramento;
- i modelli AI che saranno addestrati (interni o terzi);
- le garanzie di sicurezza e riservatezza adottate;
- la durata dell'utilizzo dei dati;
- il diritto del Cliente di revocare il consenso in qualsiasi momento.

b) previa anonimizzazione irreversibile certificata dei dati che garantisca l'impossibilità tecnica di re-identificazione del Cliente, dei suoi clienti finali o di qualsiasi persona fisica. L'anonimizzazione deve essere documentata mediante:

- relazione tecnica che descriva il processo di anonimizzazione;
- conferma che i dati non possono più essere ricondotti a persone identificate o identificabili;
- test di re-identificazione con esito negativo.

Una volta correttamente anonimizzati, i dati cessano di essere dati personali ai sensi dell'art. 4, par. 1, GDPR e Maxisoft® potrà utilizzarli per migliorare i propri algoritmi, creare benchmark di settore o sviluppare funzionalità predittive generali.

9.4.3 Dati aggregati a livello settoriale
Maxisoft® può utilizzare statistiche aggregate derivanti dall'uso del Servizio da parte di minimo 10 clienti (soglia di aggregazione) per creare modelli predittivi generali non personalizzati (es. 'tempo medio riparazione per tipologia di guasto nel settore automotive italiano'), a condizione che:

- l'aggregazione non permetta l'identificazione del singolo Cliente;
- i modelli risultanti siano utilizzabili da tutti i clienti SmartGarage.biz come servizio a valore aggiunto;
- il Cliente possa opporsi a tale utilizzo ai sensi dell'art. 21 GDPR scrivendo a privacy@maxisoft.it.

9.4.4 Sistemi AI utilizzati per l'erogazione del Servizio
Per i sistemi di IA eventualmente integrati nella piattaforma SmartGarage.biz (es. chatbot supporto clienti, agenti vocali, sistemi di raccomandazione), Maxisoft®:

- utilizza modelli di linguaggio di terze parti tramite API che, secondo le condizioni contrattuali dei fornitori, non utilizzano i dati inviati via API per addestrare i loro modelli pubblici;
- utilizza esclusivamente documentazione tecnica, FAQ e knowledge base interne Maxisoft® per fornire risposte contestualizzate;
- non invia ai modelli AI di terze parti dati personali del Cliente oltre a quanto strettamente necessario per fornire la risposta richiesta nel contesto specifico.

9.4.5 Maxisoft® dichiara di non utilizzare, né direttamente né tramite sub-responsabili, i dati personali del Cliente per addestrare modelli di intelligenza artificiale di terze parti che non garantiscano per contratto il divieto di riutilizzo dei dati inviati via API. Tale dichiarazione è aggiornata alla data dell'ultimo aggiornamento del presente DPA.

10. Ricorso a sub-responsabili

10.1 Il Cliente autorizza Maxisoft®, ai sensi dell'art. 28, par. 2 GDPR, a ricorrere a sub-responsabili per lo svolgimento di specifiche attività di trattamento connesse all'erogazione del Servizio.

10.2 Le informazioni sui sub-responsabili inizialmente autorizzati sono riportate nell'Allegato 3 e/o nel registro nominativo dei sub-responsabili espressamente richiamato dal presente DPA. Tale elenco deve indicare almeno, per ciascun sub-responsabile: ragione sociale, funzione svolta, Paese di stabilimento e, ove applicabile, base del trasferimento verso Paesi terzi.

10.3 Maxisoft® potrà aggiungere o sostituire sub-responsabili, a condizione di informarne previamente il Cliente con un preavviso non inferiore a trenta (30) giorni mediante comunicazione scritta o elettronica all'indirizzo e-mail del referente amministrativo indicato dal Cliente, oppure tramite notifica vincolante pubblicata nell'Area Clienti con obbligo di presa visione al successivo accesso.

Tale notifica dovrà contenere le seguenti informazioni minime per consentire al Cliente una valutazione informata:

- ragione sociale e sede legale del nuovo sub-responsabile;
- funzione svolta e categorie di dati trattati;
- Paese di stabilimento e, se extra-SEE, base giuridica del trasferimento;
- eventuali certificazioni di sicurezza possedute (es. ISO 27001, SOC 2);
- data prevista di inizio operatività del nuovo sub-responsabile.

Maxisoft® aggiornerà contestualmente l'Allegato 3 o il registro nominativo dei sub-responsabili.

10.4 Entro il termine di preavviso di cui all'art. 10.3, il Cliente potrà opporsi per iscritto alla nomina del nuovo sub-responsabile per motivi ragionevoli e comprovati connessi alla protezione dei dati personali, trasmettendo comunicazione motivata a privacy@maxisoft.it entro venti (20) giorni solari dal ricevimento della notifica.

L'opposizione è considerata ragionevole se fondata su:

- assenza di adeguate garanzie di sicurezza o certificazioni riconosciute;
- localizzazione in Paese terzo privo di decisione di adeguatezza e con rischi documentati per i diritti degli interessati;
- conflitto con vincoli settoriali, regolamentari o contrattuali gravanti sul Cliente;
- pregresse violazioni di sicurezza o sanzioni da parte del sub-responsabile proposte, se pubblicamente note.

In mancanza di opposizione motivata entro il termine indicato, il nuovo sub-responsabile si intenderà autorizzato e diventerà operativo alla data indicata nella notifica.

10.5 Qualora l’opposizione del Cliente sia ragionevole e non sia possibile individuare una soluzione alternativa tecnicamente o economicamente sostenibile, Maxisoft® potrà sospendere la specifica funzionalità interessata oppure recedere dal Contratto principale con preavviso ragionevole, senza responsabilità ulteriore rispetto al rimborso pro-rata dell’eventuale corrispettivo non goduto per la parte di servizio non erogata.

10.6 Maxisoft® impone a ciascun sub-responsabile, mediante contratto o altro atto giuridico vincolante, obblighi sostanzialmente equivalenti a quelli previsti dal presente DPA, in particolare in materia di riservatezza, sicurezza, assistenza, cancellazione/restituzione e audit, restando responsabile nei confronti del Cliente per l’adempimento degli obblighi del sub-responsabile, nei limiti previsti dalla legge e dal Contratto principale.

10.7 Maxisoft® si impegna a selezionare sub-responsabili che offrano garanzie sufficienti in materia di sicurezza, riservatezza, affidabilità e capacità di gestione degli incidenti, tenendo conto della natura del trattamento affidato, dei rischi connessi e della normativa applicabile.

11. Assistenza al Cliente

11.1 Tenuto conto della natura del trattamento e delle informazioni a disposizione di Maxisoft®, quest’ultimo assiste il Cliente con misure tecniche e organizzative appropriate, nella misura ragionevolmente possibile, per consentire al Cliente di adempiere ai propri obblighi relativi:

a) all’esercizio dei diritti degli interessati;
b) alla sicurezza del trattamento;
c) alla notifica di violazioni dei dati personali all’autorità di controllo e, se necessario, agli interessati;

d) alla valutazione d'impatto sulla protezione dei dati e alla consultazione preventiva dell'autorità di controllo, ove richiesta.

11.2 Qualora Maxisoft® riceva direttamente una richiesta da parte di un interessato avente a oggetto Dati personali del Cliente trattati per conto di quest'ultimo, Maxisoft® informerà il Cliente senza ingiustificato ritardo, salvo che ciò sia vietato dalla legge, e non risponderà nel merito se non su istruzione del Cliente o nei casi previsti dalla legge.

11.3 Salvo diversa previsione del Contratto principale, le attività di assistenza straordinaria, complessa o eccedente le normali funzionalità del Servizio potranno essere rese a fronte di corrispettivo secondo le condizioni economiche vigenti.

12. Gestione delle violazioni dei dati personali

12.1 Maxisoft® notificherà al Cliente qualsiasi violazione dei dati personali senza ingiustificato ritardo e, comunque, entro e non oltre 48 ore dal momento in cui il Responsabile ha acquisito la ragionevole certezza del verificarsi dell'evento, al fine di consentire al Titolare di adempiere agli obblighi di notifica di cui all'art. 33 GDPR. Qualora la natura della violazione lo richieda, Maxisoft® fornirà aggiornamenti successivi senza ritardo.

12.2 La comunicazione conterrà, nella misura in cui le informazioni siano disponibili al momento della notifica:

a) la descrizione della natura della violazione;
b) le categorie di dati e di interessati coinvolti, ove note;
c) le possibili conseguenze della violazione;
d) le misure adottate o proposte per porre rimedio alla violazione e attenuarne gli effetti negativi;
e) ogni informazione ragionevolmente utile al Cliente per adempiere ai propri obblighi di legge.

12.3 Maxisoft® adotterà le misure ragionevoli per contenere, mitigare e gestire la violazione e collaborerà con il Cliente nei limiti richiesti dall'art. 28 GDPR.

12.4 Fermo restando l'obbligo di notifica della violazione dei dati personali di cui al presente articolo, Maxisoft® informerà il Cliente senza ingiustificato ritardo anche in caso di incidente di sicurezza o indisponibilità significativa del Servizio che possa ragionevolmente incidere sulla disponibilità, integrità, autenticità o riservatezza dei Dati personali del Cliente o sulla corretta erogazione del Servizio stesso, fornendo le informazioni ragionevolmente necessarie per la valutazione dell'impatto operativo.

13. Trasferimenti di dati verso Paesi terzi

13.1 Maxisoft® non trasferisce i Dati personali del Cliente verso Paesi terzi o organizzazioni internazionali se non nel rispetto del GDPR.

13.2 Qualora, per esigenze tecniche o organizzative, un trattamento implichi il trasferimento di Dati personali del Cliente verso un Paese non appartenente allo Spazio Economico Europeo, Maxisoft® garantirà che il trasferimento avvenga sulla base di una decisione di adeguatezza della Commissione europea o di altre garanzie appropriate previste dagli artt. 44 e seguenti GDPR, incluse, ove applicabili, le clausole contrattuali standard.

13.3 Ove un sub-responsabile stabilito negli Stati Uniti sia utilizzato per specifiche componenti del Servizio, Maxisoft® potrà fare affidamento, ove applicabile, anche sull'EU-U.S. Data Privacy

Framework, fermo restando l'obbligo di adottare la base di trasferimento appropriata in concreto.

13.4 Su richiesta ragionevole del Cliente, Maxisoft® fornirà informazioni sulla base giuridica del trasferimento applicata in concreto e metterà a disposizione, nei limiti consentiti dalla legge e dagli obblighi di riservatezza verso terzi, copia delle clausole o sintesi delle garanzie appropriate adottate.

14. Audit e verifiche

14.1 Maxisoft® mette a disposizione del Cliente tutte le informazioni e le evidenze documentali o digitali (es. certificazioni di sicurezza, report di audit indipendenti) ragionevolmente necessarie a dimostrare il rispetto degli obblighi previsti dal presente DPA e dall'art. 28 GDPR.

14.2 Salvo che sussistano specifiche esigenze documentate o obblighi di legge, gli audit si svolgeranno prioritariamente mediante:

a) documentazione tecnica e organizzativa;
b) questionari di sicurezza;
c) attestazioni, report, certificazioni o evidenze equivalenti disponibili;
d) riunioni da remoto o verifiche documentali.

14.3 Qualora tali modalità non risultino ragionevolmente sufficienti e il Cliente dimostri un'esigenza concreta e proporzionata, potrà richiedere un audit in loco presso Maxisoft® o presso i locali del sub-responsabile rilevante, previo preavviso scritto di almeno 30 giorni lavorativi, nel normale orario d'ufficio, senza pregiudicare la riservatezza, la sicurezza e la continuità operativa di Maxisoft® e dei suoi altri clienti.

14.4 Gli audit dovranno essere limitati agli aspetti strettamente pertinenti al trattamento dei Dati personali del Cliente e non potranno comportare accesso a informazioni riservate di altri clienti, segreti commerciali, misure di sicurezza la cui divulgazione possa compromettere la protezione dei sistemi, né attività invasive o sproporzionate.

14.5 Ciascun audit sarà effettuato al massimo una volta per anno solare, salvo il verificarsi di una Violazione dei dati personali rilevante o una richiesta specifica dell'autorità competente.

14.6 Salvo diversa previsione inderogabile di legge, i costi degli audit richiesti dal Cliente restano a carico del Cliente.

15. Restituzione e cancellazione dei dati al termine del rapporto

15.1 Alla cessazione del Contratto principale, Maxisoft®, su scelta del Cliente ove tecnicamente possibile e salvo obblighi di legge contrari:

a) restituisce al Cliente i Dati personali del Cliente, oppure li mette a disposizione per l'esportazione tramite le funzionalità del Servizio, in formato strutturato, di uso comune e leggibile da dispositivo automatico, nei limiti delle funzionalità contrattualmente previste; e successivamente

b) cancella o rende anonimi i Dati personali del Cliente residui trattati per suo conto.

Le ulteriori condizioni contrattuali relative a portabilità, switching, tempi tecnici di export e servizi professionali eventualmente connessi restano disciplinate dai Termini e Condizioni SaaS e dalla documentazione contrattuale applicabile.

15.2 Maxisoft® potrà conservare per un periodo limitato e strettamente necessario copie residuali

contenute in sistemi di backup, log tecnici, archivi di sicurezza o supporti di disaster recovery, purché tali dati restino protetti e non siano trattati per finalità ulteriori, salvo che ciò sia richiesto dalla legge.

15.3 Su richiesta ragionevole del Cliente, Maxisoft® potrà fornire conferma dell'avvenuta cancellazione o anonimizzazione, salvo impedimenti tecnici o legali.

16. Responsabilità

16.1 Ciascuna Parte risponde delle proprie violazioni della normativa applicabile in materia di protezione dei dati personali nei limiti previsti dal GDPR, dalla legge applicabile e dal Contratto principale.

16.2 Nulla nel presente DPA limita o esclude responsabilità che non possano essere validamente limitate ai sensi della legge applicabile.

16.3 Salvo dolo o colpa grave e fatti salvi i casi inderogabili di legge, la responsabilità complessiva di Maxisoft® derivante dal presente DPA resta soggetta agli eventuali limiti di responsabilità previsti dal Contratto principale, applicati in misura compatibile con la normativa in materia di protezione dei dati personali.

17. Legge applicabile e foro competente

17.1 Il presente DPA è regolato dalla legge italiana, fatto salvo quanto previsto direttamente dal GDPR e dalla normativa europea applicabile.

17.2 Per ogni controversia relativa al presente DPA sarà competente il foro previsto nel Contratto principale, salvo diversa competenza inderogabile di legge.

18. Modifiche del DPA

18.1 Maxisoft® potrà aggiornare il presente DPA per adeguarlo a evoluzioni normative, provvedimenti delle autorità competenti, modifiche del Servizio, aggiornamenti dei sub-responsabili o esigenze organizzative e tecniche.

18.2 Le modifiche saranno pubblicate in una pagina dedicata del sito e/o dell'area clienti e, ove rilevanti, comunicate al Cliente con congruo preavviso.

18.3 Qualora l'aggiornamento del presente DPA incida in modo sostanziale sugli obblighi di cui all'art. 28 GDPR, sulle misure di sicurezza, sui diritti del Cliente in materia di audit, sub-responsabili, restituzione/cancellazione o trasferimenti verso Paesi terzi, Maxisoft® richiederà una nuova accettazione scritta o elettronica del DPA aggiornato, oppure ne disciplinerà l'efficacia mediante atto scritto/elettronico integrativo. Per modifiche non sostanziali resta ferma la possibilità di comunicazione con congruo preavviso.

Allegato 1
Descrizione del trattamento affidato a Maxisoft® ai sensi dell'art. 28 GDPR

1. Oggetto del trattamento

Erogazione del servizio software SaaS SmartGarage.biz e dei servizi tecnici connessi, inclusi hosting applicativo, conservazione dei dati, gestione degli account applicativi, configurazioni, sicurezza, backup, manutenzione, assistenza e supporto tecnico.

2. Durata del trattamento
Per tutta la durata del Contratto principale e per il tempo strettamente necessario alla cessazione tecnica del servizio, all'esportazione, restituzione, cancellazione, gestione dei backup residuali e adempimento di eventuali obblighi di legge.

3. Natura del trattamento
Raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento, consultazione, utilizzo, comunicazione limitata ai sub-responsabili autorizzati, raffronto, interconnessione, cancellazione, distruzione e ogni altra operazione strettamente necessaria all'erogazione del Servizio.

4. Finalità del trattamento
Consentire al Cliente di utilizzare SmartGarage.biz per la gestione digitale dei propri processi operativi, amministrativi, commerciali e organizzativi, nei limiti delle funzionalità acquistate e delle istruzioni impartite dal Cliente.

5. Categorie di interessati
A titolo esemplificativo:
- clienti e potenziali clienti del Cliente;
- fornitori del Cliente;
- dipendenti, collaboratori, consulenti e operatori del Cliente;
- utenti autorizzati della piattaforma;
- ulteriori soggetti i cui dati siano legittimamente inseriti dal Cliente nel Servizio.

6. Categorie di dati personali e dati tecnici identificativi
A titolo esemplificativo e non esaustivo:
- dati anagrafici e di contatto dei proprietari/utilizzatori;
- dati di contatto;
- dati professionali e organizzativi;
- dati relativi a veicoli, interventi, appuntamenti, documenti commerciali, ordini di lavoro e storico operativo, nei limiti delle funzionalità del Servizio;
- dati identificativi del veicolo (VIN - Numero di Telaio, Targa): trattati in conformità alla giurisprudenza UE (C-319/22) che qualifica tali identificativi come dati personali qualora associabili a persone fisiche;
- dati tecnici di telemetria, log di manutenzione e storico riparazioni associati al veicolo. Tali dati sono trattati in conformità al Regolamento (UE) 2023/2854 (Data Act) per quanto concerne i diritti di accesso e portabilità dei dati generati dai prodotti connessi, restando onere del Cliente gestire le richieste di accesso dei proprietari dei veicoli.
- dati amministrativi, contabili e commerciali;
- dati contenuti in note, allegati, ticket e documenti caricati dal Cliente, nonché, ove la relativa funzionalità sia attivata dal Cliente o prevista dal Servizio, eventuali registrazioni audio o trascrizioni derivanti dalle interazioni vocali con strumenti di supporto tecnico;
- dati di autenticazione e tracciamento applicativo degli utenti autorizzati.

7. Categorie particolari di dati personali (art. 9 GDPR) e dati giudiziari (art. 10 GDPR)

7.1 Divieto generale
Il Servizio SmartGarage.biz non è progettato per il trattamento sistematico o su larga scala di categorie particolari di dati ai sensi dell'art. 9 GDPR (dati sanitari, genetici, biometrici, origene razziale o etnica,

opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, vita sessuale o orientamento sessuale) o di dati relativi a condanne penali e reati ai sensi dell'art. 10 GDPR.
Il Cliente si impegna a non utilizzare il Servizio per tali trattamenti, salvo quanto previsto ai punti 7.2 e 7.3.

7.2 Trattamenti occasionali consentiti nel settore automotive
Nel contesto specifico dell'attività di officina/concessionaria automotive, il Cliente può occasionalmente trattare tramite il Servizio le seguenti categorie di dati particolari, limitatamente ai casi in cui ciò sia strettamente necessario per finalità amministrative, fiscali o contrattuali legittime:

a) **Certificati medici per agevolazioni fiscali auto disabili** (L. 104/1992):
- Certificato invalidità allegato a pratica vendita/modifica veicolo;
- Documentazione per applicazione IVA agevolata 4% su acquisto auto;
- Esenzione bollo auto;
- Base giuridica: art. 9, par. 2, lett. f) GDPR (accertamento diritti - agevolazioni fiscali).

b) **Documentazione sanitaria per accesso ZTL/parcheggi riservati disabili**
- Copie contrassegno disabili allegato a richiesta assistenza;
- Base giuridica: art. 9, par. 2, lett. f) GDPR.

c) **Dati assicurativi RCA** (contenenti potenzialmente dati sanitari in caso sinistri con lesioni):
- Documentazione sinistri per pratiche assicurative;
- Base giuridica: art. 9, par. 2, lett. f) GDPR (accertamento diritti assicurativi).

7.3 Obblighi del Cliente per trattamenti art. 9 GDPR
Qualora il Cliente tratti occasionalmente categorie particolari di dati come previsto al punto 7.2, deve:

- Verificare la sussistenza della base giuridica applicabile (es. art. 9, par. 2, lett. f);
- Adottare misure tecniche e organizzative supplementari appropriate (es. limitazione accessi, crittografia documenti, compartimentazione);
- Eseguire valutazione di impatto (DPIA) ai sensi dell'art. 35 GDPR se il trattamento presenta rischio elevato;
- Informare adeguatamente gli interessati con informativa specifica;
- Conservare i dati per il solo tempo strettamente necessario.

7.4 Trattamenti sistematici o su larga scala
Per trattamenti sistematici, su larga scala o particolarmente critici di categorie particolari di dati (es. gestione dati sanitari clienti per flotte aziendali con servizi di telemedicina, archivio massivo certificati medici), il Cliente deve:

- darne comunicazione preventiva scritta a Maxisoft® (privacy@maxisoft.it);
- richiedere la valutazione congiunta dell'adeguatezza delle misure tecniche di sicurezza del Servizio;
- sottoscrivere, se necessario, un addendum tecnico-organizzativo dedicato con misure supplementari specifiche.

In assenza di tale comunicazione e accordo, Maxisoft® non può essere ritenuta responsabile per eventuali inadeguatezze delle misure tecniche standard del Servizio rispetto ai rischi specifici di tali categorie di dati.

7.5 Dati relativi a condanne penali e reati (art. 10 GDPR)
Il trattamento di dati relativi a condanne penali e reati è consentito esclusivamente sotto il controllo dell'autorità pubblica o se autorizzato dal diritto dell'Unione o degli Stati membri. Il Cliente garantisce

di non utilizzare il Servizio per tali trattamenti, salvo che disponga di specifica autorizzazione legale e ne abbia dato preventiva comunicazione scritta a Maxisoft®.

Allegato 2
Misure tecniche e organizzative di sicurezza

Maxisoft® adotta, in modo proporzionato alla natura del Servizio e ai rischi del trattamento, misure tecniche e organizzative comprendenti, a titolo esemplificativo:

1. **Controllo degli accessi**
   Gestione credenziali, autenticazione, profilazione utenti, ruoli e permessi differenziati, limitazione degli accessi amministrativi.

2. **Protezione dei sistemi e delle comunicazioni**
   Protezione perimetrale, monitoraggio, logging tecnico, sistemi di prevenzione e rilevazione di anomalie, cifratura delle comunicazioni ove applicabile.

3. **Separazione logica e minimizzazione (Data Segregation)**
   Separazione logica dei dati tra clienti, restrizione dell'accesso ai soli soggetti autorizzati e limitazione dei trattamenti al minimo necessario. L'architettura del Servizio è progettata per ridurre il rischio di accessi incrociati non autorizzati tra ambienti o dati riferibili a clienti diversi. Ove applicabile, i dati identificativi più sensibili possono essere protetti anche mediante misure di cifratura a riposo (encryption at rest) o soluzioni tecniche equivalenti per mitigare i rischi in caso di accesso fisico non autorizzato alle infrastrutture storage.

4. **Backup e resilienza**
   Procedure di backup e ripristino, misure di continuità operativa e disaster recovery proporzionate al servizio.

5. **Gestione incidenti**
   Procedure interne per identificazione, gestione, tracciamento e risposta a incidenti di sicurezza e violazioni dei dati personali.

6. **Sicurezza organizzativa**
   Autorizzazione del personale, obblighi di riservatezza, istruzioni interne, gestione delle credenziali e processi di revisione degli accessi.

7. **Manutenzione e aggiornamento**
   Aggiornamento software e infrastrutturale, correzione vulnerabilità, interventi di manutenzione ordinaria e straordinaria.

8. **Verifiche periodiche**
   Controlli e verifiche ragionevoli sull'efficacia delle misure adottate, con eventuale adeguamento in funzione dell'evoluzione tecnologica e dei rischi.

9. **Test di vulnerabilità e verifiche tecniche**
   Maxisoft® pianifica ed esegue, con frequenza coerente con il rischio, test di vulnerabilità, verifiche tecniche e controlli di sicurezza finalizzati a valutare e migliorare l'efficacia dei controlli adottati per la protezione dei dati e dei sistemi.

10. **Standard e certificazioni**
    Maxisoft® adotta misure di sicurezza ispirate a standard internazionali:

- **norma ISO 9001:2015** (Sistema di Gestione Qualità).
  Maxisoft® opera da oltre 20 anni (2006-2026) con un Sistema di Gestione della Qualità certificato dall'Ente **IMQ**, organismo accreditato **Accredia** (**Certificato n. 9150.MXSF**);

- **norma ISO/IEC 27001** (Sistema di Gestione Sicurezza Informazioni).
  Principi e controlli applicati da Maxisoft® anche in assenza di certificazione formale;

- **Direttiva (UE) 2022/2555 (NIS2)** in materia di cybersicurezza (gestione rischi, incident management, business continuity).
  Principi e controlli applicati da Maxisoft® anche in assenza di certificazione formale.

  Resta inteso che i riferimenti alla NIS2 descrivono il framework adottato e non costituiscono dichiarazione di qualifica automatica di Maxisoft® quale soggetto essenziale o importante ai sensi della normativa, salvo diversa comunicazione ufficiale.

Allegato 3
Sub-responsabili autorizzati

Il Cliente autorizza Maxisoft® a ricorrere, ove necessario, a fornitori terzi per lo svolgimento di specifiche attività di trattamento, quali a titolo esemplificativo:

- servizi di hosting, cloud, housing e data center;
- servizi di backup, monitoraggio e sicurezza;
- servizi di assistenza tecnica e manutenzione infrastrutturale;
- servizi di gestione ticket, supporto tecnico o comunicazioni di servizio;
- provider di servizi e-mail transazionali e notifiche;
- ulteriori fornitori strettamente necessari all'erogazione del Servizio.

Alla data dell'ultimo aggiornamento del presente DPA, i sub-responsabili inizialmente autorizzati dal Cliente sono i seguenti:

1. Aruba S.p.A.
   - Funzione svolta: housing , data center, servizi cloud, hosting infrastrutturale, SMS gateway
   - Paese di stabilimento/trattamento: Italia
   - Eventuale trasferimento extra SEE: No

2. Dropbox International Unlimited Company
   - Funzione svolta: servizi di backup crittografati AES a 256 bit
   - Paese di stabilimento/trattamento: Irlanda
   - Eventuale trasferimento extra SEE: Si
   - Base del trasferimento: EU-U.S. Data Privacy Framework (DPF) / EU Cloud Code of Conduct / Clausole Contrattuali Standard (SCC) approvate da Commissione europea

3. HubSpot Ireland Ltd.
   - Funzione svolta: provider di servizi CRM, e-mail transazionali e notifiche
   - Paese di stabilimento/trattamento: Irlanda

- Eventuale trasferimento extra SEE: Si
- Base del trasferimento: Data Privacy Framework (UE-USA, Svizzera-USA, estensione UK) / Clausole Contrattuali Standard (SCC) approvate da Commissione europea

4. Stripe LLC.
    - Funzione svolta: Provider per gestione pagamenti online
    - Paese di stabilimento/trattamento: USA, California
    - Eventuale trasferimento extra SEE: Si
    - Base del trasferimento: Data Privacy Framework (DPF) UE-USA / Clausole Contrattuali Standard (SCC) approvate da Commissione europea

5. Zoom Video Communications, Inc.
    - Funzione svolta: Provider di sistemi di videoconferenza
    - Paese di stabilimento/trattamento: USA, California
    - Eventuale trasferimento extra SEE: Si
    - Base del trasferimento: EU-U.S. Data Privacy Framework / Clausole Contrattuali Standard (SCC) approvate da Commissione europea

In conformità alle raccomandazioni dell'EDPB, Maxisoft® dichiara di aver eseguito (o di avvalersi delle valutazioni fornite dai sub-responsabili) una valutazione dell'impatto del trasferimento (Transfer Impact Assessment - TIA) per i fornitori extra-SEE indicati, confermando che le garanzie adottate assicurano un livello di protezione sostanzialmente equivalente a quello garantito nell'Unione Europea.

L’elenco nominativo aggiornato dei sub-responsabili è mantenuto da Maxisoft® in una sezione dedicata dell’area clienti e/o del sito, espressamente richiamata nel presente DPA, ed è reso facilmente accessibile al Cliente. Ogni modifica all’elenco è comunicata secondo quanto previsto dall’art. 10 del presente DPA.