CONTRATTO · ART. 28 GDPR

Data Processing Agreement

Accordo sul trattamento dei dati personali dei clienti finali del Concessionario, ai sensi dell'art. 28 del Regolamento (UE) 2016/679. Il Concessionario è Titolare del trattamento, Azure S.r.l. è Responsabile per suo conto.

VERSIONE	v1.2-2026-09
DATA DI EFFICACIA	data di accettazione elettronica da parte del Titolare (artt. 2.2 e 16)
RESPONSABILE	Azure S.r.l. — P.IVA IT13005450963
TITOLARE	il Concessionario sottoscrittore
TESTO CANONICO	dealermax.app/legal/dpa
SHA-256 DEL TESTO	3773375edc23555e75b52d3a3167c4facbf55f796ed0fb3d5c90602d63787a74

Documento generato dal testo canonico versionato. L'impronta SHA-256 riportata sopra identifica in modo univoco il testo di questa versione: è la stessa archiviata come evidenza dell'accettazione (art. 16.2).

TRA

Azure S.r.l., con sede legale in Via della Resistenza 121/A, 20090 Buccinasco (MI), P.IVA IT13005450963, C.F. 13005450963, PEC azureautomotive@pec.it, in persona del legale rappresentante pro tempore (di seguito **"Responsabile"** o **"Azure"**),

E

l'Utente Concessionario sottoscrittore tramite checkbox in fase di onboarding alla piattaforma DealerMax (i cui dati identificativi — ragione sociale, sede legale, P.IVA, REA, PEC, legale rappresentante — sono raccolti in onboarding e archiviati in piattaforma) (di seguito **"Titolare"** o **"Dealer"**)

(congiuntamente le "**Parti**")

PREMESSE

(a) Azure è una società che fornisce, in modalità Software-as-a-Service, una piattaforma tecnologica integrata denominata **"DealerMax"**, comprensiva dei moduli DealerMax (gestionale dealer), DealerWebsite (siti pubblici dei concessionari), GarageMAX (piattaforma utenti finali) e servizi correlati di automazione, comunicazione e content marketing assistito da intelligenza artificiale.

(b) Il Titolare ha sottoscritto separato contratto di servizio (Termini e Condizioni d'uso e/o Contratto di servizio) con Azure per l'utilizzo della piattaforma DealerMax e tramite essa raccoglie e tratta dati personali dei propri clienti finali e prospect.

(c) L'utilizzo della piattaforma comporta che Azure tratti, in nome e per conto del Titolare, dati personali appartenenti agli interessati (clienti finali, prospect, lead, nonché utenti GarageMAX limitatamente ai dati della loro relazione con il Titolare, come precisato all'art. 3.6). Tale trattamento richiede ai sensi dell'art. 28 GDPR la stipula di un contratto di nomina a Responsabile del trattamento.

(d) Il presente DPA disciplina il trattamento dei dati personali svolto da Azure quale Responsabile del trattamento per conto del Titolare, in conformità al GDPR e alla normativa nazionale italiana applicabile (D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018).

(e) Il presente DPA si applica esclusivamente al trattamento dei dati personali svolto da Azure in nome e per conto del Titolare. Non si applica ai dati personali raccolti e trattati da Azure in qualità di Titolare autonomo (es. dati di contatto del legale rappresentante del Titolare per fini contrattuali, dati di fatturazione, ecc.), per i quali si rinvia alla Privacy Policy di Azure pubblicata su https://dealermax.app/privacy.

Tutto ciò premesso, le Parti convengono e stipulano quanto segue.

1. DEFINIZIONI

Ai fini del presente DPA, salvo diversa indicazione, si applicano le definizioni dell'art. 4 GDPR. In particolare:

- **"GDPR"**: Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016.
- **"Dato Personale"**: qualsiasi informazione riguardante una persona fisica identificata o identificabile, ai sensi dell'art. 4.1 GDPR.
- **"Trattamento"**: qualsiasi operazione svolta sui Dati Personali ai sensi dell'art. 4.2 GDPR.
- **"Titolare"**: il Dealer sottoscrittore, in quanto soggetto che determina finalità e mezzi del Trattamento dei Dati Personali dei propri clienti finali, prospect e lead.
- **"Responsabile"**: Azure S.r.l., in quanto soggetto che tratta i Dati Personali per conto del Titolare.
- **"Interessato"**: la persona fisica cui si riferiscono i Dati Personali (cliente finale, prospect, lead, utente GarageMAX limitatamente ai dati di cui all'art. 3.2 lett. (c), nei limiti di perimetro dell'art. 3.6).

- **"Sub-Responsabile"** o **"Subprocessor"**: ogni soggetto, persona fisica o giuridica, che Azure incarichi del trattamento dei Dati Personali, inclusi i fornitori di infrastruttura, comunicazione e servizi AI elencati nell'Allegato B.
- **"Violazione dei Dati Personali"** o **"Data Breach"**: ai sensi dell'art. 4.12 GDPR.
- **"Misure Tecniche e Organizzative"** o **"TOM"**: le misure di cui all'art. 32 GDPR descritte nell'Allegato A.
- **"Piattaforma"**: l'insieme dei servizi DealerMax SaaS forniti da Azure al Titolare.
- **"Periodo di Trattamento"**: la durata del contratto di servizio principale tra il Titolare e Azure, ivi compresi i periodi di conservazione post-terminazione di cui all'art. 11.

2. OGGETTO E DURATA

2.1 Oggetto

Il presente DPA disciplina il trattamento dei Dati Personali che Azure svolge in nome e per conto del Titolare per la fornitura dei servizi della Piattaforma DealerMax, conformemente all'art. 28.3 GDPR.

2.2 Durata

Il DPA ha efficacia dalla data di accettazione tramite checkbox in onboarding e resta in vigore per tutta la durata del contratto di servizio principale tra le Parti, ivi compresi i periodi successivi alla terminazione previsti dall'art. 11 per la restituzione e/o cancellazione dei dati.

2.3 Cessazione

Il DPA cessa contestualmente al contratto di servizio principale. Le obbligazioni di cancellazione e/o restituzione dei dati di cui all'art. 11 sopravvivono alla cessazione.

3. NATURA, FINALITÀ E TIPO DEI DATI PERSONALI TRATTATI

3.1 Finalità del Trattamento

Azure tratta i Dati Personali esclusivamente per le seguenti finalità, su istruzioni documentate del Titolare:

- (a) gestione del rapporto commerciale del Titolare con i propri clienti finali e prospect (CRM, gestione lead, anagrafica clienti);
- (b) comunicazioni omnichannel del Titolare verso i propri clienti finali e prospect (email transactional, in roadmap WhatsApp Business e canali di comunicazione equivalenti);
- (c) gestione del sito web pubblico del Titolare (DealerWebsite), inclusi form di contatto, configurazione vetrine veicoli, presentazione catalogo;
- (d) generazione di contenuti di marketing assistita da intelligenza artificiale (descrizioni veicoli, brand stories, podcast, materiale per social), con eventuale utilizzo di nominativo del Titolare e/o, ove strettamente necessario, di alcuni dati identificativi del cliente finale all'interno del prompt AI;
- (e) reportistica, analytics aggregate e dashboard di gestione interna del Titolare;
- (f) compliance normativa (es. archiviazione consensi, audit log, gestione diritti GDPR degli Interessati).

3.2 Categorie di Interessati

Le categorie di Interessati i cui Dati Personali sono trattati comprendono:

- (a) clienti finali del Titolare (acquirenti, persone fisiche o titolari/legali rappresentanti di persone giuridiche clienti);
- (b) prospect del Titolare (lead da form contatto, richieste informazioni, contatti telefonici);
- (c) utenti registrati alla piattaforma GarageMAX collegati al Titolare (follow del concessionario, preventivi NLT, wishlist, opt-in marketing);
- (d) destinatari di comunicazioni email/messaging in nome del Titolare (newsletter, lead nurturing, comunicazioni post-vendita).

3.3 Categorie di Dati Personali

Le categorie di Dati Personali trattati comprendono (lista esaustiva nell'Allegato C):

- (a) **dati identificativi**: nome, cognome, ragione sociale, codice fiscale, partita IVA;
- (b) **dati di contatto**: email, telefono, indirizzo postale;
- (c) **dati di interazione**: thread conversazionali tra cliente finale e Titolare (canale email, in roadmap WhatsApp), allegati a tali thread, registrazioni interazioni;
- (d) **dati di interesse commerciale**: veicoli di interesse, configurazioni preventivi, follow concessionario, opt-in marketing, consensi commerciali;
- (e) **dati tecnici dell'infrastruttura**: indirizzo IP, user-agent, timestamp accesso, log di sicurezza, log applicativi (con misure di pseudonimizzazione e minimizzazione descritte nell'Allegato A);
- (f) **dati relativi al veicolo del cliente**: targa, telaio, ricerche valutazione usato (laddove riconducibili a persona fisica via collegamento indiretto).

3.4 Esclusioni

Categorie particolari di dati personali ex art. 9 GDPR (origine razziale, opinioni politiche, convinzioni religiose, dati biometrici, dati sanitari, dati relativi alla vita sessuale o orientamento sessuale) **non sono oggetto di trattamento intenzionale tramite la Piattaforma**. Il Titolare si impegna a non immettere intenzionalmente tali categorie di dati. Eventuali categorie particolari di dati immesse occasionalmente dall'Interessato all'interno di campi free-text (es. body messaggio email) non costituiscono trattamento intenzionale ex art. 9 e sono soggette alle medesime tutele applicate ai dati comuni.

Dati relativi a condanne penali e reati ex art. 10 GDPR non sono oggetto di trattamento.

Il Titolare si impegna a non inserire intenzionalmente nella Piattaforma categorie particolari di dati personali ex art. 9 GDPR o dati relativi a condanne penali e reati ex art. 10 GDPR, salvo previa istruzione scritta, valutazione di liceità, configurazione tecnica idonea e accordo specifico tra le Parti. Azure potrà rifiutare o sospendere trattamenti che comportino l'immissione sistematica di tali categorie di dati in assenza di idoneo presupposto giuridico e misure adeguate.

3.5 Trattamenti con sistemi di intelligenza artificiale

Le funzionalità di generazione assistita da intelligenza artificiale sono utilizzate per produrre, ottimizzare o suggerire contenuti relativi a veicoli, annunci, comunicazioni commerciali, descrizioni, materiali marketing, contenuti editoriali e automazioni della Piattaforma.

Azure applica, ove tecnicamente possibile e ragionevole, principi di minimizzazione e pseudonimizzazione dei dati inviati ai sistemi AI. I prompt destinati a fornitori AI esterni devono contenere esclusivamente i dati necessari alla specifica funzionalità richiesta dal Titolare o dall'utente autorizzato.

Salvo funzionalità espressamente configurate dal Titolare, Azure non utilizza intenzionalmente categorie particolari di dati personali ex art. 9 GDPR, dati relativi a condanne penali e reati ex art. 10 GDPR o dati non necessari all'erogazione della funzionalità AI.

Azure si avvale di fornitori AI elencati tra i Sub-Responsabili, ove tali fornitori trattino Dati Personali per conto di Azure nell'erogazione della Piattaforma. Le condizioni applicabili al trattamento da parte dei fornitori AI sono documentate nell'Allegato B e nella relativa pagina subprocessor.

3.6 Perimetro GarageMAX: distinzione dei ruoli

GarageMAX è un servizio rivolto alle persone fisiche, che vi accedono con un proprio account e vi conservano informazioni relative ai propri veicoli. Rispetto a tale servizio i ruoli sono così ripartiti:

(a) **Azure è Titolare autonomo** dell'account GarageMAX e del garage personale dell'utente — creazione e autenticazione dell'account, veicoli salvati, documenti e scadenze caricati dall'utente, notifiche di servizio, sicurezza e funzionamento della piattaforma. Tali trattamenti sono determinati da Azure, sono identici per tutti gli utenti e prescindono dall'esistenza di un rapporto con un concessionario. Non rientrano nel presente DPA e sono disciplinati dall'informativa pubblicata su https://garagemax.app/privacy.

(b) **Il Titolare è titolare del trattamento e Azure agisce quale Responsabile** limitatamente ai Dati Personali che descrivono la **relazione tra l'utente GarageMAX e il Titolare**: follow del concessionario, preventivi e proposte di noleggio inviati dal Titolare, wishlist e manifestazioni di interesse rivolte al Titolare, consensi e opposizioni marketing riferiti al Titolare, conversazioni tra l'utente e il Titolare, e associazione dell'utente all'anagrafica clienti del Titolare. È questo, e soltanto questo, il perimetro dell'art. 3.2 lett. (c).

(c) Il Titolare **non accede** al garage personale dell'utente né ai dati di cui alla lettera (a); accede esclusivamente ai dati di cui alla lettera (b), tramite le funzionalità della Piattaforma.

(d) L'eventuale presentazione del servizio GarageMAX a un indirizzo recante il marchio del Titolare non modifica la ripartizione dei ruoli di cui al presente articolo e non attribuisce al Titolare la titolarità dei trattamenti di cui alla lettera (a).

4. OBBLIGHI DEL RESPONSABILE (art. 28.3 GDPR)

Azure, in qualità di Responsabile del trattamento, si obbliga a:

4.1 Trattamento su istruzioni documentate

Trattare i Dati Personali soltanto su istruzioni documentate del Titolare, anche in caso di trasferimento di Dati Personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui Azure è soggetta. Le istruzioni documentate sono costituite da:

- (a) il presente DPA;
- (b) il contratto di servizio principale;
- (c) la configurazione operativa della Piattaforma da parte del Titolare (es. attivazione moduli, attivazione lingue, attivazione canali omnichannel, configurazione retention);
- (d) eventuali istruzioni scritte aggiuntive trasmesse via email a team@azureautomotive.it o via altro canale formale concordato.

In caso di istruzione che, a parere di Azure, violi il GDPR o altre normative applicabili, Azure ne informa immediatamente il Titolare.

4.2 Riservatezza

Garantire che le persone autorizzate al trattamento dei Dati Personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza. Azure mantiene un elenco aggiornato delle persone autorizzate, con livelli di accesso differenziati secondo il principio di need-to-know e least-privilege (RBAC a 6 ruoli: admin / admin_team / dealer / dealer_team / superadmin / garage).

4.3 Misure di sicurezza

Adottare tutte le misure tecniche e organizzative richieste dall'art. 32 GDPR, descritte nel dettaglio all'Allegato A.

4.4 Sub-Responsabili

(a) Il Titolare autorizza Azure, ai sensi dell'art. 28.2 GDPR, ad avvalersi di Sub-Responsabili per l'erogazione, manutenzione, sicurezza, hosting, comunicazione, analytics, automazione e funzionalità AI della Piattaforma.

(b) La lista dei Sub-Responsabili autorizzati alla data di efficacia del presente DPA è indicata nell'Allegato B e mantenuta aggiornata all'indirizzo https://dealermax.app/legal/subprocessors.

(c) Azure informa il Titolare di ogni aggiunta o sostituzione sostanziale di Sub-Responsabili con almeno 30 giorni di preavviso, mediante email all'indirizzo comunicato dal Titolare e/o avviso in piattaforma.

(d) Il Titolare può opporsi alla nomina di un nuovo Sub-Responsabile per motivi ragionevoli e documentati connessi alla protezione dei Dati Personali, entro il termine di preavviso. In caso di opposizione, le Parti si confrontano in buona fede per individuare una soluzione alternativa ragionevole. Qualora non sia possibile individuare una soluzione senza pregiudicare l'erogazione della Piattaforma, il Titolare potrà recedere dal contratto di servizio principale senza penali,

limitatamente ai servizi interessati.

(e) In caso di sostituzione urgente necessaria per ragioni di sicurezza, continuità operativa, cessazione improvvisa del servizio da parte di un fornitore o obbligo legale, Azure può nominare un Sub-Responsabile con preavviso ridotto, informando il Titolare senza ingiustificato ritardo.

(f) Azure impone a ciascun Sub-Responsabile obblighi in materia di protezione dei dati personali sostanzialmente equivalenti a quelli previsti dal presente DPA. Azure resta responsabile nei confronti del Titolare dell'adempimento degli obblighi del Sub-Responsabile, nei limiti previsti dal GDPR e dal presente DPA.

4.5 Supporto ai diritti degli Interessati

Assistere il Titolare con misure tecniche e organizzative adeguate al fine di soddisfare l'obbligo del Titolare di rispondere alle richieste degli Interessati per l'esercizio dei diritti di cui agli artt. 15-22 GDPR (accesso, rettifica, cancellazione, limitazione, portabilità, opposizione, decisioni automatizzate).

In particolare, Azure mette a disposizione del Titolare:

- (a) endpoint applicativi e funzioni di amministrazione per esercizio diretto da parte del Titolare;
- (b) procedura di assistenza dedicata via team@azureautomotive.it per casi che richiedano intervento del Responsabile;
- (c) per gli utenti GarageMAX, accesso self-service ai diritti tramite endpoint GET /api/garage/account/export (portabilità) e DELETE /api/garage/account/me (cancellazione dell'account: archiviazione immediata dell'account e anonimizzazione immediata di email, nome, cognome e recapito telefonico; i restanti dati dell'account seguono la politica di conservazione di Azure quale Titolare autonomo, art. 3.6). Quando l'Interessato è parte di contratti conclusi, documenti sottoscritti o mandati di mediazione in corso la cui conservazione è imposta dalla legge o necessaria alla tutela di un diritto (art. 17, par. 3, lett. b ed e, GDPR), la richiesta non è eseguita in automatico: è registrata nell'audit log e presa in carico da Azure, che la evade entro un mese per i dati non soggetti a conservazione e ne informa l'Interessato.

Tempi di risposta: Azure si impegna a fornire supporto al Titolare entro 7 giorni lavorativi dalla richiesta scritta.

4.6 Supporto a DPIA e consultazione preventiva

Assistere il Titolare nel garantire il rispetto degli obblighi di cui agli artt. 32-36 GDPR, tenendo conto della natura del trattamento e delle informazioni a disposizione di Azure, in particolare per:

- (a) sicurezza del trattamento (art. 32);
- (b) notifica violazione (artt. 33-34);
- (c) Data Protection Impact Assessment / DPIA (art. 35);
- (d) consultazione preventiva del Garante (art. 36).

4.7 Notifica violazione (art. 33)

Notificare al Titolare ogni Violazione dei Dati Personali, senza ingiustificato ritardo e in ogni caso **entro 48 ore** dalla conoscenza della stessa, fornendo le informazioni di cui all'art. 33.3 GDPR. La procedura operativa è descritta nel Playbook Incident Response.

Azure assiste il Titolare nell'adempimento dell'obbligo di notifica al Garante (art. 33) e di comunicazione all'Interessato (art. 34), fornendo tutte le informazioni necessarie e supporto operativo.

4.8 Cancellazione e restituzione dati

Su richiesta del Titolare, e in ogni caso al termine del Periodo di Trattamento, cancellare o restituire al Titolare tutti i Dati Personali trattati, conformemente alla procedura dettagliata all'art. 11.

4.9 Conformità documentale

Mettere a disposizione del Titolare, su richiesta, tutte le informazioni necessarie per dimostrare il rispetto degli obblighi del presente DPA e dell'art. 28 GDPR. La modalità di esercizio del diritto di audit è disciplinata all'art. 9.

5. OBBLIGHI DEL TITOLARE

Il Titolare si obbliga a:

5.1
Trattare i Dati Personali tramite la Piattaforma in conformità al GDPR e alla normativa nazionale applicabile, fornendo in particolare adeguata informativa agli Interessati (art. 13 GDPR) e raccogliendo i consensi laddove richiesti dalla base giuridica adottata.

5.2
Configurare la Piattaforma in modo che i trattamenti effettuati siano coerenti con le finalità dichiarate e con la base giuridica scelta dal Titolare (es. consenso, esecuzione contratto, legittimo interesse).

5.3
Mantenere aggiornato il registro dei trattamenti del Titolare (art. 30.1 GDPR), avvalendosi del presente DPA quale documentazione di supporto.

5.4
Fornire ad Azure un punto di contatto Privacy del Titolare (email + telefono), aggiornato in caso di modifica.

5.5
Notificare ad Azure tempestivamente eventuali richieste degli Interessati o dell'autorità di controllo che richiedano supporto operativo del Responsabile.

5.6 Inviti e attivazioni GarageMAX su iniziativa del Titolare
Qualora il Titolare, avvalendosi delle funzionalità della Piattaforma, comunichi ad Azure i dati di contatto di un proprio cliente per invitarlo a GarageMAX o per richiedergli la sottoscrizione elettronica di un documento — determinando così la creazione o l'attivazione di un account GarageMAX intestato a quella persona — il Titolare garantisce:

- (a) di aver reso all'interessato l'informativa di cui all'art. 13 GDPR, comprensiva dell'indicazione di Azure quale destinatario dei dati e della circostanza che l'attivazione del servizio GarageMAX comporta un trattamento di cui Azure è titolare autonomo ai sensi dell'art. 3.6 lett. (a);
- (b) di disporre di una base giuridica idonea alla comunicazione dei dati ad Azure per tale finalità;
- (c) di aver verificato l'esattezza e l'aggiornamento dei dati di contatto comunicati.

Azure, dal canto proprio, rende all'interessato l'informativa relativa ai trattamenti di cui è titolare autonomo, indicandone la fonte ai sensi dell'art. 14 GDPR, alla pagina https://garagemax.app/privacy e in occasione del primo accesso al servizio.

6. SUBPROCESSOR

La lista completa dei Sub-Responsabili in essere alla data del presente DPA è riportata nell'Allegato B e mantenuta aggiornata sulla pagina pubblica https://dealermax.app/legal/subprocessors.

Modifiche e aggiornamenti seguono la procedura di cui all'art. 4.4, lett. (c) (preavviso di almeno 30 giorni) e lett. (d) (opposizione del Titolare).

7. MISURE TECNICHE E ORGANIZZATIVE (TOM)

Le misure di cui all'art. 32 GDPR sono dettagliate nell'Allegato A.

In sintesi, Azure adotta:

- (a) cifratura in-transit (TLS 1.3) e cifratura at-rest selettiva (AES-256-GCM su token sensibili e credenziali OAuth);
- (b) controllo accessi RBAC a 6 ruoli;
- (c) audit log strutturato delle operazioni rilevanti;
- (d) backup automatici con politica di retention documentata;
- (e) procedure di incident response (vedi Playbook);
- (f) programma di vulnerability management;
- (g) roadmap di penetration testing esterno annuale (target prima esecuzione: Q3-2026);
- (h) pseudonimizzazione strutturale (ID interni separati da PII);
- (i) politica di retention dati articolata su due perimetri distinti: (i.1) i Dati Personali trattati per conto del Titolare seguono i termini dell'art. 11 (cessazione del trattamento attivo entro 5 giorni lavorativi, finestra di esportazione di 90 giorni, quindi cancellazione o anonimizzazione irreversibile dai sistemi attivi, con soft-delete 30 giorni e hard-delete successivo); (i.2) i dati che Azure conserva in qualità di Titolare autonomo ai sensi dell'art. 11.6 (obblighi fiscali, contabili, contrattuali, probatori) sono conservati per il tempo previsto dalla normativa applicabile e comunque non oltre 5 anni dalla cessazione del rapporto, salvo obbligo di legge o difesa di diritti in giudizio;
- (j) tracciamento consensi versionato (consent_marketing_at, consent_source, consent_text_version).

Le misure sono soggette a evoluzione tecnologica. Azure si riserva il diritto di adottare misure equivalenti o superiori, comunicandolo al Titolare in caso di modifiche sostanziali.

8. TRASFERIMENTI EXTRA-SEE

8.1 I Dati Personali trattati per conto del Titolare sono trattati, di regola, all'interno dello Spazio Economico Europeo o mediante fornitori che garantiscono un idoneo meccanismo di trasferimento ai sensi del Capo V GDPR.

8.2 Qualora Azure o un Sub-Responsabile trasferiscano Dati Personali verso un Paese terzo o un'organizzazione internazionale, tale trasferimento avverrà esclusivamente sulla base di uno dei meccanismi previsti dagli artt. 44 e ss. GDPR, inclusi, ove applicabile:

(a) decisione di adeguatezza della Commissione Europea;

(b) Clausole Contrattuali Standard approvate dalla Commissione Europea con Decisione di esecuzione (UE) 2021/914;

(c) altro meccanismo legittimo previsto dal GDPR.

8.3 Per i Sub-Responsabili stabiliti negli Stati Uniti, Azure verifica, ove pertinente, se il fornitore risulti certificato ai sensi dell'EU-US Data Privacy Framework e se il trattamento oggetto del servizio rientri nell'ambito della certificazione. In assenza di copertura adeguata tramite decisione di adeguatezza, Azure si avvale delle Clausole Contrattuali Standard applicabili e delle eventuali misure supplementari ragionevolmente necessarie.

8.4 Azure mantiene documentazione interna relativa alla valutazione dei trasferimenti verso Paesi terzi, incluse le valutazioni d'impatto sul trasferimento ove richieste o opportune. Su richiesta ragionevole del Titolare, Azure può mettere a disposizione un riepilogo delle valutazioni rilevanti, omettendo informazioni riservate, segreti commerciali, dettagli di sicurezza o informazioni che possano compromettere la sicurezza della Piattaforma.

8.5 Azure non autorizza Sub-Responsabili a effettuare trasferimenti verso Paesi terzi in assenza di un idoneo presupposto di liceità ai sensi del GDPR.

9. AUDIT E VERIFICHE

9.1 Azure mette a disposizione del Titolare le informazioni ragionevolmente necessarie per dimostrare il rispetto degli obblighi previsti dal presente DPA e dall'art. 28 GDPR.

9.2 Il Titolare può richiedere un audit con frequenza non superiore a una volta per anno solare, salvo il caso di Violazione dei Dati Personali confermata o richiesta dell'Autorità di controllo. La richiesta deve essere trasmessa con

preavviso scritto di almeno 30 giorni all'indirizzo team@azureautomotive.it e deve indicare oggetto, finalità e ambito dell'audit.

9.3 L'audit si svolge ordinariamente in forma documentale e remota, mediante esame di documentazione, policy, evidenze tecniche, procedure, report di sicurezza, registri e informazioni ragionevolmente pertinenti. Azure non è tenuta a fornire accesso a segreti commerciali, codice sorgente, informazioni riservate, dati di altri clienti, credenziali, sistemi di produzione o elementi che possano compromettere la sicurezza della Piattaforma.

9.4 Eventuali verifiche ulteriori, incluse ispezioni on-site o verifiche tramite auditor terzo, sono ammesse solo ove ragionevolmente necessarie in relazione a una Violazione dei Dati Personali confermata, a un obbligo di legge o a una richiesta dell'Autorità di controllo, previa definizione scritta di scope, tempi, modalità, obblighi di riservatezza, misure di sicurezza e assenza di interferenza con la continuità dei servizi.

9.5 Gli auditor terzi eventualmente incaricati dal Titolare devono essere indipendenti, qualificati e vincolati da obblighi di riservatezza almeno equivalenti a quelli previsti dal presente DPA. Azure può rifiutare auditor che siano concorrenti diretti o soggetti in conflitto di interessi.

9.6 I costi interni ordinari di gestione di un audit documentale annuale sono a carico di Azure entro limiti ragionevoli. Restano a carico del Titolare i costi dei propri consulenti, auditor terzi, richieste eccedenti, audit ripetuti o attività che richiedano un impegno straordinario non giustificato.

9.7 In alternativa o in aggiunta all'audit documentale, Azure può mettere a disposizione del Titolare, ove disponibili, attestazioni, report di sicurezza, esiti di penetration test, certificazioni, policy o documentazione equivalente rilasciata da terzi o predisposta internamente. L'eventuale indisponibilità di certificazioni volontarie quali ISO 27001 o SOC 2 non costituisce inadempimento, salvo che tali certificazioni siano state espressamente pattuite nel contratto di servizio principale.

10. RESPONSABILITÀ E LIMITAZIONI

10.1 Responsabilità delle Parti

Ciascuna Parte risponde nei confronti dell'altra per l'inadempimento degli obblighi posti dal presente DPA, in conformità all'art. 82 GDPR e alle norme di legge applicabili.

10.2 Limitazione di responsabilità inter partes

Nei limiti massimi consentiti dalla legge applicabile, e fatto salvo quanto previsto al successivo art. 10.3, la responsabilità complessiva di Azure nei confronti del Titolare per danni diretti derivanti da inadempimenti del presente DPA è limitata a un importo pari ai corrispettivi netti effettivamente pagati dal Titolare ad Azure per i servizi della Piattaforma nei 12 mesi precedenti l'evento che ha generato la responsabilità.

La presente limitazione opera esclusivamente nei rapporti interni tra Azure e il Titolare e non limita né esclude i diritti degli Interessati, l'esercizio dei poteri dell'Autorità di controllo, né le responsabilità inderogabili previste dal GDPR, incluso l'art. 82 GDPR.

10.3 Esclusioni dal limite

Il limite di cui all'art. 10.2 non si applica in caso di:

- (a) dolo o colpa grave;
- (b) violazione intenzionale o gravemente negligente delle istruzioni documentate del Titolare;
- (c) trattamento per finalità proprie non autorizzate;
- (d) violazione degli obblighi di riservatezza;
- (e) trasferimenti internazionali effettuati in assenza di idoneo presupposto giuridico;
- (f) obblighi di manleva o regresso non limitabili ai sensi del GDPR o di legge applicabile.

10.4 Esclusione di responsabilità per fatto del Titolare

Azure non risponde per richieste, sanzioni o danni derivanti da:

- (a) configurazione errata della Piattaforma da parte del Titolare;
- (b) uso della Piattaforma in violazione delle istruzioni o del contratto di servizio;
- (c) mancata informativa o mancato consenso degli Interessati gestito dal Titolare;
- (d) immissione di dati che il Titolare non ha titolo di trattare.

11. RESTITUZIONE, ESPORTAZIONE E CANCELLAZIONE DEI DATI

11.1 Cessazione del trattamento attivo

Alla cessazione del contratto di servizio principale, Azure cessa il trattamento attivo dei Dati Personali trattati per conto del Titolare entro 5 giorni lavorativi, salvo quanto necessario per consentire esportazione, restituzione, cancellazione, adempimenti di legge, sicurezza, difesa di diritti o gestione della chiusura del rapporto.

11.2 Periodo di esportazione

Per 90 giorni dalla cessazione, Azure mette a disposizione del Titolare strumenti di esportazione self-service o, ove non disponibili, assistenza ragionevole tramite richiesta scritta a team@azureautomotive.it. L'esportazione riguarda i Dati Personali del Titolare in formato strutturato e ragionevolmente interoperabile, tenuto conto delle funzionalità tecniche disponibili.

11.3 Cancellazione dai sistemi attivi

Decorso il periodo di cui all'art. 11.2, salvo diversa richiesta scritta del Titolare o obbligo di legge, Azure procede alla cancellazione o anonimizzazione irreversibile dei Dati Personali trattati per conto del Titolare dai sistemi applicativi attivi.

11.4 Backup

I Dati Personali eventualmente presenti nei backup sono cancellati secondo i cicli ordinari di rotazione tecnica dei backup e non sono oggetto di ripristino selettivo, salvo necessità di continuità operativa, sicurezza, disaster recovery o obbligo di legge. In caso di ripristino da backup, Azure adotterà misure ragionevoli per evitare il ripristino permanente di dati già cancellati, ove tecnicamente possibile.

11.5 Log e audit trail

I log tecnici, di sicurezza e di audit possono essere conservati per il periodo necessario a garantire sicurezza, tracciabilità, accertamento di illeciti, difesa di diritti e dimostrazione della conformità, secondo le policy di retention applicabili. Tali log sono soggetti a minimizzazione, accesso ristretto e, ove possibile, pseudonimizzazione.

11.6 Dati conservati da Azure come Titolare autonomo

Restano esclusi dalla cancellazione di cui al presente articolo i dati che Azure conserva in qualità di Titolare autonomo per obblighi fiscali, contabili, contrattuali, probatori, compliance, prevenzione abusi, gestione pagamenti, fatturazione o difesa di diritti. Tali dati sono disciplinati dalla Privacy Policy di Azure e non dal presente DPA.

12. MODIFICHE AL DPA

12.1 Modifiche di legge

Modifiche imposte da legge, regolamento o atto vincolante del Garante o di altra autorità competente sono recepite immediatamente, con notifica al Titolare appena possibile.

12.2 Modifiche sostanziali

Azure notifica al Titolare con almeno 30 giorni di preavviso le modifiche sostanziali del presente DPA, incluse modifiche che comportino nuove finalità di trattamento per conto del Titolare, nuove categorie rilevanti di Dati Personali, modifiche significative ai trasferimenti extra-SEE, riduzione sostanziale delle Misure Tecniche e

Organizzative o modifiche rilevanti alla procedura di cancellazione.

Il Titolare può opporsi alla modifica per motivi ragionevoli connessi alla protezione dei Dati Personali. In caso di opposizione, le Parti si confrontano in buona fede per individuare una soluzione ragionevole. In mancanza di soluzione, il Titolare può recedere dal contratto di servizio principale senza penali, con applicazione della procedura di esportazione e cancellazione di cui all'art. 11.

La prosecuzione dell'utilizzo della Piattaforma decorso il termine di preavviso, in assenza di opposizione, costituisce accettazione della modifica. Azure può richiedere re-acceptance tramite checkbox o meccanismo equivalente per modifiche particolarmente rilevanti.

12.3 Modifiche non sostanziali

Modifiche cosmetiche (correzione errori materiali, aggiornamento link, rinumerazione) non richiedono re-acceptance. Sono comunicate tramite changelog versionato pubblicato su https://dealermax.app/legal/dpa.

12.4 Versioning

Ogni versione del DPA è archiviata con numero versione progressivo e data di efficacia. La versione applicabile al rapporto è quella accettata dal Titolare in fase di onboarding o tramite re-acceptance successiva.

13. COMUNICAZIONI

13.1 Comunicazioni al Responsabile

- Email: team@azureautomotive.it
- Telefono: 800 40 40 11
- PEC: azureautomotive@pec.it
- Indirizzo postale: Via della Resistenza 121/A, 20090 Buccinasco (MI)

13.2 Comunicazioni al Titolare

Indirizzi email e PEC del Titolare comunicati in onboarding e mantenuti aggiornati dal Titolare stesso. È onere del Titolare aggiornare tali recapiti tempestivamente.

14. LEGGE APPLICABILE E FORO COMPETENTE

14.1 Legge applicabile

Il presente DPA è regolato dalla legge italiana, fatte salve le norme inderogabili di diritto dell'Unione Europea.

14.2 Foro competente

Per ogni controversia tra le Parti derivante dal presente DPA o connessa allo stesso è competente in via esclusiva il Foro di Milano, fatti salvi i diritti inderogabili degli Interessati, i poteri dell'Autorità di controllo competente e ogni foro inderogabile previsto dalla legge applicabile.

15. LINGUA DEL CONTRATTO

Il presente DPA è redatto in lingua italiana. Eventuali traduzioni in altra lingua sono predisposte esclusivamente per comodità di lettura. In caso di divergenza, prevale la versione italiana.

16. ACCETTAZIONE ELETTRONICA

16.1 Modalità di accettazione

Il presente DPA è accettato dal Titolare mediante spunta di apposito checkbox in fase di onboarding, re-acceptance in piattaforma o altro meccanismo elettronico equivalente predisposto da Azure.

L'accettazione elettronica costituisce accettazione contrattuale del DPA e soddisfa il requisito della forma elettronica dell'atto giuridico previsto dall'art. 28 GDPR. Resta ferma la possibilità per Azure, per clienti enterprise o su richiesta specifica, di utilizzare strumenti di firma elettronica avanzata, qualificata o soluzioni equivalenti.

16.2 Evidenze dell'accettazione

Azure conserva evidenza dell'accettazione mediante registro tecnico contenente almeno:

(a) identificativo del Titolare o dealer_id;

(b) identificativo dell'utente che ha effettuato l'accettazione;

(c) ruolo/autorizzazione dell'utente;

(d) versione del DPA accettata;

(e) timestamp UTC;

(f) indirizzo IP;

(g) user-agent;

(h) hash SHA-256 del testo accettato;

(i) evento applicativo di accettazione o re-acceptance.

16.3 Conservazione delle evidenze

Le evidenze di accettazione sono conservate per la durata del rapporto contrattuale e successivamente per il periodo necessario alla tutela dei diritti di Azure, alla dimostrazione della conformità e alla gestione di eventuali contestazioni, nel rispetto dei principi di minimizzazione e limitazione della conservazione.

16.4 Re-acceptance

In caso di modifiche sostanziali ai sensi dell'art. 12.2, Azure può richiedere al Titolare una nuova accettazione elettronica del DPA aggiornato.

ALLEGATI

ALLEGATO A — Misure Tecniche e Organizzative (TOM) ex art. 32 GDPR

Le misure indicate nel presente Allegato descrivono lo stato delle misure tecniche e organizzative adottate alla data di efficacia del DPA. Eventuali iniziative indicate come pianificate, ove riportate in documentazione separata, non costituiscono obbligazione contrattuale salvo espresso accordo scritto tra le Parti.

A.1 Cifratura

Misura	Stato
TLS 1.3 in-transit su tutti gli endpoint pubblici	**DEPLOYED**
Cifratura at-rest (AES-256-GCM) su token e credenziali OAuth sensibili	**DEPLOYED**
HSTS attivo	**DEPLOYED**

A.2 Controllo accessi

Misura	Stato
RBAC a 6 ruoli (admin / admin_team / dealer / dealer_team / superadmin / garage)	**DEPLOYED**
ACL applicativa centralizzata	**DEPLOYED**
Pseudonimizzazione strutturale (ID interni separati dai dati identificativi)	**DEPLOYED**
2FA sulle dashboard infrastrutturali (database e hosting)	**DEPLOYED**
Credenziali di servizio solo lato backend, mai frontend	**DEPLOYED**
Magic link auth con TTL	**DEPLOYED**
Flusso magic link token-only (nessuna email in URL)	**DEPLOYED**
Controllo accessi applicativo centralizzato (RBAC + ACL per dealer) su tutte le tabelle	**DEPLOYED**
Row-Level Security a livello database sulle tabelle lead di nuova generazione (dealermax_leads, dealermax_lead_messages)	**DEPLOYED**

A.3 Audit log e diritti degli Interessati

Misura	Stato
Audit log strutturato (immutable) sulle operazioni GDPR	**DEPLOYED**
Worker schedulato di retention/cancellazione	**DEPLOYED**
Funzioni di esportazione dati (portabilità)	**DEPLOYED**
Funzioni di cancellazione self-service, con presa in carico manuale per gli Interessati con contratti conclusi	**DEPLOYED**
Audit log su tabelle critiche (utenti, configurazioni, crediti)	**DEPLOYED**

A.4 Backup e continuità

Misura	Stato
Backup automatici periodici del database	**DEPLOYED**
Point-in-time recovery (PITR)	**DEPLOYED**

A.5 Sicurezza dei dati personali

Misura	Stato
Minimizzazione dei dati personali nei log applicativi	**DEPLOYED**
Politica di retention con soft-delete e cancellazione	**DEPLOYED**
Tracciamento consensi versionato (consenso, fonte, versione del testo)	**DEPLOYED**
Cookie banner conforme alle linee guida del Garante	**DEPLOYED**
Privacy Policy e Cookie Policy esposte su tutti i siti	**DEPLOYED**
Disclosure AI Act art. 50 sui contenuti generati	**DEPLOYED**
Firma crittografica dei contenuti (C2PA)	**DEPLOYED**

A.6 Incident response

Misura	Stato
Playbook scritto di incident response	**DEPLOYED**
Notifica della Violazione al Titolare entro 48h dalla conoscenza	CONTRACTUAL
Supporto al Titolare per notifica art. 33-34 GDPR	CONTRACTUAL

A.7 Controllo accessi al database (a livelli)

- Rete: TLS 1.3 obbligatorio, HSTS, restrizione di rete tra compute e database.
- Autenticazione: credenziali di servizio lato backend; accesso applicativo autenticato; nessun accesso a Dati Personali diretto dal frontend.
- Autorizzazione applicativa: ogni accesso a Dati Personali passa per il gateway applicativo con controllo a ruoli (RBAC).
- Controllo accessi: applicativo centralizzato (RBAC + ACL per dealer) su tutte le tabelle; Row-Level Security a livello database attiva sulle tabelle lead di nuova generazione, con estensione incrementale secondo le policy di sicurezza interne.

A.8 Governance dei Sub-Responsabili

Misura	Stato
Lista pubblica Sub-Responsabili versionata	**DEPLOYED (Allegato B)**
Notifica 30 giorni di preavviso per modifiche Sub-Responsabili	CONTRACTUAL
Vincoli contrattuali di protezione dati verso i Sub-Responsabili	CONTRACTUAL

A.9 Pseudonimizzazione e minimizzazione

Misura	Stato
ID interni separati dai dati identificativi	**DEPLOYED**
Dati personali non esposti in URL query string	**DEPLOYED**
Email in forma hash nei log	**DEPLOYED**
Diritti di accesso/cancellazione per lead non registrati	**DEPLOYED**

ALLEGATO B — Sub-Responsabili

Azure mantiene una lista aggiornata dei Sub-Responsabili autorizzati all'indirizzo https://dealermax.app/legal/subprocessors. La lista pubblicata indica, per ciascun Sub-Responsabile, almeno:

(a) denominazione del fornitore;

(b) servizio fornito;

(c) categoria di trattamento;

(d) localizzazione principale del trattamento, ove nota;

(e) eventuale trasferimento extra-SEE;

(f) meccanismo di trasferimento applicabile, ove rilevante.

La versione della lista applicabile al rapporto con il Titolare è quella pubblicata alla data di accettazione del presente DPA, salvo successive modifiche comunicate secondo la procedura prevista dall'art. 4.4.

Azure si avvale esclusivamente di Sub-Responsabili vincolati da accordi, termini di servizio, data processing agreement o altri strumenti contrattuali che impongano obblighi di protezione dei dati personali sostanzialmente

equivalenti a quelli previsti dal presente DPA.

L'elenco nominativo dei Sub-Responsabili — con denominazione, servizio, categorie di dati trattati, localizzazione, eventuale trasferimento extra-SEE e relativo meccanismo — è pubblicato e mantenuto aggiornato sulla pagina https://dealermax.app/legal/subprocessors, che costituisce a tal fine l'unica fonte autoritativa. La pagina distingue inoltre:

- i Sub-Responsabili che trattano Dati Personali per conto del Titolare ai sensi dell'art. 28 GDPR, cui si applica il presente DPA;
- i fornitori di cui Azure si avvale in qualità di Titolare autonomo, che non trattano dati dei clienti finali del Titolare e non rientrano nel presente DPA;
- le fonti dati e le destinazioni di pubblicazione (banche dati tecniche di settore, marketplace e portali su cui il Titolare sceglie di pubblicare i propri annunci), che non sono Sub-Responsabili.

Ogni variazione dell'elenco è comunicata secondo la procedura dell'art. 4.4, lett. (c) e (d).

ALLEGATO C — Categorie di Dati Personali

C.1 Dati identificativi

- Nome
- Cognome
- Ragione sociale (per persone giuridiche)
- Codice fiscale
- Partita IVA

C.2 Dati di contatto

- Indirizzo email (personale e/o aziendale)
- Numero telefono (mobile e/o fisso)
- Indirizzo postale (residenza, domicilio, sede operativa)

C.3 Dati di interazione

- Body messaggi email transactional inbound (canale Postmark)
- Thread conversazionali cliente↔dealer (gdmax_threads, gdmax_messages)
- Allegati e documenti caricati in thread (gdmax_message_attachments, gdmax_thread_documents)
- Numeri WhatsApp (in roadmap DirectMax 1.5)
- Body messaggi WhatsApp (in roadmap DirectMax 1.5)
- Chat AI logs collegati a interessato identificabile (ai_chat_logs, ai_chat_logs_auto, azcore_ai_chat_message)
- Messaggi NLT WhatsApp (nlt_messaggi_whatsapp)

C.4 Dati di interesse commerciale

- Veicoli di interesse / wishlist
- Configurazioni preventivi NLT (garage_nlt_quote_proposals)
- Preventivi assicurazione (ass_preventivi, ass_preventivi_garanzie)
- Follow concessionario (garage_dealer_follows)
- Opt-out marketing (garage_dealer_marketing_opt_out)
- Consensi commerciali e versioning consenso (clienti_consensi, consent_marketing_at)

C.5 Dati tecnici

- Indirizzo IP (in audit log e/o log applicativi)

- User-agent del browser
- Timestamp eventi (login, accept DPA, esercizio diritti)
- Endpoint device push notification (garage_push_subscriptions)

C.6 Dati relativi al veicolo del cliente

- Targa veicolo (in lookup Motornet)
- Telaio veicolo (eventuale)
- Storico ricerche valutazione usato

C.7 Email events

- Bounce, delivery, open, click degli invii Postmark (email_events) collegabili indirettamente all'interessato via email.

C.8 Dati esclusi

- ■ Categorie particolari art. 9 (origine razziale, opinioni politiche, ecc.) — non trattate intenzionalmente.
- ■ Dati relativi a condanne penali e reati art. 10 — non trattati.
- ■ Dati biometrici — non trattati.
- ■ Dati sanitari — non trattati.
- ■ Dati di pagamento del cliente finale (Azure non processa pagamenti del cliente finale del dealer; Stripe processa esclusivamente pagamenti del dealer verso Azure).

ALLEGATO D — Clausole soggette ad approvazione specifica ex art. 1341, comma 2, c.c.

Ai sensi dell'art. 1341, comma 2, del Codice Civile, il Titolare approva specificamente, con separata manifestazione di consenso rispetto all'accettazione del DPA nel suo complesso, le seguenti clausole:

1. Foro competente esclusivo di Milano (art. 14)
2. Limitazione di responsabilità — cap 12 mesi di corrispettivo (art. 10.2)
3. Modifiche unilaterali del DPA con preavviso (art. 12)
4. Limiti al diritto di audit — max 1/anno, documentale, no on-site (art. 9)
5. Recesso e cessazione del trattamento (artt. 2, 11)
6. Obiezione su nuovi Sub-Responsabili con preavviso 30 giorni (art. 4.4)

L'approvazione specifica è raccolta in fase di accettazione elettronica con una seconda spunta dedicata, distinta da quella di accettazione del DPA, e registrata tra le evidenze di cui all'art. 16.2.

FINE DEL DOCUMENTO

Documento finale — versione 1.2 (sostituisce la 1.1 del 2026-07; rispetto alla 1.1 cambiano soltanto l'art. 4.5 lett. (c) e la corrispondente riga dell'Allegato A.3, che descrivono la cancellazione self-service dell'account GarageMAX quando l'Interessato è parte di contratti conclusi). Le misure dichiarate nell'Allegato A riflettono lo stato in produzione alla data di efficacia. Allegati: A (Misure Tecniche e Organizzative), B (Sub-Responsabili), C (Categorie di Dati Personali), D (Clausole ex art. 1341 c.c.).