ACCORDO SUL TRATTAMENTO DEI DATI PERSONALI

ai sensi dell'art. 28 del Regolamento (UE) 2016/679

Versione 1.2 del 17 novembre 2026

Parti

la concessionaria che conclude il contratto per il servizio Piazzale con il modulo d'ordine o con l'iscrizione online, come identificata nell'Ordine (il «**Titolare**»),

e

BJ Consulting di Jacopo Beduini, impresa individuale con sede in Via Cavour 29C, 06016 San Giustino (PG), P. IVA 03565780545, PEC upyourlike@pec.it (il «**Responsabile**»).

Premesso che

a) il Titolare usa il servizio gestionale «Piazzale» (il «**Servizio**») fornito dal Responsabile, in base alle Condizioni generali del Servizio Piazzale e all'Ordine sottoscritto (il «**Contratto**»). Se il Servizio è fornito a titolo gratuito, per esempio nell'ambito del programma «design partner», per «Contratto» si intende l'accordo di collaborazione in essere tra le parti;

b) nel fornire il Servizio il Responsabile tratta, per conto del Titolare, dati personali dei clienti, dei potenziali clienti, dei fornitori e degli altri interessati del Titolare;

c) il presente Accordo stabilisce le condizioni di questi trattamenti, come richiesto dall'art. 28, par. 3, del Regolamento (UE) 2016/679 («**GDPR**»), e del D.Lgs. 30 giugno 2003, n. 196 («**Codice privacy**»);

le parti convengono quanto segue.

Art. 1 — Definizioni

Hanno il significato dell'art. 4 GDPR i termini «dato personale», «trattamento», «titolare», «responsabile», «sub-responsabile» (inteso come «altro responsabile» ai sensi dell'art. 28, par. 2 e 4, GDPR), «interessato» e «violazione dei dati personali».

Dati sono i dati personali trattati dal Responsabile per conto del Titolare nell'ambito del Servizio, descritti nell'**Allegato 1**.

Art. 2 — Oggetto e istruzioni

2.1. Il Responsabile tratta i Dati solo per fornire il Servizio e soltanto secondo le **istruzioni documentate** del Titolare. Le istruzioni sono contenute:

- nel presente Accordo e nel Contratto;
- nelle impostazioni e nelle funzioni del Servizio usate dal Titolare e dai suoi utenti;

- in eventuali istruzioni scritte successive, compatibili con il Servizio.

2.2. **Il Titolare fin d'ora dà istruzione al Responsabile di:**
a) conservare i Dati sui sistemi del Servizio, elaborarli e renderli disponibili agli utenti del Titolare secondo i rispettivi ruoli;
b) ricevere all'indirizzo dedicato del Titolare le email che il Titolare vi inoltra o che i portali di annunci vi inviano; farle leggere da un programma automatico, anche con un modello di intelligenza artificiale, attraverso i sub-responsabili indicati per questo servizio nell'Allegato 3 e secondo l'art. 7.5, per riconoscere le richieste ed estrarne i dati; registrare le richieste nel Servizio; scartare le altre email; cancellarne il testo nei tempi dell'Allegato 1;
c) inviare le email di servizio previste dal Servizio (avvisi, inviti agli utenti, recupero della password);
d) eseguire copie di sicurezza e verifiche di ripristino;
e) importare i dati che il Titolare consegna per il caricamento iniziale;
f) accedere ai Dati per l'assistenza, con le modalità dell'art. 6;
g) cancellare i Dati alla cessazione del Servizio, secondo l'art. 11;
h) se il Titolare le attiva, svolgere le funzioni di intelligenza artificiale descritte nell'**Allegato 4**, con i sub-responsabili indicati per queste funzioni nell'Allegato 3, secondo gli artt. 7.5 e 7.6. In ogni funzione il modello propone dati, testi, immagini o stime e un utente del Titolare li controlla prima di salvarli, usarli, inviarli o pubblicarli. Nessuna funzione prende decisioni sulle persone né valuta clienti o utenti;
i) inviare documenti e dati ai destinatari che un utente del Titolare sceglie, quando lo comanda (per esempio il pacchetto della pratica all'agenzia di consulenza automobilistica).

2.3. Il Responsabile **informa immediatamente** il Titolare se ritiene che un'istruzione violi il GDPR o altre norme sulla protezione dei dati (art. 28, par. 3, ultimo periodo, GDPR).

2.4. Il Responsabile non tratta i Dati per finalità proprie. Può elaborare statistiche aggregate e anonime sull'uso del Servizio, che non consentono di identificare alcuna persona fisica.

Art. 3 — Obblighi del Titolare

Il Titolare garantisce che:
a) i Dati sono raccolti e trattati lecitamente, con una base giuridica adeguata e dopo aver fornito agli interessati l'informativa (artt. 13 e 14 GDPR);
b) non inserisce nel Servizio categorie particolari di dati (art. 9 GDPR), dati relativi a condanne penali e reati (art. 10 GDPR), né copie o scansioni di documenti d'identità, salvo che una funzione del Servizio non sia espressamente destinata a riceverle;
c) gestisce correttamente gli account dei propri utenti e ne revoca tempestivamente gli accessi.

Art. 4 — Persone autorizzate e riservatezza

4.1. I Dati sono trattati solo da persone autorizzate dal Responsabile e istruite ai sensi dell'art. 29 GDPR e dell'art. 2-quaterdecies del Codice privacy. Queste persone sono vincolate alla riservatezza per contratto o per obbligo di legge.

4.2. Il Responsabile autorizza per iscritto ciascuna persona, le dà istruzioni sul trattamento e tiene l'elenco aggiornato delle persone autorizzate.

4.3. **Strumenti di intelligenza artificiale.** Il Responsabile non comunica i Dati a servizi di intelligenza artificiale di terzi, salvo i sub-responsabili dell'Allegato 3. Gli assistenti di intelligenza artificiale usati per lo sviluppo e l'assistenza possono vedere Dati solo in modo occasionale, quando serve a risolvere un malfunzionamento, e nella misura minima necessaria.

Art. 5 — Sicurezza

5.1. Il Responsabile adotta le misure tecniche e organizzative adeguate al rischio richieste dall'art. 32 GDPR, descritte nell'**Allegato 2**. Può aggiornarle nel tempo, senza ridurre il livello complessivo di protezione.

5.2. Il Servizio isola i Dati del Titolare da quelli degli altri clienti del Responsabile. L'isolamento è applicato dal database ed è verificato con controlli automatici a ogni modifica del software.

Art. 6 — Accesso dell'assistenza

6.1. Il Titolare autorizza le persone di cui all'art. 4 ad accedere al Servizio con l'identità di un suo utente, alle condizioni dell'art. 9.3 delle Condizioni generali. In sintesi:

- solo per l'assistenza, il caricamento iniziale e la verifica del funzionamento;
- solo dalla rete privata del Responsabile;
- con il motivo registrato ogni volta;
- con chiusura automatica dopo al massimo un'ora.

6.2. Le modifiche fatte durante l'accesso risultano nello storico a nome dell'utente con cui l'assistenza è entrata. Il Responsabile tiene un **registro completo** degli accessi e delle modifiche e ne consegna copia al Titolare entro **5 giorni lavorativi** dalla richiesta. Il registro è conservato per la durata del Contratto e per i 10 anni successivi.

6.3. Il Titolare può chiedere per iscritto che ogni accesso sia preceduto da una sua autorizzazione specifica, salvo i casi urgenti di sicurezza, che il Responsabile gli comunica entro 24 ore.

6.4. Fuori da questi casi, nessuna persona del Responsabile consulta i Dati del Titolare. Gli strumenti di amministrazione diretta del database di produzione restano spenti e si accendono solo per un intervento, che viene registrato.

Art. 7 — Sub-responsabili

7.1. Il Titolare dà al Responsabile un'**autorizzazione scritta generale** a ricorrere ai sub-responsabili elencati nell'**Allegato 3** (art. 28, par. 2, GDPR).

7.2. Salvo l'art. 7.6, il Responsabile comunica per email al Titolare ogni aggiunta o sostituzione di un sub-responsabile almeno **30 giorni** prima, indicando nome, sede, servizio e luogo del trattamento. Entro questo termine il Titolare può opporsi per motivi ragionevoli legati alla protezione dei dati. Se le parti non trovano una soluzione, il Titolare può recedere dal Contratto senza penale e con il rimborso dei corrispettivi pagati per il periodo successivo.

7.3. Il Responsabile impone a ciascun sub-responsabile, per contratto, obblighi di protezione dei dati sostanzialmente equivalenti a quelli del presente Accordo. Il Responsabile risponde verso il Titolare dell'adempimento dei sub-responsabili (art. 28, par. 4, GDPR).

7.4. **Non sono sub-responsabili:**

- il prestatore dei servizi di pagamento Stripe, che tratta i dati di pagamento del Titolare come titolare autonomo;
- i servizi del Responsabile che non trattano i Dati, come il monitoraggio della raggiungibilità del Servizio, il gestore delle password del Responsabile e il servizio di conservazione del codice sorgente.

7.5. **Modelli Claude: due modalità.** Per la lettura automatica dell'art. 2.2, lett. b), e per le funzioni dell'art. 2.2, lett. h), svolte con i modelli Claude di Anthropic, il Responsabile usa, in alternativa, una delle due

modalità indicate nell'Allegato 3:
a) **diretta**: il modello è fornito da Amazon Web Services EMEA SARL per conto del Responsabile;
b) **con intermediario**: il Responsabile si avvale di Cortecs GmbH, che a sua volta si avvale, per questo servizio, solo di Amazon Web Services EMEA SARL e di OVH SAS.

Il Titolare autorizza entrambe le modalità. Il passaggio dall'una all'altra non è un'aggiunta né una sostituzione di sub-responsabili ai sensi dell'art. 7.2. Il Responsabile indica la modalità in uso nella pagina del Servizio dedicata alle richieste dai portali e la aggiorna il giorno stesso del passaggio. Nella modalità b) il Responsabile si assicura che Cortecs GmbH imponga ai propri sub-responsabili obblighi equivalenti e non usi altri fornitori per i Dati.

7.6. **Fornitori nuovi di una funzione facoltativa.** Se una funzione dell'Allegato 4 richiede un sub-responsabile non indicato nell'Allegato 3, il Responsabile ne indica nella pagina di attivazione nome, sede, servizio e luogo del trattamento. Attivando la funzione, il Titolare lo autorizza in modo specifico (art. 28, par. 2, GDPR). Finché il Titolare non attiva la funzione, quel sub-responsabile non tratta Dati del Titolare. Il Responsabile lo aggiunge all'Allegato 3 nella versione successiva dell'Accordo. Per i Titolari che hanno già attivato la funzione, ogni aggiunta o sostituzione successiva segue l'art. 7.2.

Art. 8 — Luogo del trattamento e trasferimenti

8.1. I Dati del Servizio (database, foto, copie di sicurezza, email ricevute all'indirizzo dedicato e loro lettura automatica) sono conservati e trattati **nell'Unione europea**, nei data center indicati nell'Allegato 3. Fanno eccezione:

- la casella email dell'assistenza, che il Titolare usa per le proprie segnalazioni e per l'invio dei dati del caricamento iniziale, gestita da Google;
- gli assistenti di intelligenza artificiale dell'art. 4.3, che possono vedere Dati negli Stati Uniti in modo occasionale.

Per entrambi valgono le garanzie indicate nell'Allegato 3.

8.2. Il Responsabile non trasferisce i Dati verso Paesi terzi o organizzazioni internazionali, salvo:
a) verso Paesi oggetto di una decisione di adeguatezza della Commissione europea (art. 45 GDPR), nei casi indicati nell'Allegato 3;
b) su istruzione scritta del Titolare;
c) se lo impone il diritto dell'Unione o dello Stato membro. In tal caso il Responsabile informa prima il Titolare, salvo che la legge lo vieti;
d) verso gli Stati Uniti, per i soli assistenti di intelligenza artificiale dell'art. 4.3, con le clausole contrattuali tipo adottate dalla Commissione europea (art. 46, par. 2, lett. c), GDPR; Decisione di esecuzione (UE) 2021/914).

8.3. Se un'autorità di un Paese terzo chiede l'accesso ai Dati, il Responsabile:

- informa senza ritardo il Titolare, salvo che sia vietato;
- contesta la richiesta se non è fondata su un accordo internazionale o su una norma applicabile dell'Unione;
- comunica solo i Dati minimi necessari.

Art. 9 — Assistenza al Titolare

9.1. Tenendo conto della natura del trattamento, il Responsabile assiste il Titolare con misure tecniche e organizzative adeguate per dare seguito alle richieste di esercizio dei diritti degli interessati (artt. 15-22

GDPR). Il Servizio consente al Titolare di consultare, correggere, esportare e cancellare i dati degli interessati.

Se il Responsabile riceve direttamente una richiesta di un interessato:

- la inoltra al Titolare entro **3 giorni lavorativi**;
- non risponde nel merito senza istruzioni.

9.2. Il Responsabile assiste il Titolare, fornendo le informazioni in suo possesso, nel garantire il rispetto degli obblighi:

- di sicurezza (art. 32 GDPR);
- di notifica e comunicazione delle violazioni (artt. 33 e 34 GDPR);
- di valutazione d'impatto e consultazione preventiva (artt. 35 e 36 GDPR).

9.3. L'assistenza ordinaria è gratuita. Per attività straordinarie su richiesta del Titolare, non dovute a un inadempimento del Responsabile, le parti concordano un compenso prima di iniziare.

Art. 10 — Violazioni dei dati personali

10.1. Il Responsabile informa il Titolare **senza ingiustificato ritardo** e comunque **entro 24 ore** da quando è venuto a conoscenza di una violazione dei dati personali che riguarda i Dati (art. 33, par. 2, GDPR).

10.2. La comunicazione è inviata alla PEC e all'email del titolare indicate nell'Ordine e, se possibile, anticipata per telefono. Contiene, nella misura in cui sono disponibili, le informazioni dell'art. 33, par. 3, GDPR:

- natura della violazione;
- categorie e numero approssimativo di interessati e di registrazioni;
- probabili conseguenze;
- misure adottate o proposte;
- un contatto.

Le informazioni non ancora disponibili sono fornite in fasi successive, senza ulteriore ritardo.

10.3. Il Responsabile adotta subito le misure per contenere la violazione e attenuarne gli effetti, e documenta i fatti. La notifica al Garante e la comunicazione agli interessati spettano al Titolare. Il Responsabile non le fa in nome del Titolare senza sua istruzione.

Art. 11 — Cessazione: restituzione e cancellazione

11.1. Alla cessazione del Contratto per qualunque causa, i Dati restano consultabili ed esportabili dal Titolare:

- per **30 giorni** in sola lettura;
- per ulteriori **60 giorni** con la sola funzione di esportazione.

Su richiesta, il Responsabile consegna gratuitamente i Dati in formato Excel entro 5 giorni lavorativi (art. 28, par. 3, lett. g), GDPR).

11.2. Trascorsi i 90 giorni, o prima su richiesta scritta del Titolare, il Responsabile **cancella** i Dati dai sistemi del Servizio, previo avviso di 7 giorni. I Dati presenti nelle copie di sicurezza sono cancellati alla scadenza del ciclo di conservazione delle copie, comunque entro **45 giorni** dalla cancellazione. Fino ad allora restano protetti e non sono usati se non per ripristini.

11.3. Su richiesta il Responsabile conferma per iscritto l'avvenuta cancellazione. Resta salvo l'obbligo di conservazione previsto dal diritto dell'Unione o dello Stato membro.

Art. 12 — Documentazione e verifiche

12.1. Il Responsabile mette a disposizione del Titolare le informazioni necessarie a dimostrare il rispetto dell'art. 28 GDPR (art. 28, par. 3, lett. h), GDPR), comprese la descrizione aggiornata delle misure di sicurezza e l'elenco dei sub-responsabili.

12.2. Il Titolare, direttamente o tramite un revisore vincolato alla riservatezza e non concorrente del Responsabile, può svolgere verifiche, anche presso il Responsabile:

- con preavviso scritto di almeno **30 giorni**;
- non più di **una volta l'anno**, salvo dopo una violazione dei dati o su richiesta di un'autorità;
- a proprie spese;
- senza accedere ai dati di altri clienti né compromettere la sicurezza del Servizio.

12.3. Il Responsabile tiene il registro delle attività di trattamento svolte per conto del Titolare (art. 30, par. 2, GDPR) e collabora con l'autorità di controllo (art. 31 GDPR).

Art. 13 — Responsabilità

Le parti rispondono verso gli interessati e verso le autorità secondo gli artt. 82 e 83 GDPR. Nei rapporti tra le parti si applica l'art. 15 delle Condizioni generali, nei limiti in cui la legge lo consente.

Art. 14 — Durata e disposizioni finali

14.1. Il presente Accordo ha la stessa durata del Contratto. Gli obblighi di riservatezza, cancellazione e assistenza continuano finché il Responsabile tratta i Dati.

14.2. Per quanto riguarda la protezione dei dati personali, il presente Accordo prevale sul Contratto.

14.3. Il presente Accordo è regolato dalla legge italiana. Il foro competente è quello previsto dal Contratto.

14.4. Il presente Accordo è concluso in forma scritta, anche elettronica (art. 28, par. 9, GDPR):

- con la firma dell'Ordine, che lo richiama;
- con la sua accettazione nel percorso di iscrizione online;
- oppure con la firma delle parti qui sotto.

ALLEGATO 1 — Descrizione del trattamento

Voce	Descrizione
Natura del trattamento	Raccolta tramite inserimento, importazione e ricezione di email; lettura automatica delle email ricevute all'indirizzo dedicato, anche con un modello di intelligenza artificiale, per estrarne i dati delle richieste; lettura automatica dei documenti caricati e preparazione di testi, immagini e stime proposti agli utenti, nelle funzioni dell'Allegato 4 attivate dal Titolare; trasmissione di documenti ai destinatari scelti dal Titolare; registrazione; organizzazione; conservazione; consultazione; elaborazione (calcoli, composizione di documenti e registri); estrazione ed esportazione; copia di sicurezza; cancellazione

Voce	Descrizione
Finalità	Fornire al Titolare il Servizio di gestione della concessionaria: stock dei veicoli, costi e margini, anagrafiche di clienti e fornitori, richieste dei potenziali clienti, trattative, permute, documenti di vendita, registri, calendario
Categorie di interessati	Clienti e potenziali clienti del Titolare (acquirenti, cointestatari, cedenti di permute); fornitori persone fisiche e referenti dei fornitori; persone che contattano il Titolare tramite i portali di annunci o il suo sito; mittenti e altre persone citate nelle email inoltrate per errore all'indirizzo dedicato; intestatari dei veicoli e altre persone indicate nei documenti caricati; persone riprese per caso nelle foto dei veicoli; utenti del Servizio del Titolare (titolare, back office, venditori) per le operazioni registrate nello storico
Categorie di dati	Dati anagrafici (nome, cognome, luogo e data di nascita, codice fiscale, residenza); estremi del documento d'identità (tipo, numero, rilascio, scadenza); copie o scansioni dei documenti d'identità **solo nel fascicolo digitale**, se il Titolare lo attiva (Allegato 4); contatti (telefono, email); IBAN; dati dei veicoli collegati alla persona (targa, telaio, intestazione); dati economici delle trattative (prezzi, permute, caparre, finanziamenti, garanzie); contenuto delle email ricevute all'indirizzo dedicato, comprese quelle inoltrate per errore, trattate solo per riconoscerle e scartarle; note ed eventi di calendario; foto dei veicoli, che possono ritrarre targhe e persone riprese per caso; documenti caricati dagli utenti (carte di circolazione e documenti unici, certificati di proprietà, DDT, fatture, contratti, documenti dei finanziamenti); storico delle operazioni con l'utente che le ha eseguite
Categorie particolari e dati giudiziari	Nessuna. Il Titolare si impegna a non inserirne (art. 3, lett. b)
Durata	Per la durata del Contratto e fino alla cancellazione dell'art. 11
Email ricevute all'indirizzo dedicato	Il testo si cancella appena il Servizio l'ha letto. Le email che il Servizio non riesce a leggere restano, con il testo, finché un utente del Titolare le esamina, al massimo 30 giorni. Del testo restano mittente, oggetto e data: con la richiesta, per le email diventate richieste; 7 giorni, per quelle scartate; 30 giorni, per quelle scadute senza esame. Il fornitore della posta conserva le email per 1 giorno. Nelle copie di sicurezza il testo resta fino a 45 giorni ed è usato solo per i ripristini. Dalle richieste perse senza trattativa i dati personali si tolgono 24 mesi dopo l'ultimo contatto
Documenti caricati	Nella lettura dei documenti senza fascicolo il file si cancella appena letto e non entra nelle copie di sicurezza. Nel fascicolo digitale i file restano per i tempi scelti dal Titolare per tipo di documento, e comunque non oltre la cancellazione dell'art. 11. Le copie dei documenti d'identità si cancellano da sole 12 mesi dopo la consegna dell'auto o la chiusura della trattativa a cui si riferiscono, salvo un termine diverso scelto dal Titolare. Nelle copie di sicurezza i file cancellati restano fino a 45 giorni, usati solo per i ripristini
Luogo	Unione europea (Germania, Francia, Paesi Bassi e, per la lettura delle email, regioni dell'Unione europea di Amazon Web Services e, nella modalità con intermediario, server in Francia). Per la casella email dell'assistenza (Google) e per gli assistenti di intelligenza artificiale dell'art. 4.3 (Anthropic): possibile trattamento negli Stati Uniti. Si veda l'Allegato 3

ALLEGATO 2 — Misure tecniche e organizzative (art. 32 GDPR)

Infrastruttura e accessi amministrativi

- Server dedicati al Responsabile, ospitati in data center nell'Unione europea (Germania). Il database di produzione si trova su un server separato, collegato solo alla rete privata e senza porte aperte verso internet.
- Amministrazione di server, database e pannelli **solo attraverso una VPN** (WireGuard) con chiavi personali. Accesso SSH solo con chiave, firewall attivo, aggiornamenti di sicurezza automatici del sistema operativo.

- Strumenti di amministrazione diretta del database di produzione spenti per impostazione; accesi solo per un intervento, che viene registrato.
- Segreti (password, chiavi, chiave di cifratura dei backup) custoditi in un gestore di password con autenticazione a due fattori, mai nel codice sorgente.

Isolamento e controllo degli accessi applicativi

- Ogni concessionaria è isolata a livello di database (Row Level Security). Controlli automatici di sicurezza tra concessionarie vengono eseguiti a ogni modifica del software.
- Ruoli e permessi per utente: il venditore non vede costi e margini, né a schermo né nelle esportazioni.
- Password conservate solo in forma cifrata con funzione di hash. Sessioni valide solo sull'indirizzo della singola concessionaria.
- Comunicazioni cifrate in transito (HTTPS/TLS) su tutti gli indirizzi del Servizio.
- Storico delle modifiche (audit log) su prezzi, costi, stati, registri e documenti.
- Accesso dell'assistenza tracciato: motivo obbligatorio, scadenza dopo un'ora, registro scaricabile (art. 6).
- Email ricevute all'indirizzo dedicato: le email scartate e quelle non lette in automatico con un mittente che non è un portale noto né il sito del Titolare sono visibili solo al titolare e al back office, non ai venditori. Se in un giorno le email scartate sono più di 10, il titolare riceve l'avviso di controllare la regola di inoltro.
- Copie dei documenti d'identità nel fascicolo digitale: in uno spazio separato; visibili solo al titolare e al back office (gli altri utenti possono caricarle ma non riaprirle); aperte con collegamenti che scadono dopo pochi minuti; ogni apertura è registrata con utente, data e ora.

Minimizzazione

- Il Servizio non conserva i PDF dei documenti generati: li ricompone dai dati. Conserva copie dei documenti d'identità solo nel fascicolo digitale, se il Titolare lo attiva, con le misure indicate sopra.
- Dalle email ricevute all'indirizzo dedicato si salvano solo i dati della richiesta (nome, cognome, telefono, email, provenienza, auto, messaggio del cliente, metodo di contatto preferito). Gli altri dati aggiunti dai portali non si salvano. Il testo si cancella nei tempi dell'Allegato 1.
- La lettura automatica avviene senza registrazione delle chiamate e dei testi presso i sub-responsabili che vi partecipano. Nessuno di loro usa i testi per addestrare i modelli. Nella modalità con intermediario, Cortecs GmbH tratta i testi solo in memoria, li cancella a fine richiesta ed è impostata per usare solo Amazon Web Services EMEA SARL, nell'Unione europea, senza altri fornitori di riserva.
- I modelli ricevono solo i dati che servono alla funzione (Allegato 4). Il fornitore del listino per la stima della permuta riceve la sola targa.
- Il testo delle email e dei documenti è trattato come contenuto da leggere, mai come istruzione: il modello non compie azioni nel Servizio e la sua risposta compila solo i campi previsti, che un utente controlla.

Disponibilità e ripristino

- Backup continuo del database (pgBackRest) cifrato, su storage a oggetti nell'UE (Germania).
- Seconda copia presso un altro fornitore (Francia), protetta contro la cancellazione per 30 giorni (blocco degli oggetti).
- Copia notturna delle foto presso il secondo fornitore.
- Prova automatica settimanale di ripristino completo su un server temporaneo, con avviso in caso di esito negativo.

- Monitoraggio esterno della raggiungibilità del Servizio e controllo dei backup con avvisi automatici.

Organizzazione

- Accesso ai Dati solo per le persone autorizzate per iscritto (art. 4), istruite e vincolate alla riservatezza.
- Casella email dell'assistenza con autenticazione a due fattori. I file ricevuti per il caricamento iniziale si cancellano entro 30 giorni dal caricamento.
- Dati dei clienti mai copiati in ambienti di sviluppo o di test, nel codice sorgente o in strumenti di intelligenza artificiale. Fanno eccezione: la lettura delle email e le funzioni dell'art. 2.2, lett. b) e h), con i sub-responsabili dell'Allegato 3; la visione occasionale da parte degli assistenti di intelligenza artificiale, nei limiti dell'art. 4.3, con un account commerciale in cui il fornitore non usa i contenuti per addestrare i modelli; gli esempi di email, documenti dei veicoli, fogli di calcolo e foto resi anonimi su istruzione scritta del Titolare prima di entrare negli ambienti di sviluppo. I documenti d'identità e le tessere sanitarie non si usano mai come esempi.
- Procedura scritta di gestione delle violazioni dei dati, con registro delle violazioni.
- Cancellazione documentata dei dati alla cessazione (art. 11).

ALLEGATO 3 — Sub-responsabili autorizzati

Sub-responsabile	Sede	Servizio	Luogo dei Dati	Garanzie
Hetzner Online GmbH	Industriestr. 25, 91710 Gunzenhausen, Germania	Server, database, storage delle foto e prima copia dei backup	Germania (data center di Norimberga e Falkenstein)	Accordo ex art. 28 GDPR del fornitore
Scaleway SAS	8 rue de la Ville l'Évêque, 75008 Parigi, Francia	Seconda copia cifrata dei backup e delle foto	Francia (regione di Parigi)	Accordo ex art. 28 GDPR del fornitore
AhaSend B.V.	Willem Fenengastraat 16, 1096 BN Amsterdam, Paesi Bassi	Ricezione delle email all'indirizzo dedicato, conservate per 1 giorno; invio delle email di servizio e dei documenti inviati su comando degli utenti (art. 2.2, lett. i))	Unione europea (il fornitore dichiara l'ospitalità in Europa senza indicare il Paese del data center)	Accordo ex art. 28 GDPR del fornitore

Sub-responsabile	Sede	Servizio	Luogo dei Dati	Garanzie
Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy, L-1855 Lussemburgo	Lettura automatica delle email e funzioni di intelligenza artificiale dell'Allegato 4, con i modelli del servizio Amazon Bedrock (modelli Claude di Anthropic e, per le immagini, altri modelli dello stesso servizio), per conto del Responsabile (modalità diretta) o, per i modelli Claude, come sub-responsabile di Cortecs GmbH (modalità con intermediario), secondo l'art. 7.5. Si usano solo modelli per i quali il fornitore non conserva i testi e le immagini, non li usa per addestrare i modelli e non li rende accessibili ai fornitori dei modelli	Unione europea (solo regioni di Amazon Web Services negli Stati membri dell'Unione)	Accordo ex art. 28 GDPR del fornitore (AWS GDPR Data Processing Addendum), concluso con il Responsabile o con Cortecs GmbH. Per l'eventuale accesso dagli Stati Uniti: decisione di adeguatezza UE-USA (Decisione di esecuzione (UE) 2023/1795, Data Privacy Framework), art. 45 GDPR
Cortecs GmbH	Althanstraße 4, 1090 Vienna, Austria	Solo nella modalità con intermediario (art. 7.5): riceve dal Servizio il testo delle email o i contenuti delle altre funzioni dell'Allegato 4, li passa al modello Claude presso Amazon Web Services EMEA SARL e restituisce i dati letti. Tratta i testi solo in memoria e li cancella a fine richiesta; non li usa per addestrare modelli. Per questo servizio si avvale solo di Amazon Web Services EMEA SARL (riga sopra) e di **OVH SAS**, 2 rue Kellermann, 59100 Roubaix, Francia, che ospita il servizio di instradamento	Unione europea (Francia, server di OVH; il modello nelle regioni dell'Unione europea di Amazon Web Services)	Accordo ex art. 28 GDPR del fornitore (Data Processing Agreement di Cortecs), che impone gli stessi obblighi ai suoi sub-responsabili
Google Cloud EMEA Limited (servizio Google Workspace)	70 Sir John Rogerson's Quay, Dublino 2, Irlanda	Casella email dell'assistenza (info@piazzale.app), che può ricevere Dati nelle segnalazioni del Titolare e nei file per il caricamento iniziale	Unione europea e Stati Uniti (data center del gruppo Google)	Cloud Data Processing Addendum di Google (art. 28 GDPR). Trasferimenti verso gli Stati Uniti: decisione di adeguatezza UE-USA (Decisione di esecuzione (UE) 2023/1795, Data Privacy Framework, a cui Google LLC aderisce) e clausole contrattuali standard (Decisione di esecuzione (UE) 2021/914), artt. 45 e 46 GDPR

Sub-responsabile	Sede	Servizio	Luogo dei Dati	Garanzie
Anthropic Ireland, Limited e la capogruppo **Anthropic, PBC**	6th Floor, South Bank House, Barrow Street, Dublino 4, D04 TR29, Irlanda; 548 Market St, PMB 90375, San Francisco, CA 94104, Stati Uniti	Assistenti di intelligenza artificiale (Claude) usati per lo sviluppo del software e per l'assistenza tecnica. Possono vedere Dati solo in modo occasionale, quando serve a risolvere un malfunzionamento, e nella misura minima necessaria (art. 4.3). Il fornitore non usa i contenuti per addestrare i modelli	Stati Uniti	Data Processing Addendum di Anthropic, parte dei suoi termini commerciali (art. 28 GDPR). Trasferimento verso gli Stati Uniti: clausole contrattuali tipo (Decisione di esecuzione (UE) 2021/914; art. 46, par. 2, lett. c), GDPR), con la valutazione del trasferimento del Responsabile

ALLEGATO 4 — Funzioni di intelligenza artificiale

Ogni funzione parte solo se il Titolare la attiva e si ferma quando la disattiva (art. 2.2, lett. h)). In ogni funzione il modello propone e un utente del Titolare controlla prima di salvare, usare, inviare o pubblicare. Nessuna funzione prende decisioni sulle persone, assegna punteggi o valuta clienti o utenti.

Funzione	Che cosa fa	Dati che il modello riceve	Che cosa resta
1. Lettura delle richieste	Riconosce le richieste nelle email ricevute all'indirizzo dedicato e ne estrae i dati (art. 2.2, lett. b))	Il testo delle email	Allegato 1, riga «Email ricevute all'indirizzo dedicato»
2. Lettura dei documenti	Da una foto o da un PDF compila il modulo della pagina in cui l'utente si trova: anagrafica, scheda dell'auto, DDT ricevuto, fattura d'acquisto, finanziamento e simili	Il documento caricato: carta di circolazione o documento unico, certificato di proprietà, documento d'identità, tessera sanitaria (per il solo codice fiscale), DDT, fattura, contratto, documenti della finanziaria	Solo i campi che l'utente salva. Il file non si conserva: è trattato in memoria, si cancella a fine lettura e non entra nelle copie di sicurezza
3. Fascicolo digitale	Conserva i file caricati, collegati al veicolo, alla trattativa, all'anagrafica o al DDT; li legge come la funzione 2	Come la funzione 2	I file, nei tempi dell'Allegato 1, riga «Documenti caricati»
4. Testi	Propone il testo degli annunci e le bozze di risposta ai clienti, anche tradotte; l'utente le corregge e le invia lui	Dati e foto dell'auto; per le risposte, la richiesta del cliente	Il testo, se l'utente lo salva
5. Foto delle auto	Copre targhe e volti, migliora la luce, sostituisce lo sfondo con uno neutro. Non modifica l'auto	Le foto dell'auto	La foto modificata, accanto all'originale

Funzione	Che cosa fa	Dati che il modello riceve	Che cosa resta
6. Stima della permuta	Propone un prezzo d'acquisto dell'auto del cliente, con i dati di un listino e le foto	Dati e foto dell'auto; la targa, al solo fornitore del listino. Mai il nome del cliente	La stima, se l'utente la salva
7. Importazione dei fogli	Riconosce le colonne di un foglio di calcolo da importare	Le intestazioni e alcune righe del foglio	Niente oltre all'importazione che l'utente conferma
8. Assistente della guida	Risponde alle domande sull'uso del Servizio con le pagine della guida	La domanda dell'utente. Non riceve i Dati del Titolare	Niente oltre alla risposta mostrata
9. Riassunti del Cruscotto	Commenta l'andamento della concessionaria	Numeri aggregati della concessionaria, mai riferiti a un singolo utente o cliente	Niente oltre al riassunto mostrato