ACCORDO DI PROTEZIONE DEI DATI PERSONALI (DPA) PER I SERVIZI VDO FLEET (ALLEGATO E)

Il presente DPA stabilisce gli obblighi contrattuali delle PARTI con riferimento alla protezione dei dati che risulta dal trattamento dei dati personali collegati al contratto stipulato dal Cliente per l'erogazione dei Servizi VDO FLEET. Il presente DPA è stilato sulla base delle clausole contrattuali tipo stabilite dalla Commissione europea in conformità alla Decisione di esecuzione (UE) 2021/915.

Il Cliente, in qualità di "titolare del trattamento" e Continental Automotive Trading Italia S.r.l., in qualità di "responsabile del trattamento", stipulano quanto segue:

SEZIONE I

CLAUSOLA 1
Finalità e ambito di applicazione

a) Scopo delle presenti clausole contrattuali tipo (di seguito "clausole") è garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

b) Il(i) titolare(i) del trattamento e il(i) responsabile(i) del trattamento hanno accettato le presenti clausole al fine di garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del Regolamento (UE) 2016/679 e/o dell'articolo 29, paragrafi 3 e 4, del Regolamento (UE) 2018/1725.

c) Le presenti clausole si applicano al trattamento dei dati personali come specificato all'Allegato I.

d) Gli allegati da I a III costituiscono parte integrante delle clausole.

e) Le presenti clausole lasciano impregiudicati gli obblighi cui è soggetto il titolare del trattamento a norma del Regolamento (UE) 2016/679 e/o del Regolamento (UE) 2018/1725.

f) Le presenti clausole non garantiscono, di per sé, il rispetto degli obblighi connessi ai trasferimenti internazionali conformemente al Capo V del Regolamento (UE) 2016/679 e/o del Regolamento (UE) 2018/1725.

CLAUSOLA 2
Invariabilità delle clausole

a) Le Parti si impegnano a non modificare le clausole se non per aggiungere o aggiornare informazioni negli Allegati.

b) Ciò non impedisce alle Parti di includere le clausole contrattuali tipo stabilite nelle presenti clausole in un contratto più ampio o di aggiungere altre clausole o garanzie supplementari, purché queste non contraddicano, direttamente o indirettamente, le presenti clausole o ledano i diritti o le libertà fondamentali degli interessati.

CLAUSOLA 3
Interpretazione

a) Quando le presenti clausole utilizzano i termini definiti, rispettivamente, nel Regolamento (UE) 2016/679 o nel Regolamento (UE) 2018/1725, tali termini hanno lo stesso significato di cui al regolamento interessato.

b) Le presenti clausole vanno lette e interpretate alla luce delle disposizioni del Regolamento (UE) 2016/679 o del Regolamento (UE) 2018/1725, rispettivamente.

c) Le presenti clausole non devono essere interpretate in un senso che non sia conforme ai diritti e agli obblighi previsti dal Regolamento (UE) 2016/679 e/o dal Regolamento (UE) 2018/1725, o che pregiudichi i diritti o le libertà fondamentali dei soggetti interessati al trattamento.

CLAUSOLA 4
Gerarchia / Ordine di precedenza

In caso di contraddizione tra le presenti clausole e le disposizioni di accordi correlati, vigenti tra le Parti al momento dell'accettazione delle presenti clausole, o conclusi successivamente, prevalgono le presenti clausole.

CLAUSOLA 5
Clausola di adesione successiva

a) Qualunque entità che non sia Parte delle presenti clausole può, con l'accordo di tutte le Parti, aderire alle presenti clausole in qualunque momento, in qualità di titolare del trattamento o di responsabile del trattamento, compilando gli allegati e firmando congiuntamente il presente DPA.

b) Una volta compilati e firmati gli Allegati di cui alla lettera a), l'entità aderente è considerata Parte delle presenti clausole e ha i diritti e gli obblighi di un titolare del trattamento o di un responsabile del trattamento, conformemente alla sua designazione nel DPA.

c) L'entità aderente non ha diritti od obblighi derivanti a norma delle presenti clausole per il periodo precedente all'adesione.

SEZIONE II
OBBLIGHI DELLE PARTI

CLAUSOLA 6
Descrizione del(i) trattamento(i)

I dettagli del/i trattamento/i, in particolare le categorie di dati personali e le finalità del trattamento per le quali i dati personali sono trattati per conto del titolare del trattamento, sono specificati nell'Allegato I.

CLAUSOLA 7
Obblighi delle Parti

7.1. Istruzioni

a) Il responsabile del trattamento tratta i dati personali soltanto su istruzione documentata del titolare del trattamento, salvo che lo richieda il diritto dell'Unione o di uno Stato membro cui è soggetto il responsabile del

trattamento. In tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto lo vieti per rilevanti motivi di interesse pubblico. Il titolare del trattamento può anche impartire istruzioni successive per tutta la durata del trattamento dei dati personali. Tali istruzioni sono sempre documentate.

b) Il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, le istruzioni del titolare del trattamento violino il Regolamento (UE) 2016/679 e/o il Regolamento (UE) 2018/1725 o le disposizioni applicabili, dell'Unione e/o di uno Stato membro, relative alla protezione dei dati.

7.2. Limitazione delle finalità

Il responsabile del trattamento tratta i dati personali soltanto per le finalità specifiche del trattamento di cui all'Allegato I, salvo ulteriori istruzioni del titolare del trattamento.

7.3. Durata del trattamento dei dati personali

Il responsabile del trattamento tratta i dati personali soltanto per la durata specificata nell'Allegato I.

7.4. Sicurezza del trattamento

a) Il responsabile del trattamento mette in atto almeno le misure tecniche e organizzative specificate nell'Allegato II per garantire la sicurezza dei dati personali. Ciò include la protezione da ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati (violazione dei dati personali). Nel valutare l'adeguato livello di sicurezza, le Parti tengono debitamente conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per i soggetti interessati al trattamento.

b) Il responsabile del trattamento concede l'accesso ai dati personali oggetto di trattamento ai membri del suo personale soltanto nella misura strettamente necessaria per l'attuazione, la gestione e il controllo del contratto. Il responsabile del trattamento garantisce che le persone autorizzate al trattamento dei dati personali ricevuti si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

7.5. Dati sensibili

Se il trattamento riguarda dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici o dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o dati relativi a condanne penali e a reati ("dati sensibili"), il responsabile del trattamento applica limitazioni specifiche e/o garanzie supplementari.

7.6 Documentazione e rispetto

a) Le Parti devono essere in grado di dimostrare il rispetto delle presenti clausole.

b) Il responsabile del trattamento risponde prontamente e adeguatamente alle richieste di informazioni del titolare del trattamento relative al trattamento dei dati conformemente alle presenti clausole.

c) Il responsabile del trattamento mette a disposizione del titolare del trattamento tutte le informazioni necessarie a dimostrare il rispetto degli obblighi stabiliti nelle presenti clausole e che derivano direttamente dal Regolamento (UE) 2016/679 e/o dal Regolamento (UE) 2018/1725. Su richiesta del titolare del trattamento, il responsabile del trattamento consente e contribuisce alle attività di revisione delle attività di trattamento di cui alle presenti clausole, a intervalli ragionevoli o se vi sono indicazioni di inosservanza. Nel decidere in merito a un riesame o a un'attività di revisione, il titolare del trattamento può tenere conto delle pertinenti certificazioni in possesso del responsabile del trattamento.

d) Il titolare del trattamento può scegliere di condurre l'attività di revisione autonomamente o incaricare un revisore indipendente. Le attività di revisione possono comprendere anche ispezioni nei locali o nelle strutture fisiche del responsabile del trattamento e, se del caso, sono effettuate con un preavviso ragionevole.

e) Su richiesta, le Parti mettono a disposizione della o delle autorità di controllo competenti le informazioni di cui alla presente clausola, compresi i risultati di eventuali attività di revisione.

7.7. Impiego di sub-responsabili del trattamento

a) Il responsabile del trattamento ha l'autorizzazione generale del titolare del trattamento per ricorrere a sub-responsabili del trattamento sulla base di un elenco concordato. Il responsabile del trattamento informa specificamente per iscritto il titolare del trattamento di eventuali modifiche previste di tale elenco riguardanti l'aggiunta o la sostituzione di sub-responsabili del trattamento con un anticipo di almeno trenta (30) giorni, dando così al titolare del trattamento tempo sufficiente per poter opporsi a tali modifiche prima del ricorso al o ai sub-responsabili del trattamento in questione. Il responsabile del trattamento fornisce al titolare del trattamento le informazioni necessarie per consentirgli di esercitare il diritto di opposizione. Il consenso del titolare del trattamento è da intendersi accordato qualora lo stesso non si avvalga del diritto di opposizione entro trenta (30) giorni dalla data di notifica del(i) sub-responsabile(i) individuato(i) dal responsabile del trattamento.

Il titolare accetta il coinvolgimento dei sub-responsabili così come elencati all'Allegato III.

b) Qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento per l'esecuzione di specifiche attività di trattamento (per conto del responsabile del trattamento), stipula un contratto che impone al sub-responsabile del trattamento, nella sostanza, gli stessi obblighi in materia di protezione dei dati imposti al responsabile del trattamento conformemente alle presenti clausole. Il responsabile del trattamento si assicura che il sub-responsabile del trattamento rispetti gli obblighi cui il responsabile del trattamento è soggetto a norma delle presenti clausole e del Regolamento (UE) 2016/679 e/o del Regolamento (UE) 2018/1725.

c) Su richiesta del titolare del trattamento, il responsabile del trattamento gli fornisce copia del contratto stipulato con il sub-responsabile del trattamento e di ogni successiva modifica. Nella misura necessaria a proteggere segreti aziendali o altre informazioni riservate, compresi i dati personali, il responsabile del trattamento può espungere informazioni dal contratto prima di trasmetterne una copia.

d) Il responsabile del trattamento rimane pienamente responsabile nei confronti del titolare del trattamento dell'adempimento degli obblighi del sub-responsabile del trattamento derivanti dal contratto che questi ha stipulato con il responsabile del trattamento. Il responsabile del trattamento notifica al titolare del trattamento qualunque inadempimento, da parte del sub-responsabile del trattamento, degli obblighi contrattuali.

7.8. Trasferimento/trattamento di dati a paesi terzi o organizzazioni internazionali

a) Qualunque trasferimento di dati verso un paese terzo o un'organizzazione internazionale da parte del responsabile del trattamento è effettuato soltanto:

i. sulla base di istruzione documentata;

ii. sulla base del preventivo e generale assenso del titolare del trattamento, oppure

iii. per adempiere a un requisito specifico a norma del diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento, e nel rispetto del Capo V del Regolamento (UE) 2016/679 o del Regolamento (UE) 2018/1725.

b) In aggiunta e, comunque, indipendentemente dal requisito del suindicato articolo 7.8, lettera a, qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento conformemente alla clausola 7.7 per l'esecuzione di specifiche attività di trattamento (per conto del titolare del trattamento) e tali attività di trattamento comportino il trasferimento di dati personali ai sensi del Capo V del Regolamento (UE) 2016/679, il titolare trattamento accetta altresì che tale trattamento sia consentito a condizione che:

i. il trattamento sia eseguito in un paese per il quale la Commissione europea ha adottato una decisione di adeguatezza in conformità a quanto disposto all'articolo 45 del Regolamento (UE) 2016/679, ovvero

ii. il responsabile del trattamento e il sub-responsabile del trattamento possono garantire il rispetto del Capo V del Regolamento (UE) 2016/679 utilizzando le clausole contrattuali tipo adottate dalla Commissione conformemente all'articolo 46, paragrafo 2, del Regolamento (UE) 2016/679, purché le condizioni per l'uso di tali clausole contrattuali tipo siano soddisfatte.

c) Il titolare del trattamento conviene pertanto che il trasferimento e il trattamento dei dati personali sia eseguito dal responsabile del trattamento e/o dai sub-responsabili al trattamento elencati all'Allegato III e in conformità al Capo V del Regolamento (UE) 2016/679.

CLAUSOLA 8
Assistenza al titolare del trattamento

a) Il responsabile del trattamento notifica prontamente al titolare del trattamento qualunque richiesta ricevuta dal soggetto interessato al trattamento. Non risponde egli stesso alla richiesta, a meno che sia stato autorizzato in tal senso dal titolare del trattamento.

b) Il responsabile del trattamento assiste il titolare del trattamento nell'adempimento degli obblighi di rispondere alle richieste dei soggetti interessati al trattamento per l'esercizio dei loro diritti, tenuto conto della natura del trattamento. Nell'adempiere agli obblighi di cui alle lettere a) e b), il responsabile del trattamento si attiene alle istruzioni del titolare del trattamento.

c) Oltre all'obbligo di assistere il titolare del trattamento in conformità della clausola 8, lettera b), il responsabile del trattamento assiste il titolare del trattamento anche nel garantire il rispetto dei seguenti obblighi, tenuto conto della natura del trattamento dei dati e delle informazioni a disposizione del responsabile del trattamento:

i. l'obbligo di effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali ("valutazione d'impatto sulla protezione dei dati") qualora un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;

ii. l'obbligo, prima di procedere al trattamento, di consultare la o le autorità di controllo competenti qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio;

iii. l'obbligo di garantire che i dati personali siano esatti e aggiornati, informando senza indugio il titolare del trattamento qualora il responsabile del trattamento venga a conoscenza del fatto che i dati personali che sta trattando sono inesatti o obsoleti;

iv. gli obblighi di cui all'articolo 32 del Regolamento (UE) 2016/679.

d) Le Parti stabiliscono nell'Allegato II le misure tecniche e organizzative adeguate con cui il responsabile del trattamento è tenuto ad assistere il titolare del trattamento nell'applicazione della presente clausola, nonché l'ambito di applicazione e la portata dell'assistenza richiesta.

CLAUSOLA 9
Notifica di una violazione dei dati personali

In caso di violazione dei dati personali, il responsabile del trattamento coopera con il titolare del trattamento e lo assiste nell'adempimento degli obblighi che incombono a quest'ultimo a norma degli articoli 33 e 34 del Regolamento (UE) 2016/679 o degli articoli 34 e 35 del Regolamento (UE) 2018/1725, ove applicabile, tenuto conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento.

9.1 Violazione riguardante dati trattati dal titolare del trattamento

In caso di una violazione dei dati personali trattati dal titolare del trattamento, il responsabile del trattamento assiste il titolare del trattamento:

a) nel notificare la violazione dei dati personali alla o alle autorità di controllo competenti, senza ingiustificato ritardo dopo che il titolare del trattamento ne sia venuto a conoscenza, se del caso (a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche);

b) nell'ottenere le seguenti informazioni che, in conformità dell'articolo 33, paragrafo 3, del Regolamento (UE) 2016/679, devono essere elencate nella notifica del titolare del trattamento, la quale contiene almeno:

i. la natura dei dati personali compresi, ove possibile, le categorie e il numero approssimativo dei soggetti interessati al trattamento in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

ii. le probabili conseguenze della violazione dei dati personali;

iii. le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali, se del caso anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

c) nell'adempiere, in conformità dell'articolo 34 del Regolamento (UE) 2016/679, all'obbligo di comunicare senza ingiustificato ritardo la violazione dei dati personali all'interessato, qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

9.2 Violazione riguardante dati trattati dal responsabile del trattamento

In caso di una violazione dei dati personali trattati dal responsabile del trattamento, quest'ultimo ne dà notifica al titolare del trattamento senza ingiustificato ritardo dopo esserne venuto a conoscenza. La notifica contiene almeno:

a) una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo dei soggetti interessati al trattamento e di registrazioni dei dati in questione);

b) i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni sulla violazione dei dati personali;

c) le probabili conseguenze della violazione dei dati personali e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione, anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

Le Parti stabiliscono nell'Allegato II tutti gli altri elementi che il responsabile del trattamento è tenuto a fornire quando assiste il titolare del trattamento nell'adempimento degli obblighi che incombono al titolare del trattamento a norma degli articoli 33 e 34 del Regolamento (UE) 2016/679.

SEZIONE III
DISPOSIZIONI FINALI

CLAUSOLA 10
Inosservanza delle clausole e risoluzione

a) Fatte salve le disposizioni del Regolamento (UE) 2016/679 e/o del Regolamento (UE) 2018/1725, qualora il responsabile del trattamento violi gli obblighi che gli incombono a norma delle presenti clausole, il titolare del trattamento può dare istruzione al responsabile del trattamento di sospendere il trattamento dei dati personali fino a quando quest'ultimo non rispetti le presenti clausole o non sia risolto il contratto. Il responsabile del trattamento informa prontamente il titolare del trattamento qualora, per qualunque motivo, non sia in grado di rispettare le presenti clausole.

b) Il titolare del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali conformemente alle presenti clausole qualora:

i. il trattamento dei dati personali da parte del responsabile del trattamento sia stato sospeso dal titolare del trattamento in conformità della lettera a) e il rispetto delle presenti clausole non sia ripristinato entro un termine ragionevole e in ogni caso entro un (1) mese dalla sospensione;

ii. il responsabile del trattamento violi in modo sostanziale o persistente le presenti clausole o gli obblighi che gli incombono a norma del Regolamento (UE) 2016/679 e/o del Regolamento (UE) 2018/1725;

iii. il responsabile del trattamento non rispetti una decisione vincolante di un organo giurisdizionale competente o della(e) autorità di controllo competente(i) per quanto riguarda i suoi obblighi in conformità delle presenti clausole o del Regolamento (UE) 2016/679 e/o del Regolamento (UE) 2018/1725.

c) Il responsabile del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali a norma delle presenti clausole qualora, dopo aver informato il titolare del trattamento che le sue istruzioni violano i requisiti giuridici applicabili in conformità della clausola 7.1, lettera b), il titolare del trattamento insista sul rispetto delle istruzioni.

d) Dopo la risoluzione del contratto il responsabile del trattamento, a scelta del titolare del trattamento, cancella tutti i dati personali trattati per conto del titolare del trattamento e certifica a quest'ultimo di averlo fatto, oppure restituisce al titolare del trattamento tutti i dati personali e cancella le copie esistenti, a meno che il diritto dell'Unione o dello Stato membro non richieda la conservazione dei dati personali. Finché i dati non sono cancellati o restituiti, il responsabile del trattamento continua ad assicurare il rispetto delle presenti clausole.

CLAUSOLA 11
Allegati

Allegato I: Dettagli del trattamento
Allegato II: Misure tecniche e organizzative attuate da CONTINENTAL.
Allegato III: Sub-responsabili al trattamento, trasferimenti/trattamenti internazionali di dati personali

ALLEGATO I DESCRIZIONE DEL TRATTAMENTO

1. FINALITÀ DEL TRATTAMENTO

CONTINENTAL è consapevole di operare in qualità di responsabile del trattamento, per conto del Cliente (titolare del trattamento), dei dati personali che sono necessari per l'erogazione dei servizi VDO FLEET.

2. MODALITA' DEL TRATTAMENTO:

2.1 CONTINENTAL ha facoltà di raccogliere, trattare ed utilizzare dati personali esclusivamente con riferimento al contratto di fornitura dei servizi VDO FLEET e in conformità alle istruzioni fornite dal Cliente (cfr. clausola 7.1 precedente).

2.2 I dettagli sull'ambito di applicazione, natura e finalità della raccolta, del trattamento e/o dell'utilizzo dei dati personali sono soggetti ai Termini e alle Condizioni Generali del Contratto principale, nella descrizione dei servizi offerti e nella descrizione funzionale dei servizi offerti.

2.3 Ogni comunicazione da parte del Cliente relativa al trattamento dei dati personali, così come ogni richiesta di correzione, rettifica o cancellazione degli stessi deve essere inoltrata all'indirizzo e-mail: gdpritalia.nm@continental.com

3. CATEGORIE DI SOGGETTI INTERESSATI AL TRATTAMENTO

- ☒ CLIENTE(I)
- ☐ Visitatori
- ☐ Partecipanti a eventi
- ☒ Utenti del servizio
- ☒ Partecipanti alle comunicazioni
- ☒ Sottoscrittori
- ☐ Parti interessate
- ☐ Fornitore e/o Service Provider (contatti individuali presso questi venditori)
- ☒ Personale dipendente
- ☐ Applicanti
- ☐ Ex personale dipendente
- ☐ Apprendisti/tirocinanti
- ☐ Famigliari del personale dipendente
- ☐ Consulenti
- ☒ Rappresentanti di vendita
- ☐ Azionisti
- ☒ Persone di contatto professionale
- ☐ Fornitori e service providers
- ☒ Partner commerciali
- ☒ Altro (si prega di specificare): coloro che sono occupati presso clienti, come ad es. loro conducenti e utenti dei servizi VDO FLEET

4. CATEGORIE DI DATI PROCESSATI

Dati generali / dati privati di contatto:

- ☒ Profili nominativi
- ☐ Immagini
- ☒ Indirizzi privati
- ☒ Data di nascita
- ☒ Documento d'identità (ad es. Carta d'identità, Passaporto, Codice Fiscale, Patente)

☐ Altro: _____

Dati contrattuali

- ☒ Condizioni di pagamento
- ☒ Coordinate bancarie / Carte di credito
- ☒ Solvibilità finanziaria
- ☒ Storicità contrattuale
- ☐ Altro: _____

Dati professionali

- ☒ Dettali personali
- ☐ Posizione e occupazione
- ☒ Gestione della performance
- ☐ Qualifica e formazione
- ☒ Dati retributivi e previdenziali
- ☒ Assenza dal lavoro

☒ Altro:

- Dati di accesso del Cliente e dei suoi operatori/utenti
- Dati dei conducenti (ad es. sede l'azienda o residenza anagrafica laddove applicabile), genere, data di nascita, numero di patente di guida, numero di carta tachigrafica)
- Dati dei veicoli e profili dei veicoli
- Dati delle comunicazioni (ad esempio telefonate, e-mail)
- Dati di movimento, dati GPS
- Attività dei conducenti e profilo di distribuzione dell'attività, inclusi i periodi di guida e i periodi di riposo in conformità a quanto previsto dall'Allegato 1B al Regolamento (UE) 561/2006, Regolamento (UE) 2020/1054, Regolamento (CE) 1360/2002, Regolamento (UE) 165/2014 e Regolamento di attuazione (UE) 2016/799.
- Dati per l'uso del servizio da parte degli utenti e dei download per la carta del conducente e il tachigrafo

Dati di servizio e di utilizzo IT

☐ Identificazione degli accessi
☐ Immagini / dati video
☐ Dati audio / voce
☒ Dati di accesso
☐ Dati meta
☐ Altro: _____
☒ Dati di uso e connessione
☒ Dati e contenuti di telecomunicazione
☐ Dati di identificazione
☐ Autorizzazioni

Qualora applicabile, restrizioni o salvaguardie dei dati sensibili oggetto del trattamento considerano la natura dei dati trattati e i rischi conseguenti, ossia, a titolo di esempio indicativo e non esaustivo: limitazione delle finalità del trattamento, restrizioni all'accesso (ovvero accesso limitato ai soli dipendenti appositamente istruiti e formati a riguardo), registro degli accessi a tali dati, restrizioni al trasferimento o ulteriori misure di sicurezza.

Speciali categorie di dati personali:

☐ Origine etnica o razziale
☐ Salute fisica o mentale
☐ Dati biometrici
☐ Associazionismo sindacale
☐ Condanne/casellario giudiziale
☐ Altro: _____
☐ Credo religioso o filosofico
☐ Opinioni politiche
☐ Dati genetici
☐ Vita sessuale

5. DURATA DEL TRATTAMENTO

5.1 La durata del trattamento è stabilita nei Termini e nelle Condizioni Generali del Contratto principale, e/o in accordi individuali o, ancora, in ordini basati su accordi quadro.

5.2 Dopo avere completato il lavoro o su richiesta del titolare del trattamento – ma al più tardi dopo avere concluso l'esecuzione del contratto – il responsabile del trattamento è tenuto a fornire al titolare del trattamento o a una terza parte nominata dal titolare del trattamento tutti i documenti, i risultati dei trattamenti e degli utilizzi, nonché tutti i dati che sono ancora in suo possesso e che sono connessi o derivanti dal Contratto principale o dal presente DPA.

Tale obbligo si estende anche alle copie e/o alle riproduzioni di supporti dati e/o dei dati conservati o archiviati. Non sussiste alcun diritto di conservazione. Salvo diversamente pattuito nel Contratto, la restituzione deve

avvenire a titolo gratuito. Ogni eventuale costo o spesa relativi a tale restituzione sono da intendersi a carico del responsabile del trattamento.

5.3 Il titolare del trattamento non ha diritto di chiedere al responsabile del trattamento la cancellazione di dati che lo stesso, in conformità di obblighi di legge è, invece, tenuto ad archiviare. Il trattamento di tali dati deve essere ristretto in luogo della cancellazione laddove ciò sia legalmente ammesso (ad esempio se richiesto da specifiche normative nazionali di implementazione della protezione dei dati personali). Ciò si applica, in particolare, qualora per ragioni legati alla specifica modalità di archiviazione, la cancellazione non sia possibile, ovvero lo sia ma solo a fronte di un costo elevatamente sproporzionato.

ALLEGATO II MISURE TECNICHE ED ORGANIZZATIVE IMPLEMENTATE DA CONTINENTAL AI SENSI DELL'ARTICOLO 32 DEL REGOLAMENTO GDPR (UE) 2016/679

Le linee guida di CONTINENTAL (Corporate Policy Continental Information Security Guideline - CISG) definiscono i requisiti minimi relativi alle misure tecniche ed organizzative implementate da CONTINENTAL per la gestione dei dati. Coerentemente con la classificazione dei dati, tali misure sono implementate per un livello superiore agli standard minimi definiti.

I requisiti delle CISG sono implementati all'interno del Gruppo sulla base del, e in conformità alla regolamentazione sulla sicurezza informatica (Corporate Standard Information Security Framework) e del corrispondente sistema di gestione (Information Security Management System - ISMS).

Continental IT Cybersecurity Policy
Corporate Standard Information Security Framework
Annex 1 - Information Security Management System (ISMS)
Annex 2 - Roles & Responsibilities in Information Security - RACI Chart

1. CONTROLLO DEGLI ACCESSI FISICI ALLE STRUTTURE

La salvaguardia dell'accesso ai sistemi che operano il trattamento dei dati è garantita contro l'accesso di soggetti terzi non autorizzati (ad esempio, mediante strutture fisiche di protezione della proprietà, cancelli d'ingresso, barriere e tornelli di ingresso, porte con accesso mediante lettore badge, videosorveglianza, sicurezza organizzativa della proprietà, regolamentazione delle autorizzazioni all'accesso, registrazione degli accessi).

Corporate Standard Classification of Security Zones
Annex 1 - Layout and Security Requirements
Annex 2 - Audio/Visual Recording in Locations
Corporate Standard Continental ID Cards

Dettaglio delle misure adottate:

☒	Sistema di allarme
☒	Sistema automatico di controllo degli accessi
☐	Sistema di chiusura con chiusura a codice
☐	Barriera di accesso con controllo biometrico
☐	Fotocellule/sensori di movimento
☒	Sistema manuale di chiusura incluso procedura di gestione delle chiavi (registro delle chiavi, Sistema di distribuzione delle chiavi)
☒	Mantenimento del registro dei visitatori
☒	Selezione accurata del personale addetto alla sicurezza
☒	Badge chip card/Sistema di chiusura transponder
☒	Video sorveglianza dei punti di ingresso
☒	Chiusure di sicurezza
☒	Controlli di sicurezza delle persone al cancello / alla reception
☒	Attenta selezione del personale di pulizia
☒	Obbligo di indossare tesserino identificativo come dipendente/visitatore
☐	Altro:

2. CONTROLLO DELL'ACCESSO AI DATI E CONTROLLO DELLE AUTENTICAZIONI

Deve essere assicurato per il tramite di adeguati strumenti per la trasmissione dei dati che soggetti terzi non autorizzati non usino sistemi automatizzati di trattamento dei dati (ad es. autenticazione mediante user-name e password).

Corporate Standard Authentication Security Guide (COR-S-3738759)
Corporate Standard CUSTOMER Security Regulation (che sostituisce M60.02.10)
Corporate Standard Mobile Environment Governance (che sostituisce M60.05.01)

Dettaglio delle misure adottate:

☒	Autenticazione con username / password (l'attribuzione delle password è basata sulle vigenti procedure di assegnazione di password)
☐	Uso di sistemi di rilevamento intrusioni
☒	Uso di software antivirus
☒	Uso di un firewall
☒	Creazione dei profili dell'utente
☒	Assegnazione dei profili dell'utente nei sistemi IT
☒	Uso di tecnologia VPN
☒	Crittografia dei supporti di dati mobile
☐	Crittografia dei supporti di dati nei laptop / notebook
☐	Uso di un software di amministrazione centrale degli smartphone (ad esempio per la cancellazione dall'esterno di dati)
☐	Altro:

3. USO DEI DATI, CONTROLLO MEMORIA E CONSERVAZIONE DEI DATI

Deve essere assicurato che i dispositivi di conservazione dei dati non possano essere letti, copiati o rimossi da personale non autorizzato (principio del controllo dei dispositivi di conservazione dati). Deve essere assicurato che all'informazione personale e, quindi, alla sua modifica o cancellazione, non abbia accesso personale non autorizzato (principio del controllo di memoria).

Deve essere assicurato che i soggetti autorizzati ad utilizzare sistemi automatizzati di trattamento dei dati possano avere accesso all'informazione personale solo per il livello corrispondente al loro grado di autorizzazione (ad esempio, mediante protocolli di autorizzazione, password, disposizioni che disciplinano le dimissioni del personale o il suo trasferimento ad altri dipartimenti dell'azienda) (principio del controllo dell'uso dei dati).

Corporate Standard Authentication Security Guide (COR-S-3738759)
Corporate Standard Classification and Control of Information
Corporate Manual Security Guidelines for Databases - 3.4.6 Data Integrity

Dettaglio delle misure adottate:

☒	Ruolo e autorizzazioni sulla base del "need to know principle"
☒	Numero di amministratori limitato alle "assolute necessità"
☒	Mantenimento del registro di accesso alle applicazioni e in particolare degli inserimenti di dati, delle modifiche di dati e della cancellazione di dati
☒	Cancellazione fisica dei dati dai supporti di dati prima del loro riutilizzo
☒	Uso di distruggi documenti o di fornitori di servizi
☒	Gestioni dei diritti ad opera di amministratori di sistema definiti
☒	Policy delle password inclusa la lunghezza delle password, nonché la modifica delle password
☒	Conservazione sicura dei supporti dati
☒	Corretta cancellazione dei supporti dati (DIN 66399)
☐	Mantenimento del registro delle cancellazioni
☐	Altro:

4. CONTROLLO DEL TRASFERIMENTO E DEL TRASPORTO DEI DATI

Deve essere assicurato che la confidenzialità ed integrità dei dati siano protette in occasione del trasferimento di dati personali e del loro trasporto su supporto di dati (ad esempio mediante potenti sistemi crittografati di trasmissione dati, buste chiuse usate per le spedizioni, supporti criptati di conservazione dati)

Corporate Standard Classification and Control of Information

Dettaglio delle misure adottate:

☒	Installazione di linee dedicate e di tunnel VPN
☒	Trasmissione crittografata dei dati su internet (ad esempio HTTPS, SFTP etc.)
☒	Crittografia delle email
☒	Documentazione dei destinatari dei dati e dei periodi di trasferimento programmato e dei concordati periodi di cancellazione
☐	Per il trasporto fisico: attenta selezione del personale addetto al trasporto e dei veicoli
☐	Trasferimento dei dati in forma anonimizzata o pseudonimizzata
☐	Per il trasporto fisico: contenitori/imballaggio per il trasporto sicuro
☐	Altro:

5. CONTROLLO DELL'INSERIMENTO E DELLA TRASMISSIONE DEI DATI

Deve essere assicurato che si possa, a posteriori, verificare e stabilire quale informazione personale sia stata inserita o modificata, in quale momento e ad opera di quale persona all'interno di sistemi di trattamento automatizzati, ad esempio mediante accesso (principio del controllo dell'inserimento). A seconda del sistema in uso, deve essere assicurato che sia possibile verificare e determinare a quali uffici/siti le informazioni personali siano state trasmesse o trasferite utilizzando sistemi di trasmissione dati, o a quali uffici/siti queste possano essere trasmesse (principio del controllo di trasmissione).

Continental IT Cybersecurity Policy
Corporate Standard Authentication Security Guide (COR-S-3738759)
Corporate Standard Classification and Control of Information
Corporate Manual Security Guidelines for Databases - 3.4.6 Data Integrity

Dettaglio delle misure adottate:

☒	Mantenimento di un registro dell'inserimento di dati, delle modifiche o delle cancellazioni di dati
☒	Tracciabilità degli inserimenti, delle modifiche e delle cancellazioni di dati attraverso user-name individuali (non username di gruppo)
☒	Riconoscimento del diritto di inserire, modificare o cancellare dati sulla base del concetto di autorizzazione
☐	Sviluppo di una procedura di supervisione che stabilisca con quali applicazioni i dati possono essere inseriti, modificati o cancellati
☐	Conservazione delle forme da cui I dati sono stati presi con una procedura automatizzata
☐	Altro:

6. CONTROLLO DISPONIBILITÀ, RECUPERO AFFIDABILITÀ ED INTEGRITÀ DEI DATI

Deve essere assicurato che i sistemi in uso per il trattamento dei dati possano essere ricostituiti in caso di interruzione di servizio (principio di ripristino). Deve essere assicurato che tutte le funzioni di sistema siano disponibili e che ogni malfunzionamento sia riportato (principio di affidabilità). Deve essere assicurato che le informazioni personali salvate non siano state danneggiate dai malfunzionamenti di sistema (principio di integrità). Deve essere assicurato che i dati personali siano protetti da perdite o distruzioni accidentali (principio di controllo di disponibilità), ad esempio mediante l'attuazione di misure appropriate di backup o di disaster recovery.

Corporate Standard Backup and Recovery Security Guide (COR-S-0600208)

Dettaglio delle misure adottate:

☒	Alimentazione elettrica senza interruzioni (UPS)
☒	Attrezzature per controllare le temperature e l'umidità nei locali dove sono allocati i server.
☒	Sistemi di rilevamento di fuoco e fumo
☐	Allarme in caso di ingresso non autorizzato ai locali in cui sono allocati i server
☒	Test di recupero dei dati/data recovery
☒	Conservazione di dati in luogo sicuro ed esterno all'azienda
☐	In zone soggette ad allagamento: i locali in cui sono allocati i server sono posti al di sopra del livello dell'acqua
☒	Aria condizionata nei locali in cui sono allocati i server
☐	Prese di corrente multipla sicure nei locali in cui sono allocati i server
☒	Estintori nei locali in cui sono allocati i server
☒	Sviluppo del concetto di backup & recovery
☐	Creazione di un piano di emergenza
☐	Altro:

7. REGOLA DELLA SEPARAZIONE E DEL CONTROLLO DEI DATI

Deve essere assicurato che i diversi dati raccolti per finalità diverse possano essere trattati in maniera diversa (ad esempio mediante una logica separazione dei dati afferenti alla clientela, controlli di accesso specializzati (concetto di autorizzazione), separazione dei dati utilizzati nelle fasi di controllo e di produzione).

Continental IT Cybersecurity Policy

Dettaglio delle misure adottate:

☒	Conservazione fisicamente separata su sistemi o supporti di dati separati
☐	Aggiunta di aggiunte di oggetti/campi di dati ai registri di dati
☒	Determinazione dei diritti di database
☐	Separazione logica cliente (basato sul software)
☐	Per i dati pseudonimizzati: separazione del file di assegnazione e archiviazione su un Sistema IT separato e sicuro
☒	Separazione del sistema produttivo e di quello di controllo
☐	Altro:

ALLEGATO III SUB-RESPONSABILI/TRASFERIMENTI INTERNAZIONALI

CONTINENTAL assicura che un livello appropriato di misure tecniche e organizzative sia garantito da tutti i soggetti sub-responsabili coinvolti nel processo di trattamento dei dati personali all'interno di un contesto sicuro e appropriato (principio di adeguatezza del sub-responsabile).

Nel caso in cui sub-responsabili siano stati contrattualizzati (ad esempio per servizi di hosting, servizi di allocamento dati in remoto, software di elaborazione delle informazioni personali, ecc.) per la raccolta, trattamento o uso delle informazioni personali, l'implementazione di misure tecniche e organizzative attuati dai singoli sub-responsabili è oggetto di un'apposita regolazione a opera di specifici Accordi di Protezione dei Dati Personali. Il sub-responsabile deve assicurare almeno – con sufficienti garanzie – il livello di misure tecniche ed organizzative pattuite dal Cliente con CONTINENTAL.

Con il fine di prevenire e/o di evitare ogni accesso non autorizzato e/o ogni tentativo non autorizzato di accesso ai sistemi informatici e di archiviazione di CONTINENTAL, ivi inclusi i dati in essi salvati e processati – sia esternamente, sia internamente o ancora da sub-responsabili esterni al trattamento – CONTINENTAL ha implementato misure permanenti di controllo e di monitoraggio per i propri sistemi informatici, ivi inclusi il controllo dell'accesso e del monitoraggio (24/7, 365 giorni l'anno) attraverso l'adozione di sistemi aggiornati di individuazione delle intrusioni come, a titolo di esempio, firewalls, controllo degli accessi, ecc. Laddove sia individuato un accesso non autorizzato o un tentativo di accesso non autorizzato, esso sarà bloccato automaticamente senza ritardo. Il Service Team di Continental Automotive Technologies GmbH in Europa detiene il controllo esclusivo di tali sistemi di sicurezza; l'accesso a tali sistemi da parte dei responsabili al trattamento così come di ogni altro soggetto è escluso.

I seguenti sub-responsabili/sub-fornitori sono coinvolti da CONTINENTAL:

	SUB-RESPONSABILI APPLICABILI A TUTTI I PAESI/CLIENTI
☒	**Eviden Germania GmbH**, Otto-Hahn Ring 6, 81739 Monaco di Baviera, Germania. (Servizi di Supporto e Manutenzione)
☒	**Clearblade Inc.**, 1701 Directors BLVD STE 250, Austin, TX 78744, Stati Uniti (Soluzioni per la gestione della connettività dei dispositivi telematici, attività di supporto e di manutenzione) **Nota importante:** Continental assicura che i servizi e i dati personali ad essi collegati che sono originati all'interno dello Spazio Economico europeo (SEE) saranno esclusivamente trattati su server situati all'interno di esso. Inoltre, a ulteriore garanzia, si applicano le condizioni contrattuali tipo della Commissione europea (così come previsto dalla Decisione di esecuzione (UE) 2021/914 della Commissione del 4 giugno 2021 relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi) che sono state accettate da Clearblade. Trova poi applicazione anche la nuova decisione della Commissione europea del 10 luglio 2023 sul quadro UE-USA per la protezione dei dati personali. In aggiunta, CONTINENTAL ha implementato specifiche misure tecniche di sicurezza come sopra descritto e finalizzate a prevenire ogni accesso non autorizzato ai dati, specialmente se proveniente dall'esterno dallo Spazio Economico Europeo (SEE).
☒	**Com-a-tec GmbH**, Am Krebsgraben 15, 78048 Villingen-Schwenningen, Germania. (Supporto di Livello 2)
☒	**Continental Automotive Technologies GmbH e le aziende ad essa affiliate**, Vahrenwalder Straße 9, 30165 Hannover, Germania. (Sviluppo e Supporto)
☒	**DataDog Inc.,** New York Times Building, 620 8th Ave 45th Floor, New York, MA, Stati Uniti. (Servizi di Supporto e Servizi di disponibilità)

	Nota importante: Data Dog tratta esclusivamente i dati in modo aggregato e pseudonomizzato. Inoltre, e a ulteriore garanzia, si applicano le clausole contrattuali tipo della Commissione europea (così come previsto dalla Decisione di esecuzione (UE) 2021/914 della Commissione del 4 giugno 2021 relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi), così come la nuova decisione della Commissione europea del 10 luglio 2023 sul quadro UE-USA per la protezione dei dati personali. In aggiunta, CONTINENTAL ha implementato specifiche misure tecniche di sicurezza come sopra descritto e finalizzate a prevenire ogni accesso non autorizzato ai dati, specialmente se proveniente dall'esterno dallo Spazio Economico Europeo (SEE).
☒	**Google Ireland Limited, Google Ireland Limited** Gordon House, Barrow Street, Dublino 4, Irlanda. (Servizi Cloud, ad es. Piattaforma Cloud Google). **Nota importante:** Google sarà utilizzato in qualità di sub-responsabile per l'erogazione di servizi cloud. A tale riguardo, CONTINENTAL assicura che i dati originati all'interno dello Spazio Economico Europeo (SEE) siano trattati esclusivamente all'interno di esso, salvo diversamente pattuito con il Cliente. Inoltre, a ulteriore garanzia, si applicano le condizioni contrattuali tipo della Commissione europea (così come previsto dalla Decisione di esecuzione (UE) 2021/914 della Commissione del 4 giugno 2021 relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi), così come la nuova decisione della Commissione europea del 10 luglio 2023 sul quadro UE-USA per la protezione dei dati personali. In aggiunta, CONTINENTAL ha implementato specifiche misure tecniche di sicurezza come sopra descritto e finalizzate a prevenire ogni accesso non autorizzato ai dati, specialmente se proveniente dall'esterno dallo Spazio Economico Europeo (SEE).
☒	**kernel concepts GmbH**, Hauptstraße 16, 57074 Siegen, Germania. (Provider di servizi kernel, miglioramento, manutenzione, ecc.). I dati sono trattati esclusivamente all'interno dello Spazio Economico Europeo (SEE)
☒	**MongoDB Limited**, 3 Shelbourne Buildings, Ballsbridge, Dublino 4, Irlanda. (Servizi Cloud). I servizi cloud sono limitati allo Spazio Economico Europeo (SEE.
☒	**OKTA Inc.**, 100 First Street, 6th Floor, San Francisco, CA 94105, Stati Uniti (Provider di Servizi Customer Identity & Access Management - CIAM) **Nota importante:** Continental assicura che i servizi e i dati personali ad essi collegati che sono originati all'interno dello Spazio Economico europeo (SEE) saranno esclusivamente trattati su server situati all'interno di esso. Inoltre, a ulteriore garanzia, si applicano le condizioni contrattuali tipo della Commissione europea (così come previsto dalla Decisione di esecuzione (UE) 2021/914 della Commissione del 4 giugno 2021 relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi) che sono state accettate da Okta. Trova poi applicazione anche la nuova decisione della Commissione europea del 10 luglio 2023 sul quadro UE-USA per la protezione dei dati personali. In aggiunta, CONTINENTAL ha implementato specifiche misure tecniche di sicurezza come sopra descritto e finalizzate a prevenire ogni accesso non autorizzato ai dati, specialmente se proveniente dall'esterno dallo Spazio Economico Europeo (SEE).
☒	**pendo.io Inc.**, 150 Fayetteville St., Raleigh, NC 27601, Stati Uniti. Rappresentante in Europa ai sensi dell'articolo 27 del Regolamento 2016/679: DP-Dock GmbH, Ballindamm 39, 20095 Amburgo, Germania (Servizi di supporto e di sviluppo). **Nota importante**: pendo.io tratta esclusivamente i dati in modo aggregato e pseudonomizzato. I dati sono trattati e archiviati esclusivamente all'interno dello Spazio Economico Europeo (SEE). Inoltre, a ulteriore garanzia, si applicano le condizioni contrattuali tipo della Commissione europea (così come previsto dalla Decisione di esecuzione (UE) 2021/914 della Commissione del 4 giugno 2021 relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi), così come la nuova decisione della Commissione europea del 10 luglio 2023 sul quadro UE-USA per la protezione dei dati personali. In aggiunta, CONTINENTAL ha implementato specifiche misure tecniche di sicurezza come sopra descritto e finalizzate a prevenire ogni accesso non autorizzato ai dati, specialmente se proveniente dall'esterno dallo Spazio Economico Europeo (SEE).

☒	**SYZYGY Deutschland GmbH**, Im Atzelnest 3, 61352 Bad Homburg, Germania (Servizi di Hosting)
☒	**Thales**, 31 Place des Corolles, CS 20001 - 92098 Paris La Défense, Francia (Servizi di hosting encryption keys nell'ambito di sistemi key management - KMS)
☒	**Zonar Systems, Inc.**, 18200 Cascade Ave S, Seattle, WA 98188, Stati Uniti. Zonar Systems, Inc. è un soggetto sussidiario interamente di proprietà del Gruppo Continental. Zonar Systems fornisce attività di supporto, manutenzione e sviluppo dei servizi VDO FLEET CONTINENTAL. **Nota importante**: Ogni accesso effettuato da Zonar Systems ai dati personali dei clienti VDO FLEET avviene all'interno dello Spazio Economico Europeo (SEE) ed è soggetto alle Binding Corporate Rules del Gruppo Continental che assicurano un adeguato livello di protezione del trattamento dei dati personali in conformità all'articolo 45 e ss. del Regolamento (UE) 2016/679; esso è altresì assicurato dall'applicazione della nuova decisione della Commissione europea del 10 luglio 2023 sul quadro UE-USA per la protezione dei dati personali. In aggiunta, CONTINENTAL ha implementato specifiche misure tecniche di sicurezza come sopra descritto e finalizzate a prevenire ogni accesso non autorizzato ai dati, specialmente se proveniente dall'esterno dallo Spazio Economico Europeo (SEE).

	Note generali: I diritti del Cliente così previsti dal Regolamento 2016/679/UE (Regolamento GDPR) rimangono invariati. CONTINENTAL conferma, inoltre, che i dati del Cliente sono archiviati in centri di raccolta dati localizzati all'interno del territorio dell'Unione europea. CONTINENTAL applica i più severi e stringenti criteri e standard di sicurezza (ad es. ISO/DIN/https/encryption) e tutela i dati personali durante le operazioni di trasmissione e d archiviazione.

	ULTERIORI SUB-RESPONSABILI APPLICABILI ALL'ITALIA/CLIENTI ITALIANI
☒	**Astrata Europe B.V.**, High Tech Campus 32, 5656 AE Eindhoven, Paesi Bassi. (Servizi di Cloud/Hosting)
☒	**B2YOU S.r.l.**, Viale Col di Lana 12, 20136 Milano, Italia. (Servizi di segreteria remotizzata)
☒	**Citrix Systems, Inc.,** 74114 Hollister Avenue, 93117 Goleta, Stati Uniti. (Servizi di Cloud / Hosting) **Nota importante:** Citrix Systems, Inc. opera il trattamento dei dati personali nell'ambito del Data Processing Agreement siglato con Continental Automotive Trading Italia S.r.l., è effettuato in conformità all'articolo 32 del Regolamento (UE) 2016/679 ed è soggetto alle Binding Corporate Rules del Gruppo Continental che assicurano un adeguato livello di protezione del trattamento dei dati personali in conformità all'articolo 45 e ss. del Regolamento (UE) 2016/679. Inoltre, a ulteriore garanzia, si applicano le condizioni contrattuali tipo della Commissione europea (così come previsto dalla Decisione di esecuzione (UE) 2021/914 della Commissione del 4 giugno 2021 relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi, così come la nuova decisione della Commissione europea del 10 luglio 2023 sul quadro UE-USA per la protezione dei dati personali. In aggiunta, CONTINENTAL ha implementato specifiche misure tecniche di sicurezza come sopra descritto e finalizzate a prevenire ogni accesso non autorizzato ai dati, specialmente se proveniente dall'esterno dallo Spazio Economico Europeo (SEE).
☒	**Datimedia S.r.l.**, Via Vittorio Emanuele II 42, 25122 Brescia, Italia (Servizi di segreteria remotizzata)
☒	**DI ITALIA S.r.l.**, Via Giovanni della Casa 5, 20151 Milano, Italia (Servizi di RTM)
☒	**Frotcom International,** Av. do Forte, 6 - Ed. Ramazzotti – Piso 3 – P2.31, 2790-072, Carnaxide, Portogallo (Servizi di RTM)
☒	**MiX Telematics Europe Ltd.,** 6180 Knights Court, Solihull Parkway, Birmingham Business Park, Birmingham, B37 7YB, Gran Bretagna. (Servizi di RTM) **Nota importante**: MiX Telematics Europe Limited opera il trattamento dei dati personali nell'ambito del Data Sub-Processing Agreement siglato con Continental Automotive Trading Italia S.r.l., è effettuato in conformità all'articolo 32 del Regolamento (UE) 2016/679 ed è, infine, soggetto alle Binding Corporate Rules del Gruppo Continental che assicurano un adeguato livello di protezione del trattamento dei dati personali in conformità all'articolo 45 e ss. del Regolamento (UE) 2016/679. Inoltre, a ulteriore garanzia, si applicano le condizioni contrattuali tipo della Commissione europea (così come previsto dalla Decisione di esecuzione (UE) 2021/914 della Commissione del 4 giugno 2021 relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi.
☒	**UAB RUPTELA,** Perkūnkiemio str. 6. LT-12130 Vilnius, Lituania. (Servizi di scarico dati da remoto e servizi di telematica)

	Note generali: I diritti del Cliente così previsti dal Regolamento 2016/679/UE (Regolamento GDPR) rimangono invariati. CONTINENTAL conferma, inoltre, che i dati del Cliente sono archiviati in centri di raccolta dati localizzati all'interno del territorio dell'Unione europea. CONTINENTAL applica i più severi e stringenti criteri e standard di sicurezza (ad es. ISO/DIN/https/encryption) e tutela i dati personali durante le operazioni di trasmissione e d archiviazione.

* * *