LOGISTIK IM FLUSS.

Contratto per l'Elaborazione dei Dati degli Ordini (ai sensi dell'art. 28 dell'RGPD)

tra

l'**Utente** (come definito nel Contratto principale)

(di seguito denominato "**Committente**")

e

TB Digital Services GmbH, Oskar-Schlemmer-Str. 19 - 21, 80807 Monaco di Baviera

(di seguito denominata "**Fornitore**")
(Committente e Fornitore verranno di seguito denominati "**Parte**" o "**Parti**" a seconda che vengano intesi singolarmente o nel loro insieme).

Premessa

(A) Il presente Contratto per l'Elaborazione dei Dati degli Ordini (di seguito denominato "**Contratto**") si applica a tutte quelle attività in cui il Fornitore viene a conoscenza dei dati personali (come definiti nel punto 1.5) del Committente, di fornitori terzi o di altri soggetti coinvolti nelle attività di cui al punto 2 delle Condizioni Generali per l'utilizzo della piattaforma nonché eventualmente dei contratti individuali stipulati per altri servizi (di seguito denominati "**Contratto principale**").

(B) Nel presente Contratto, Committente e Fornitore attuano rispettivamente in qualità di responsabile e di incaricato del trattamento nell'ambito dell'elaborazione dei dati degli ordini ai sensi dell'art. 28 del Regolamento Generale sulla Protezione dei Dati (RGPD), come illustrato in seguito.

Ciò premesso, le Parti concordano quanto segue:

1 Definizioni e interpretazione

1.1 Con il termine "**diritto europeo**" si intende il diritto applicabile dell'Unione Europea, le leggi applicabili degli Stati membri attuali dell'Unione Europea e le leggi applicabili di ciascuno Stato che entrerà a far parte dell'Unione Europea.

1.2 Con il termine "**legislazione europea in materia di protezione dei dati**" si intende l'insieme delle norme applicabili dell'Unione Europea relative al trattamento dei dati personali (in particolare l'RGPD), le leggi applicabili degli Stati membri attuali dell'Unione Europea in materia di trattamento dei dati personali (in particolare la BDSG nella sua versione attuale), nonché le leggi applicabili di ciascuno Stato che entrerà a far parte dell'Unione Europea relative al trattamento dei dati personali.

1.3 La sigla "**RGPD**" si riferisce al "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)".

1.4 "**BDSG**" è la sigla che sta per *Bundesdatenschutzgesetz*, la legge federale in materia di protezione dei dati.

1.5 Il termine "**dati personali**" presenta la stessa accezione riportata nella BDSG/nell'RGPD.

2 Oggetto del trattamento dei dati / Obblighi del Committente

2.1 Il presente Contratto disciplina gli obblighi delle Parti per quanto riguarda il trattamento dei dati personali del Committente da parte del Fornitore nell'ambito del Contratto principale di cui all'Allegato 1.

2.2 L'oggetto, la durata, le modalità e le finalità del trattamento, il tipo di dati personali raccolti, le categorie dei soggetti coinvolti, nonché gli obblighi e i diritti del responsabile vengono illustrati nell'Allegato 1 del presente Contratto e nella descrizione dei servizi del Contratto principale.

2.3 Il Committente detiene la responsabilità per il trattamento dei dati ai sensi dell'RGPD e si impegna a garantire l'ammissibilità del trattamento dei dati personali dei soggetti interessati (conducenti ed eventuali altre persone). In virtù di ciò, egli è inoltre tenuto ad adempiere in particolare a tutti gli obblighi di informazione, garantendo l'esistenza di un'apposita base giuridica per la protezione dei dati personali (ad es. stipula di un accordo operativo, limitazione del trattamento agli scopi concernenti il rapporto di lavoro).

3 Obblighi del Fornitore

3.1 Il Fornitore elabora i dati personali del Committente solo ed esclusivamente per le finalità previste dall'Allegato 1 e nell'ambito del Contratto principale, nonché su incarico e secondo le istruzioni impartite dal Committente di cui all'Allegato 1. Il Fornitore non dovrà elaborare i dati personali per scopi diversi da quelli previsti dal presente Contratto. Resta salvo il trattamento eseguito al di fuori del presente Contratto per scopi interni di cui al punto 8.3.4 del Contratto principale. Non possono essere create copie né duplicati dei dati personali a insaputa del Committente, ad eccezione delle copie di sicurezza necessarie a garantire un corretto trattamento dei dati, nonché dei dati richiesti dalla legge (rispetto degli obblighi di conservazione dei dati).

3.2 Una volta conclusa l'erogazione dei servizi per cui è richiesto il trattamento dei dati personali, il Fornitore è tenuto, in base alla scelta del Committente, a consegnare a quest'ultimo tutti i suoi dati personali e/o a eliminarli nel rispetto della privacy, purché si osservino i tempi di conservazione previsti

dalla legge e purché i dati non debbano essere elaborati per scopi interni che esulano dal presente Contratto di cui al punto 8.3.4 del Contratto principale. Lo stesso vale per i materiali di prova e di scarto. Su richiesta, la completa cancellazione e/o la restituzione dei dati al Committente devono essere comunicate a quest'ultimo per iscritto indicandone la data.

3.3 In base alle prestazioni pattuite, il Fornitore dovrà supportare il Committente nell'adempimento dei diritti degli interessati (informazione, rettifica, opposizione, cancellazione) secondo le istruzioni impartite dal Committente stesso.

3.4 Nei casi previsti dalla legge, il Fornitore deve attestare di aver nominato un responsabile della protezione dei dati interno all'azienda (cfr. § 38 della BDSG/art. 37 dell'RGPD).

3.5 Il Fornitore si impegna a comunicare tempestivamente al Committente il risultato delle verifiche condotte dalle autorità di controllo della protezione dei dati qualora queste siano legate al trattamento dei dati del Committente. Il Fornitore provvederà a risolvere ogni eventuale difetto riscontrato entro un termine congruo e a informare il Committente.

3.6 Il trattamento dei dati da parte del Fornitore e dei subfornitori autorizzati dal Committente avrà luogo esclusivamente nel territorio della Repubblica Federale Tedesca, in uno Stato membro dell'Unione Europea o in un altro Stato contraente dell'accordo sullo Spazio Economico Europeo. Qualsiasi trasferimento in un altro Paese (di seguito denominato "**Paese terzo**") necessiterà della previa ed esplicita autorizzazione da parte del Committente e dovrà altresì avvenire soltanto nel caso in cui vengano soddisfatti i particolari requisiti previsti per l'esportazione dei dati in Paesi terzi (cfr. art. 40 e segg. dell'RGPD). A tale scopo, occorre seguire le indicazioni riportate nell'Allegato 1 ed eventualmente accludere ulteriori documenti (contrattuali).

3.7 Il Fornitore ha il compito di istruire i dipendenti impiegati nella realizzazione dei lavori, affinché familiarizzino con le disposizioni in materia di protezione dei dati rilevanti ai fini della loro attività e mantengano l'obbligo di riservatezza dei dati (cfr. art. 28 dell'RGPD comma 3 b). Il Fornitore deve inoltre assicurarsi, attraverso appositi provvedimenti, che ciascun dipendente elabori i dati personali solo su istruzione del Committente.

3.8 Il Fornitore controlla che le norme sulla protezione dei dati di cui al presente Contratto e le istruzioni documentate impartite dal Committente vengano rispettate in modo regolare per tutta la durata del Contratto. I risultati delle verifiche dovranno essere inoltrati al Committente, previa specifica richiesta, qualora questi siano rilevanti ai fini del trattamento dei dati dello stesso. Le misure necessarie per la verifica sono descritte in un programma per la protezione dei dati, che in caso di richiesta dovrà essere presentato al Committente.

3.9 In base alla modalità del trattamento e secondo le possibilità, il Fornitore è tenuto ad aiutare il Committente con apposite misure tecniche e organizzative ad adempiere al proprio obbligo di

rispondere alle domande sull'esercizio dei diritti dei soggetti coinvolti di cui al capitolo III dell'RGPD. In questo caso, il Committente dovrà sostenere i costi risultanti dall'intervento del Fornitore.

3.10 In base alla modalità del trattamento e alle informazioni disponibili, il Fornitore dovrà aiutare il Committente a rispettare gli obblighi previsti dagli art. da 32 a 36 dell'RGPD.

4 Misure tecniche e organizzative per la sicurezza dei dati

4.1 Il Fornitore dovrà adottare adeguate misure tecniche e organizzative al fine di garantire una corretta protezione dei dati (cfr. art. 32 dell'RGPD). In particolare, il Fornitore è tenuto ad attuare le misure tecniche e organizzative stabilite contrattualmente e riportate nell'Allegato 2 del presente Contratto. Durante il rapporto di mandato, il Fornitore dovrà inoltre adeguare tali misure allo sviluppo tecnico e organizzativo senza tuttavia diminuire il livello di protezione. Le modifiche sostanziali devono essere pattuite per iscritto.

4.2 Su richiesta, il Fornitore dovrà provare al Committente l'effettiva osservanza delle misure tecniche e organizzative.

4.3 Il Fornitore è tenuto a fornire un'idonea documentazione relativa al trattamento dei dati che servirà al Committente per comprovare la correttezza dell'operazione. La prova può essere prodotta anche mediante un certificato autorizzato come previsto dall'art. 42 dell'RGPD.

5 Subfornitori

5.1 Al Fornitore è concesso inserire subfornitori di cui all'Allegato 1.

5.2 In generale viene comunque accettato anche l'inserimento di altri subfornitori. Il Fornitore provvederà tuttavia a informare il Committente ogni qual volta sarà prevista una modifica relativamente all'utilizzo o alla sostituzione dei subfornitori. Il Committente avrà la facoltà di opporsi a queste modifiche programmate. Ai sensi del presente regolamento, i servizi aggiuntivi che il Fornitore richiede a terzi a supporto della realizzazione dell'incarico non devono intendersi come rapporti di subfornitura. Questi servizi comprendono ad esempio servizi di telecomunicazione, personale addetto alle pulizie, revisori o servizi per lo smaltimento di supporti dati. Al fine di garantire la massima protezione e sicurezza dei dati del Committente, il Fornitore è tuttavia tenuto a prendere opportuni accordi contrattuali a norma di legge e ad adottare misure di controllo anche per i servizi aggiuntivi forniti da terzi.

5.3 Qualora il Fornitore si avvalesse di un subfornitore, il Fornitore deve assicurarsi che a quest'ultimo vengano imposti gli stessi obblighi in materia di protezione dei dati prescritti al Fornitore nell'ambito del presente Contratto mediante (i) la stipula di un contratto tra il subfornitore e il Fornitore, oppure (ii) tramite altri strumenti giuridici previsti dalla legislazione europea in materia di protezione dei dati. Inoltre, il Fornitore deve soprattutto accertarsi che il subfornitore adotti tutte le misure tecniche e

organizzative opportune in modo tale che il trattamento dei dati personali risulti conforme ai requisiti previsti dall'RGPD. Su esplicita richiesta scritta da parte del Committente, il Fornitore dovrà fornire a quest'ultimo tutte le informazioni riguardanti il contenuto essenziale del contratto e l'attuazione degli obblighi rilevanti ai fini della protezione dei dati. Qualora fosse necessario, il Fornitore dovrà procurare anche la relativa documentazione. In questo caso, il Fornitore può nascondere le condizioni commerciali. Il Committente è tenuto a mantenere la riservatezza in merito alle informazioni ricevute.

6 Diritti di controllo

6.1 Il Committente ha il diritto di controllare personalmente o tramite una terza persona da lui nominata che gli obblighi derivanti dal presente Contratto (comprese le istruzioni impartite) vengano rispettati.

6.2 Durante queste verifiche, il Fornitore deve offrire al Committente tutto il supporto necessario. In particolare, il Fornitore deve garantire l'accesso alle unità di elaborazione dati e fornire tutte le informazioni richieste.

6.3 Nel caso in cui da un controllo emerga che il Fornitore e/o il trattamento non rispettino le disposizioni del presente Contratto e/o della legislazione europea in materia di protezione dei dati, il Fornitore dovrà provvedere ad attuare qualsiasi misura correttiva necessaria al fine di garantire il rispetto delle disposizioni del presente Contratto e/o della legislazione europea in materia di protezione dei dati.

6.4 I costi derivati dal controllo da parte del Committente sono a carico del Committente stesso. I costi che il Fornitore sostiene per il controllo da parte del Committente possono essere richiesti al Committente stesso qualora quest'ultimo esegua o faccia eseguire più di un controllo durante l'anno.

6.5 I controlli effettuati presso la sede del Fornitore devono essere comunicati in modo tempestivo e devono influire il meno possibile sull'attività del Fornitore.

7 Obblighi di informazione

Il Fornitore è tenuto a informare tempestivamente il Committente qualora reputi che un'istruzione impartita da quest'ultimo violi la legislazione europea in materia di protezione dei dati. L'istruzione in questione non dovrà essere seguita fintanto che non verrà modificata o espressamente confermata dal Committente. Il Fornitore non è tenuto a effettuare una verifica sostanziale delle istruzioni.

Nel caso in cui il Fornitore riscontri la presenza di errori o irregolarità nel trattamento dei dati o sospetti una violazione della privacy (di seguito definiti entrambi come "**accaduto**"), dovrà darne opportuna e tempestiva comunicazione al Committente. Il Fornitore dovrà documentare l'accaduto includendo tutte le circostanze dei fatti, le conseguenze che questo ha avuto e tutte le misure attuate per risolverlo; inoltre, su richiesta del Committente, dovrà provvedere a trasmettere immediatamente a quest'ultimo tutte le informazioni documentate in forma scritta o usando mezzi elettronici.

8 Responsabilità ed esenzione

8.1 Il Fornitore risponde per i danni che sono stati causati per dolo e/o negligenza grave da parte del Fornitore stesso o dei suoi ausiliari. Per i danni causati da negligenza lieve da parte del Fornitore o dei suoi ausiliari, il Fornitore risponde solamente in caso di violazione di un obbligo fondamentale. Per "obbligo fondamentale" si intende un obbligo contrattuale importante che ha reso possibile in un primo momento una corretta esecuzione del Contratto e sul cui rispetto il Committente ha riposto e ha dovuto riporre la propria fiducia. In caso di negligenza lieve riguardante la violazione di tali obblighi fondamentali, la responsabilità del Fornitore è limitata ai danni tipici e prevedibili.

8.2 Il Committente esonera il Fornitore da ogni pretesa di terzi (inclusi i soggetti coinvolti e/o le autorità di controllo della protezione dei dati), danni e spese derivati in seguito a una violazione da parte del Committente nei confronti delle disposizioni del presente Contratto e/o nei confronti della legislazione europea in materia di protezione dei dati. Tale principio non si applica se il Committente non è colpevole della violazione o se il Fornitore ha contribuito alla realizzazione della stessa.

9 Periodo di validità

Il periodo di validità del presente Contratto corrisponde a quello del Contratto principale. Nel caso in cui il Contratto principale dovesse terminare per un qualunque motivo, il presente Contratto verrà automaticamente cessato. Ciò non pregiudica la disdetta per motivi importanti.

10 Altro

10.1 I servizi offerti dal Fornitore sulla base del presente Contratto vengono saldati attraverso un sistema di retribuzione disciplinato dal Contratto principale.

10.2 Se i dati personali del Committente depositati presso il Fornitore vengono minacciati da misure di terzi (ad es. da pignoramento o confisca), insolvenza o procedure di concordato oppure da avvenimenti analoghi, il Fornitore ha il dovere di informare immediatamente il Committente.

10.3 Qualora una disposizione del presente Contratto dovesse risultare o divenire inefficace, l'efficacia delle restanti disposizioni rimarrà impregiudicata. Nel caso in cui una clausola diventi inefficace, le Parti provvederanno a sostituirla con un'altra clausola in linea con le finalità del Contratto dal punto di vista economico e materiale.

10.4 Per il caso del Regno Unito, che in futuro non farà più parte dell'Unione Europea, il Fornitore si impegna fin da subito a stipulare tutti gli accordi e a intraprendere tutte le misure necessarie affinché il trattamento dei dati, che costituisce l'oggetto del presente Contratto, possa avvenire nel dato Paese nel rispetto delle leggi sulla protezione dei dati nel momento in cui si separerà definitivamente dall'UE. Se, al momento dell'uscita definitiva, la Commissione europea non dovesse ancora aver presentato alcuna

decisione positiva sull'adeguatezza, queste saranno, dalla prospettiva attuale, le clausole standard in materia di protezione dei dati ai sensi dell'art. 46 comma 2 c) per la trasmissione dei dati personali agli incaricati del trattamento che risiedono in Paesi terzi in cui non è garantito un adeguato livello di protezione.

Qualora il Fornitore non adempiesse a tali obblighi, il Committente ha il diritto di richiedere al Fornitore, con effetto a partire dall'uscita del Regno Unito dall'Unione Europea, che i relativi servizi vengano forniti da una società collegata o da una succursale dell'azienda con sede fissa nel territorio dell'UE, senza che questo comporti ulteriori spese o costi aggiuntivi per il Committente.

10.5 Il presente Contratto per l'Elaborazione dei Dati degli Ordini è stato tradotto in 18 lingue. In caso di discrepanze, farà fede la versione originale in lingua tedesca.

10.6 Il presente Contratto è soggetto alle leggi della Repubblica Federale Tedesca, ad esclusione della Convenzione delle Nazioni Unite sui contratti di compravendita internazionale di merci. Il foro competente esclusivo è Monaco di Baviera.

10.7 I seguenti allegati sono parte integrante del presente Contratto:

Allegato 1 – Descrizione del trattamento dei dati per la gestione degli ordini
Allegato 2 – Misure tecniche e organizzative

ALLEGATO 1 – Descrizione del trattamento dei dati per la gestione degli ordini

1 Contratto principale

Ai sensi del punto 2.1 della parte principale del Contratto, per "Contratto principale" si intendono le "Condizioni Generali per l'utilizzo della piattaforma".

Titolo / Parti: **TB Digital Services GmbH**, Oskar-Schlemmer-Str. 19 - 21, 80807 Monaco di Baviera / **Utente**

2 Oggetto e durata dell'incarico

L'oggetto dell'incarico viene definito al punto 1 (*Oggetto*) e al punto 8 (*Dati dell'Utente e protezione dei dati*) del Contratto principale; la durata dell'incarico è invece esplicitata al punto 7 (*Stipula del Contratto, durata del Contratto e diritti di risoluzione*) del Contratto principale.

3 Entità, modalità e finalità del trattamento dei dati / misure relative al trattamento dei dati

L'entità, le modalità e le finalità del trattamento dei dati personali sono illustrate al punto 8 del Contratto principale.

Di seguito viene riportata una descrizione più dettagliata dell'oggetto dell'incarico con riferimento all'entità, alle modalità e alle finalità:

Al fine di poter espletare i servizi offerti dal Fornitore (come definito nel Contratto principale), quest'ultimo deve raccogliere i dati personali del Committente tramite Connected Vehicle o dispositivi mobili (ed eventualmente i dati personali trasmessi da un fornitore terzo con il quale l'Utente ha stipulato un contratto per servizi di terzi) nella misura necessaria all'espletamento di tali servizi, nonché trasferirli nella propria piattaforma dove andranno memorizzati. Il Fornitore provvederà a trattare i dati memorizzati nella piattaforma nella misura necessaria a espletare i servizi (ad esempio per analizzare, sulla scorta dei dati personali, il comportamento di marcia dei conducenti e l'utilizzo del Connected Vehicle o del dispositivo mobile, nonché per inoltrare al Committente apposite offerte su misura, come corsi di formazione per i conducenti, dettagli per l'allestimento e proposte per aumentare l'efficienza dei veicoli). Maggiori dettagli riguardo all'entità, alle modalità e alle finalità vengono forniti soprattutto nei contratti individuali che andranno stipulati in aggiunta a quelli generali.

4 Categorie dei soggetti coinvolti

Il trattamento dei dati per la gestione degli ordini riguarda le seguenti categorie di soggetti:

- **conducenti e altri collaboratori** (collaboratori della società del Committente), ad es. dipendenti, tirocinanti, candidati, ex dipendenti;
- **conducenti** non dipendenti dell'azienda;

- **referenti** di operatori addetti al carico e allo scarico o di altri partner commerciali del Committente;
- **dipendenti di un gruppo industriale** (dipendenti di un'altra società del gruppo del Committente).

5 Tipologia di dati personali

Il trattamento dei dati per la gestione degli ordini coinvolge le seguenti tipologie di dati personali:

- nome del conducente e n. di identificazione del conducente;
- n. di identificazione del veicolo;
- dati relativi alla posizione;
- dati relativi ai tempi di guida e di riposo;
- dati relativi al comportamento di marcia;
- dati relativi alla condizione del Connected Vehicle;
- dati relativi alla condizione del rimorchio;
- dati relativi alla condizione degli allestimenti e/o delle parti aggiuntive, dei gruppi e degli altri componenti del veicolo;
- dati relativi alla condizione dei dispositivi IoT eventualmente collegati;
- dati relativi alla condizione dei dispositivi mobili;
- dati di caricamento;
- dati degli ordini;
- dati di contatto dei referenti degli operatori addetti al carico e allo scarico o di altri partner commerciali del Committente.

6 Istruzioni documentate

Con queste istruzioni, il Committente incarica il Fornitore di provvedere al trattamento dei dati personali come indicato nel punto 8 del Contratto principale. Questo include in particolar modo le seguenti procedure:

- I dati personali devono essere trasferiti sulla piattaforma basata su cloud del Fornitore attraverso Connected Vehicle o dispositivi mobili per poi essere memorizzati all'interno della stessa.
- Nell'ambito del presente Contratto, i dati personali vengono elaborati solo se necessari per l'adempimento del Contratto principale. Resta salvo quanto previsto dal punto 8.3.4 del Contratto principale.
- Il Fornitore trasmette i dati personali a un fornitore terzo (come definito nel Contratto principale) soltanto se e nella misura in cui è richiesta la trasmissione dei dati personali al fornitore terzo affinché quest'ultimo possa fornire i servizi di terzi (come definiti nel Contratto principale) al Committente.
- Sulla scorta dei dati personali a sua disposizione, il Fornitore analizzerà il comportamento di marcia dei conducenti e l'utilizzo del Connected Vehicle o del dispositivo mobile, nonché inoltrerà al Committente apposite offerte su misura come corsi di formazione per i conducenti, dettagli per l'allestimento e proposte per aumentare l'efficienza dei veicoli.

7 Luogo del trattamento

- Germania.
- Regno Unito; se i dati vengono trattati all'interno dell'Unione Europea per finalità di hosting e/o di supporto IT, sono stati stipulati appositi contratti per l'elaborazione dei dati degli ordini.
- Qualora il Fornitore ricorra a un subfornitore al di fuori dell'Unione Europea (a tale proposito vedere il punto 8 dell'Allegato 1) per finalità di hosting e/o di supporto IT, i dati personali andranno inoltrati sulla base delle clausole di contratto standard/clausole standard relative alla protezione dei dati stipulate tra il Fornitore e il subfornitore per la trasmissione dei dati personali agli incaricati del trattamento che risiedono in Paesi terzi secondo l'art. 46 comma 2 c) dell'RGPD.

8 Subfornitori

Il Fornitore può impiegare i seguenti subfornitori (che a loro volta possono eventualmente ricorrere ad altri subfornitori):

N.	Subfornitore (nome azienda, indirizzo, referente)	Categorie di dati trattati	Fasi del trattamento / Finalità del trattamento dei dati per la gestione degli ordini del subfornitore
1	Salesforce.com EMEA Limited Salesforce.com Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, USA	Tutti i dati personali della piattaforma che hanno a che fare con la vendita (ossia l'area della piattaforma in cui un cliente può registrarsi ed effettuare gli ordini)	Hosting della piattaforma
2	Salesforce.com, Inc., Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, USA	Tutti i dati personali della piattaforma che hanno a che fare con la vendita (ossia l'area della piattaforma in cui un cliente può registrarsi ed effettuare gli ordini)	Supporto IT relativo alla piattaforma
3	Amazon Webservices, Inc., Amazon Web Services, Inc. 410 Terry Avenue North Seattle WA 98109 USA https://aws.amazon.com/de/compliance/contact/	Tutti gli altri dati personali dell'Utente che vengono trasmessi al Fornitore attraverso il veicolo	Hosting della piattaforma / supporto IT relativo all'hosting della piattaforma
4	In futuro probabilmente al posto del n. 3: Amazon Webservices (EU) Amazon Web Services, Inc. P.O. Box 81226 Seattle, WA 98108-1226 USA https://aws.amazon.com/de/compliance/contact/	Tutti gli altri dati personali dell'Utente che vengono trasmessi al Fornitore attraverso il veicolo	Hosting della piattaforma

5	MAN Service und Support GmbH Dachauer Straße 667 80995 Monaco di Baviera Germania	Tutti i dati personali necessari per elaborare le richieste dei clienti nell'ambito dell'assistenza di primo e secondo livello	Assistenza di primo livello
6	Zuora Inc. 3050 S. Delaware Street, Suite 301 San Mateo, CA 94403 USA	Tutti i dati personali necessari per elaborare la fatturazione e lo svolgimento dell'ordine	Hosting della piattaforma (EU Tenant – host: Amazon Web Services (EU) – vedi punto 4
7	MAN Truck & Bus AG Dachauer Str. 667 80995 Monaco di Baviera Germania	Tutti gli altri dati personali dell'Utente che vengono trasmessi al Fornitore attraverso il Connected Vehicle e/o il dispositivo mobile	Hosting della piattaforma
8	T-Systems International GmbH Hahnstraße 43 d 60528 Francoforte sul Meno Germania	Tutti gli altri dati personali dell'Utente che vengono trasmessi al Fornitore attraverso i veicoli TBM1/2	Hosting della piattaforma
9	Scania AB Vagnmakarvägen 1 15187 Södertälje Svezia	Tutti gli altri dati personali dell'Utente che vengono trasmessi al Fornitore attraverso il veicolo	Hosting della piattaforma
10	Volkswagen Veicoli Commerciali Mecklenheidestr. 74 30419 Hannover Germania	Tutti gli altri dati personali dell'Utente che vengono trasmessi al Fornitore attraverso il veicolo	Hosting della piattaforma

ALLEGATO 2 – Misure tecniche e organizzative

Le misure tecniche e organizzative che il Fornitore deve adottare al fine di garantire un livello di protezione commisurato al rischio sono descritte nel programma per la protezione dei dati relativo alla piattaforma di RIO e comprendono quanto segue:

1. Pseudonimizzazione

Qualora i dati personali vengano utilizzati per effettuare analisi statistiche, realizzabili anche con dati in forma pseudonimizzata, vanno adottate apposite tecniche di pseudonimizzazione. Questa operazione prevede di stabilire fin dall'inizio quale campo di dati debba essere pseudonimizzato o meno, poiché altrimenti si potrebbe risalire all'identità della persona. Le chiavi per la pseudonimizzazione vengono memorizzate in un "data safe" ad accesso limitato.

2. Crittografia

I dispositivi mobili comunicano in modo criptato con il terminale in base al certificato di ogni singolo apparecchio. I dati vengono trasmessi in modo criptato all'interno della piattaforma di RIO ("Ubiquitous encryption" o "encryption everywhere").

3. Garanzia della riservatezza

Tutti i dipendenti e i collaboratori sono e vengono informati riguardo al loro obbligo di segretezza e sono tenuti a mantenere l'obbligo di riservatezza dei dati mediante un apposito accordo scritto.

L'infrastruttura informatica impiegata viene fornita da Amazon Web Services (di seguito denominato AWS) sotto forma di cloud (IaaS e PaaS). I controlli di accesso vengono effettuati dall'operatore del Centro Elaborazione Dati di AWS. I centri di elaborazione di AWS sono altamente sicuri e utilizzano misure di controllo elettroniche di ultima generazione, nonché sistemi di controllo di accesso strutturati su più livelli. I centri di elaborazione sono attivi 24 ore su 24 e dispongono di personale addetto alla sicurezza altamente qualificato; l'accesso viene rigorosamente concesso secondo il principio dei privilegi minimi ed esclusivamente per finalità legate all'amministrazione del sistema.

L'accesso ai componenti hardware (client) presso l'azienda TB Digital Services GmbH avviene sulla scorta di misure standard vigenti e adatte al caso specifico. Queste misure includono ad es. limiti di accesso mediante l'utilizzo di tornelli (tornelli a tutt'altezza), impianti di videosorveglianza, sistemi di allarme e/o servizio di sorveglianza, porte con sistemi di sicurezza elettronici o meccanici, edifici con sistemi antiscasso, accessi autorizzati documentati (visitatori, personale esterno) o zone di sicurezza segnalate.

I controlli di accesso comprendono le misure relative alla sicurezza degli apparecchi, della rete e delle applicazioni.

Per garantire la sicurezza degli apparecchi all'interno del veicolo, vengono attuate diverse misure: i dispositivi mobili vengono installati nel veicolo e dotati di un "secure boot", un sistema che blocca qualsiasi tentativo di caricare o avviare un sistema operativo proveniente da fonti esterne. I dispositivi mobili comunicano in modo criptato con il terminale in base al certificato di ogni singolo apparecchio. I dati vengono trasmessi in modo criptato all'interno della piattaforma di RIO ("Ubiquitous encryption" o "encryption everywhere"). Grazie a continui aggiornamenti, i dispositivi sono sempre aggiornati dal punto di vista della sicurezza (patch management).

Anche per quanto riguarda la sicurezza della rete vengono impiegate diverse misure standard. Vengono stabilite apposite regole (conformi allo stato della tecnica) per l'impostazione delle password (lunghezza, grado di complessità, periodo di validità, ecc.). Dopo un certo numero di tentativi in cui l'user ID o la password inserita non risultano corretti, l'ID dell'utente viene (temporaneamente) bloccato. Grazie a un firewall, la rete aziendale rimane protetta dalle reti pubbliche non sicure. Un apposito processo garantisce che i dispositivi mobili vengano regolarmente aggiornati dal punto di vista della sicurezza (processo OTA). Per scoprire o evitare eventuali attacchi hacker alla rete aziendale (Intranet), si ricorre all'utilizzo di adeguate tecnologie come per esempio l'Intrusion Detection System. In tal senso i dipendenti vengono costantemente sensibilizzati in merito agli eventuali pericoli e rischi per la sicurezza.

Per garantire la sicurezza delle applicazioni, vengono adottate alcune misure standard:

Le applicazioni più importanti vengono protette dagli accessi non autorizzati tramite appositi sistemi di autenticazione e autorizzazione. Vengono stabilite apposite regole (conformi allo stato della tecnica) per l'impostazione delle password (lunghezza, grado di complessità, periodo di validità, ecc.). Per le applicazioni che necessitano di una protezione particolare, vengono utilizzati sistemi di autenticazione forte (ad es. token, PKI). Dopo un certo numero di tentativi in cui l'user ID o la password inserita non risultano corretti, l'ID dell'utente viene (temporaneamente) bloccato. I dati utilizzati nel relativo processo vengono memorizzati in forma criptata all'interno di un supporto dati mobile. Gli accessi effettuati e i tentativi di accesso alle applicazioni vengono opportunamente protocollati. I file di protocollo generati vengono conservati per un determinato periodo (min. 90 giorni) e verificati a campione.

Le autorizzazioni dell'utente (per effettuare l'accesso) vengono garantite da diverse misure, che consentono generalmente di attribuirle a una determinata persona. L'assegnazione delle autorizzazioni è responsabilità del titolare della piattaforma e viene regolarmente verificata. Il conferimento dei diritti di accesso avviene solamente in base a un processo prestabilito e documentato. Qualsiasi modifica ai diritti di accesso viene effettuata secondo il "principio dei quattro occhi" e documentata in un file di registro che non sovrascrive il precedente.

Per controllare l'accesso, vengono attuate diverse misure: i diritti di accesso vengono definiti e documentati nell'ambito dei concetti di "ruolo" e "autorizzazione" e vengono attribuiti ai rispettivi ruoli in base ai requisiti legati all'incarico in questione. Gli amministratori tecnici dispongono di ruoli/autorizzazioni specifiche (che, per

quanto tecnicamente possibile, non permettono di accedere ai dati personali). Vi sono ruoli/autorizzazioni specifiche anche per l'assistenza tecnica, che non includono diritti amministrativi.

Per quanto possibile dal punto di vista tecnico e organizzativo, la definizione e l'attribuzione dei ruoli e delle autorizzazioni non vengono eseguite dalle stesse persone. Queste operazioni vengono effettuate all'interno di una procedura (di approvazione) a prova di revisione e hanno una durata limitata. Gli accessi diretti al database eludendo i concetti di ruolo e autorizzazione possono essere effettuati solo da amministratori del database autorizzati. Una norma vieta l'utilizzo di supporti dati privati e vi sono altre norme vincolanti riguardo all'accesso durante le manutenzioni esterne, le manutenzioni remote e il telelavoro. I documenti e i supporti dati vengono distrutti/smaltiti da aziende fidate addette allo smaltimento nel rispetto delle norme in materia di protezione dei dati (ad es. tramite una macchina distruggi documenti).

I ruoli e le autorizzazioni vengono regolarmente adeguati alle strutture organizzative in via di cambiamento (ad es. nuovi ruoli); i ruoli e le autorizzazioni assegnate vengono costantemente verificati (ad es. dai superiori) e, se necessario, adattati o eliminati. A intervalli regolari, viene effettuato un controllo centrale relativamente ai profili standard attribuiti. Gli accessi modificanti (scrittura, cancellazione) vengono protocollati e i file di protocollo generati vengono conservati per un determinato periodo (min. 90 giorni) nonché verificati a campione.

Per garantire una trasmissione sicura dei dati, vengono implementate diverse misure standard:

Le persone incaricate di trasmettere i dati vengono preventivamente istruite sulle misure di sicurezza da adottare. I destinatari vengono già prestabiliti in modo da poter effettuare un controllo adeguato (autenticazione). L'intero processo riguardante la trasmissione dei dati viene stabilito e documentato, così come viene protocollata e documentata l'esecuzione della trasmissione effettiva (ad es. conferma di ricezione, ricevuta). Le persone incaricate di trasmettere i dati eseguono preventivamente una verifica in merito alla plausibilità, alla completezza e alla correttezza degli stessi.

Prima di eseguire l'effettiva trasmissione dei dati, viene verificato l'indirizzo del destinatario (ad es. l'indirizzo e-mail). La trasmissione dei dati tramite Internet avviene in forma criptata (ad es. file crittografati). Per quanto tecnicamente possibile, l'integrità dei dati trasmessi viene garantita dall'impiego della firma digitale. Le conferme di ricezione elettroniche vengono archiviate in modo adeguato. Qualsiasi trasmissione indesiderata di dati su Internet viene bloccata da appositi sistemi (ad es. server proxy, firewall).

Al fine di adempiere all'obbligo di separazione, vengono inoltre adottate le seguenti misure standard:

Vi sono norme vincolanti relative alla limitazione delle finalità del trattamento per l'osservanza dell'obbligo di separazione. I dati raccolti per determinati scopi vengono memorizzati in un archivio separato rispetto ai dati raccolti per altre finalità. I sistemi informatici utilizzati permettono di memorizzare i dati separatamente (tramite multi-tenancy o programmi di accesso). La separazione dei dati viene eseguita nei sistemi di prova e nei sistemi di produzione. In presenza di dati pseudonimizzati, la chiave che permette di reidentificarli viene

memorizzata e conservata in un archivio a parte. In caso di trattamento dei dati per la gestione degli ordini o di trasmissione delle funzioni, il Fornitore elabora i dati di diversi Committenti separatamente. I ruoli e le autorizzazioni già presenti consentono, grazie alla loro struttura, di separare i dati trattati secondo un criterio logico.

4. Garanzia dell'integrità

Al fine di eseguire la protocollazione per l'inserimento dei dati, vengono attuate diverse misure standard:

Vengono protocollate tutte le modifiche relative ai diritti di accesso nonché tutte le attività dell'amministratore. Vengono protocollati gli accessi di scrittura (immissioni, modifiche, cancellazioni) e le modifiche ai campi di dati (ad es. contenuto del record di dati appena immesso o modificato). Viene eseguita una protocollazione sia delle trasmissioni (ad es. download) che dei login.

I documenti utilizzati ai fini della registrazione vengono verificati e archiviati per poter rendere tracciabile l'operazione. Durante la protocollazione vengono registrate tutte le informazioni quali data, ora, nome utente, tipo di attività, programma applicativo e numero d'ordine del record di dati. Le impostazioni della protocollazione vengono documentate.

Viene concesso solamente un accesso di lettura ai file di protocollo. La cerchia di persone autorizzate ad accedere ai file di protocollo è molto ristretta (si limita ad es. all'amministratore, all'incaricato della protezione dei dati e al revisore). I file di protocollo vengono conservati per un periodo di tempo prestabilito (ad es. 1 anno) e poi vengono cancellati nel rispetto della privacy. I file di protocollo vengono regolarmente analizzati tramite processi automatizzati. Le analisi dei file di protocollo vengono redatte, per quanto possibile, in forma pseudonimizzata.

5. Garanzia della disponibilità

Il sistema viene protetto dalla perdita dei dati attraverso meccanismi di replicazione interni presenti nella piattaforma di AWS. Ai fini della sicurezza oggettiva, vengono inoltre attuate le seguenti misure standard di AWS:

Vengono realizzate apposite misure antincendio (ad es. porte antincendio, rilevatori di fumo, pareti antincendio, divieto di fumo). I sistemi computerizzati sono protetti contro le alluvioni (ad es. aula computer situata al 1° piano, rilevatori d'acqua). Vengono adottate misure contro le scosse di terremoto (ad es. aula computer non situata nei pressi di strade statali, binari dei treni, sale macchine). I sistemi computerizzati sono protetti dai campi elettromagnetici (ad es. piastre d'acciaio nelle pareti esterne). Vengono intraprese misure contro gli atti di vandalismo e i furti (cfr. controlli sugli accessi). I sistemi computerizzati sono situati in luoghi climatizzati (temperatura e umidità vengono regolate da un impianto di climatizzazione). I sistemi computerizzati sono protetti contro i picchi di sovratensione mediante un apposito sistema di protezione. Vengono attuate misure per garantire un'alimentazione elettrica continua e priva di anomalie (ad es. gruppi statici di continuità, gruppi elettrogeni di emergenza).

I dati vengono regolarmente salvati all'interno della piattaforma di AWS sotto forma di copie di backup. Il processo di backup è documentato e viene regolarmente controllato e aggiornato. I mezzi di backup sono protetti dall'accesso non autorizzato. I programmi di backup utilizzati sono conformi agli attuali standard qualitativi e vengono regolarmente aggiornati sulla base di questi ultimi. Lontano dal luogo del trattamento è presente un centro di elaborazione con connettività ridondante che, in caso di calamità, è in grado di proseguire l'attività di elaborazione dei dati. Le varie misure finalizzate al controllo della disponibilità sono documentate in un piano per la gestione dei casi d'emergenza messo a punto da AWS.

Prima che gli venga conferito l'incarico di effettuare il trattamento dei dati, il Fornitore viene sottoposto ad attente verifiche in base a criteri prestabiliti (misure tecniche e organizzative). A tale scopo, gli viene in particolare richiesto di presentare in modo dettagliato le misure tecniche e organizzative da lui attuate per garantire la protezione dei dati (risposta al questionario o al concetto sulla protezione dei dati); il tutto verrà poi accuratamente controllato. A seconda della quantità e della sensibilità dei dati trattati, questa verifica può essere eseguita anche in loco presso la sede del Fornitore. Durante la scelta del Fornitore viene tenuto conto della presenza di certificazioni adeguate (ad es. ISO 27001). La verifica dell'idoneità del Fornitore viene documentata in modo chiaro e adeguato.

Per stabilire il rapporto di mandato, tra Committente e Fornitore viene stipulato un Contratto per l'Elaborazione dei Dati degli Ordini. Questo Contratto sancisce in modo dettagliato e per iscritto le competenze, le responsabilità e gli obblighi di entrambe le Parti. Nel caso in cui un fornitore di servizi incaricato dovesse risiedere al di fuori dell'UE o dello Spazio Economico Europeo, vengono applicate le clausole di contratto standard per l'Unione Europea. Il Contratto stabilisce che il Fornitore deve provvedere al trattamento dei dati solo in base alle istruzioni fornitegli dal Committente. Il Fornitore è tenuto a informare tempestivamente il Committente qualora reputi che una delle sue istruzioni violi le norme in materia di protezione dei dati. Al fine di soddisfare i diritti delle Parti coinvolte, nel Contratto per l'Elaborazione dei Dati degli Ordini viene pattuito che il Fornitore debba prestare aiuto al Committente qualora necessario (ad es. nel caso in cui si debbano fornire informazioni ai soggetti interessati).

In seguito, il Contratto stabilisce che il Committente deve controllare il lavoro finale del Fornitore dal punto di vista della forma e del contenuto. Il rispetto delle misure tecniche e organizzative adottate dal Fornitore viene verificato con regolarità. A tal fine, viene preso come riferimento soprattutto il modello degli attestati attuali o delle certificazioni idonee, oppure la prova certificata dei controlli effettuati circa la protezione dei dati e la sicurezza dei sistemi informatici. Nel caso in cui vengano impiegati dei subfornitori, il Contratto prevede apposite misure di controllo anche per questi soggetti.

6. Garanzia della capacità dei sistemi

Il cloud di AWS è strutturato in maniera tale da essere una delle piattaforme di cloud computing più flessibili e sicure al mondo. Progettato per garantire la massima disponibilità ai clienti, questo cloud fornisce una piattaforma estremamente scalabile e sicura al 100%, permettendo al cliente di eseguire all'occorrenza applicazioni e contenuti in modo rapido e sicuro a livello mondiale. I servizi offerti da AWS sono indipendenti dai

contenuti in quanto garantiscono a tutti i clienti lo stesso livello di sicurezza elevato, nonché indipendenti dal tipo di contenuti o dalla regione geografica in cui i contenuti vengono salvati.

I centri di elaborazione di AWS sono altamente sicuri e di livello mondiale e utilizzano misure di controllo elettroniche di ultima generazione nonché sistemi di controllo di accesso strutturati su più livelli. I centri di elaborazione sono attivi 24 ore su 24 e dispongono di personale addetto alla sicurezza altamente qualificato; l'accesso viene rigorosamente concesso secondo il principio dei privilegi minimi ed esclusivamente per finalità legate all'amministrazione del sistema.

7. Procedure per il ripristino della disponibilità dei dati personali in seguito a un incidente di natura fisica o tecnica

I centri di elaborazione di AWS sono strutturati in gruppi e sono distribuiti in diverse regioni del mondo. Tutti i centri di elaborazione sono disponibili online e sono al servizio dei clienti; nessun centro di elaborazione è inattivo. In caso di guasto, i processi automatici spostano il traffico dei dati dei clienti in un'area diversa da quella interessata. Le applicazioni di base vengono impostate con un tipo di configurazione N+1, in modo tale da garantire, in caso di un guasto al centro di elaborazione, una capacità sufficiente per distribuire il traffico di dati agli stabilimenti rimasti (in base al carico).

AWS offre una piattaforma flessibile dove inserire le proprie richieste e memorizzare i dati all'interno di più regioni geografiche, nonché all'interno di una sola regione scegliendo tra diverse zone di disponibilità. Ogni zona di disponibilità nasce come zona a basso rischio. Le zone di disponibilità sono infatti distribuite in base alle caratteristiche fisiche di una regione e si trovano ad esempio in aree a basso rischio di alluvioni (ogni regione ha diverse zone a rischio di alluvione). Oltre alla presenza di gruppi di continuità autonomi e di generatori elettrogeni di emergenza in loco, tutte le zone di disponibilità vengono alimentate tramite diverse reti elettriche di fornitori indipendenti per ridurre al minimo i guasti isolati. Tutte le zone di disponibilità sono connesse in modo ridondante a più provider Tier 1 Transit.

Il team di Amazon addetto alla gestione degli incidenti si avvale di procedure diagnostiche comuni per accelerare la risoluzione dei casi che possono compromettere il funzionamento dell'azienda. Il personale operativo è disponibile 24 su 24, 7 giorni su 7 e 365 giorni all'anno per rilevare la presenza di guasti, gestirne le conseguenze e provvedere alla loro eliminazione.

8. Procedure per la verifica regolare e la valutazione dell'efficacia delle misure tecniche e organizzative

Le direttive e le istruzioni presenti all'interno dell'azienda e le misure standard implementate per garantire la sicurezza delle informazioni vengono applicate anche in relazione al lancio e al funzionamento della piattaforma di RIO. All'interno dell'azienda sono presenti le figure preposte alla protezione dei dati e della sicurezza delle informazioni (incaricato della protezione dei dati e Information Security Officer). I dipendenti

sono tenuti a mantenere la riservatezza dei dati e vengono informati riguardo alle misure in materia di sicurezza dei dati o dei sistemi informatici attraverso brochure, volantini o avvisi via Intranet.

I processi interni vengono controllati per quanto concerne il rispetto delle misure tecniche e organizzative finalizzate alla sicurezza dei dati tramite procedure di revisione, per la sicurezza delle informazioni e la protezione dei dati.

Le operazioni legate al trattamento e le misure per la sicurezza dei dati vengono documentate in un apposito registro delle attività. A intervalli regolari viene eseguita una verifica (a livello interno ed esterno) dell'efficacia delle misure adottate.