Accordo sul trattamento dei dati

Regolamento sulla protezione e sulla sicurezza dei dati nei rapporti contrattuali
ai sensi dell'art. 28 RGPD

Shiftmove GmbH
Warschauer Straße 57
10243 Berlino

- di seguito denominato "Incaricato del trattamento" -

e Lei

- di seguito denominato "Titolare del trattamento" -

- di seguito denominati "Parti contraenti" -

Premessa

Il presente Accordo sul trattamento dei dati ("ATD") ai sensi dell'art. 28 RGPD è parte integrante delle nostre Condizioni generali di contratto ("Contratto principale"), stipulate tra i nostri utenti e Shiftmove GmbH e consultabili qui: **https://www.shiftmove.com/it/legal/agb**. In base al presente accordo, il presente ATD si applica al trattamento dei dati personali dell'utente nel contesto della fornitura del nostro prodotto.

Con la firma del modulo d'ordine, i Termini e condizioni, compreso il presente ATD, si considerano accettati in modo vincolante, pertanto non è generalmente richiesta una firma separata del presente DPA.

Ciononostante, offriamo ai nostri clienti la possibilità di scaricare separatamente il ATD, firmarlo e restituircelo. In tal caso, vi preghiamo di inviare una copia della versione firmata all'indirizzo **privacy@shiftmove.com**.

L'accordo si basa sulle disposizioni del GDPR, della legge federale tedesca sulla protezione dei dati (BDSG) e della legge sui dati.

§ 1 Oggetto dell'accordo; tipo e finalità del trattamento; tipo di dati personali, categorie di interessati

(1) Oggetto dell'accordo è la fornitura di servizi Software as a Service offerti dal Gruppo Shiftmove ("Servizi"). L'oggetto e la finalità del trattamento sono inoltre descritti più in dettaglio nell'allegato 1a. Il tipo di trattamento è definito nell'allegato 1b.

(2) Le categorie di interessati sono indicate nell'allegato 1c.

(3) Il tipo di dati personali trattati è definito nell'allegato 1d.

(4) L'allegato 1 è parte integrante del presente accordo.

(5) Il Titolare del trattamento istruisce l'Incaricato del trattamento a trattare tali dati per queste finalità.

§ 2 Durata dell'incarico

La durata del presente incarico (validità) corrisponde alla durata del Contratto principale.

§ 3 Responsabilità e diritto di impartire istruzioni

(1) Il Titolare del trattamento è responsabile della conformità alle norme sulla protezione dei dati, in particolare della legittimità del trattamento dei dati e del trasferimento dei dati all'Incaricato del trattamento (art. 4 n. 7 RGPD). L'Incaricato del trattamento non utilizzerà i dati per scopi diversi da quelli specificati nel presente Accordo sul trattamento dei dati e nel Contratto principale e, in particolare, non è autorizzato a trasmetterli a terzi. È vietato produrre copie e duplicati all'insaputa del Titolare del trattamento. Eventuali deroghe si applicano solo nei casi di cui al paragrafo 2.

(2) L'Incaricato del trattamento tratta i dati personali solo su istruzioni documentate del Titolare del trattamento, a meno che non sussista un altro obbligo ai sensi del diritto comunitario o dello Stato membro a cui l'Incaricato del trattamento è soggetto. In caso di altri obblighi, l'Incaricato del trattamento informerà tempestivamente il Titolare del trattamento dei relativi requisiti legali prima di procedere al trattamento.

(3) Il Titolare del trattamento, ma non il incaricato del trattamento, è il titolare dei dati (cfr. considerando 22 del Data Act). Il incaricato del trattamento garantisce di non utilizzare tutti i dati trasmessi dal titolare del trattamento (dati personali e non personali) per propri scopi, per la profilazione o per il miglioramento dei prodotti, a meno che ciò non sia stato espressamente autorizzato al Incaricato del trattamento. Il Incaricato del trattamento soddisfa quindi i requisiti di cui all'articolo 6 e all'articolo 8, paragrafo 2, del Data Act.

(4) Se l'Incaricato del trattamento ritiene che una determinata istruzione violi le norme sulla protezione dei dati, ne informa immediatamente il Titolare del trattamento ai sensi dell'art. 28

comma 3 cpv. 3 RGPD. Fino alla conferma o alla modifica della relativa istruzione, l'Incaricato del trattamento è autorizzato a sospenderne l'esecuzione.

(5) Eventuali modifiche all'oggetto del trattamento con variazioni procedurali devono essere concordate e documentate di comune accordo. L'Incaricato del trattamento può fornire informazioni a terzi o all'interessato solo previo consenso scritto del Titolare del trattamento.

§ 4 Riservatezza

Nell'esecuzione delle mansioni, l'Incaricato del trattamento si avvarrà esclusivamente di collaboratori tenuti alla riservatezza ai sensi dell'art. 28 comma 3 cpv. 2 lett. b RGPD e che abbiano precedentemente preso conoscenza delle disposizioni rilevanti in materia di protezione dei dati. L'Incaricato del trattamento e qualsiasi persona a esso subordinata avente accesso ai dati personali possono trattare tali dati solo in conformità alle istruzioni del Titolare del trattamento, comprese le autorizzazioni concesse nel presente Accordo sul trattamento dei dati, a meno che non siano legalmente obbligati a farlo.

§ 5 Sicurezza dei dati

(1) Le Parti contraenti si accordano sulle precise misure di sicurezza dei dati indicate nell'allegato 2 "Misure tecniche e organizzative" del presente accordo, ai sensi dell'art. 28 comma 3 lett. c RGPD in combinato disposto con l'art. 32 comma 1 RGPD, al fine di garantire la sicurezza del trattamento per conto di terzi. In generale, le misure da adottare sono provvedimenti volti a garantire la sicurezza dei dati e un adeguato livello di tutela dai rischi in materia di riservatezza, integrità, disponibilità e affidabilità dei sistemi. A tale proposito, occorre tenere conto dello stato dell'arte, dei costi di attuazione, della natura, dell'ambito e delle finalità del trattamento, nonché della probabilità di incidenza e gravità del rischio per i diritti e le libertà delle persone fisiche ai sensi dell'art. 32 comma 1 RGPD.

(2) L'allegato 2 è parte integrante del presente accordo.

(3) L'Incaricato del trattamento è tenuto a rispettare i principi del corretto trattamento dei dati. Garantisce le misure di sicurezza dei dati concordate in sede contrattuale e prescritte dalla legge. Le misure tecniche e organizzative sono subordinate all'evoluzione e al perfezionamento della tecnologia. In tal senso, l'Incaricato del trattamento è autorizzato a implementare misure alternative adeguate. Nel farlo, non è consentito compromettere il livello di sicurezza offerto dalle misure indicate. Qualsiasi variazione rilevante deve essere documentata e comunicata per iscritto al Titolare del trattamento.

(4) In caso di violazione della protezione dei dati personali, l'Incaricato del trattamento collabora con il Titolare del trattamento e lo supporta adeguatamente affinché il Titolare del trattamento possa adempiere ai propri obblighi ai sensi degli artt. 33, 34 del GDPR, tenendo conto della natura del trattamento e delle informazioni a sua disposizione.

(5) In caso di violazione della protezione dei dati personali relativi ai dati trattati dall'Incaricato del trattamento, quest'ultimo segnala tale violazione al Titolare del trattamento senza indugio, non

appena ne viene a conoscenza. Questa segnalazione deve contenere almeno le seguenti informazioni:

- una descrizione della natura della violazione (indicando possibilmente le categorie e il numero approssimativo delle persone interessate e il numero approssimativo dei registri dei dati interessati);
- dati di contatto di un referente presso il quale si possono ottenere ulteriori informazioni sulla violazione della protezione dei dati personali;
- le probabili conseguenze e le misure adottate o proposte per porre rimedio alla violazione della protezione dei dati personali, comprese le misure per attenuare i possibili effetti negativi.

Qualora e nella misura in cui non tutte queste informazioni possano essere fornite contemporaneamente, la comunicazione iniziale contiene le informazioni disponibili in quel momento, e ulteriori informazioni saranno fornite successivamente senza indebiti ritardi non appena disponibili.

§ 6 Coinvolgimento di ulteriori incaricati del trattamento (subappaltatori)

(1) Per subappaltatori ai sensi del presente regolamento si intendono altri incaricati del trattamento i cui servizi sono direttamente correlati alla fornitura del servizio principale. Non sono inclusi i servizi accessori di cui l'Incaricato del trattamento si avvale, ad es. servizi di telecomunicazione, servizi postali/di trasporto e di pulizia. Tuttavia, l'Incaricato del trattamento è tenuto a stipulare accordi contrattuali e ad adottare misure di controllo adeguate e legalmente conformi per garantire la protezione e la sicurezza dei dati del Titolare del trattamento, anche nel caso di servizi accessori esternalizzati.

(2) È consentito ricorrere a subappaltatori o cambiare l'attuale subappaltatore, a condizione che:

- l'Incaricato del trattamento notifichi al Titolare del trattamento tale esternalizzazione a subappaltatori con 14 giorni di calendario di anticipo per iscritto o in forma testuale;
- il Titolare del trattamento non si opponga all'esternalizzazione prevista dandone comunicazione scritta o in forma testuale all'Incaricato del trattamento prima della trasmissione dei dati.

(3) Qualora il titolare del trattamento si opponga alla modifica del subappaltatore entro il periodo di opposizione di cui al § 6 (2), l'incaricato del trattamento verificherà e informerà il titolare del trattamento se il servizio può essere fornito senza la modifica del subappaltatore. Se, in base alla verifica, l'incaricato del trattamento non può fornire il servizio senza la modifica del subappaltatore, entrambe le parti hanno il diritto di recedere dal contratto per iscritto con un preavviso di 14 giorni.

(4) È necessario stipulare un accordo contrattuale con il subappaltatore ai sensi dell'art. 28 commi 3 e 4 RGPD.

(5) Il trasferimento dei dati personali dal Titolare del trattamento al subappaltatore e l'inizio delle attività di quest'ultimo sono consentiti solo a condizione che tutti i requisiti legali per il subappalto

siano soddisfatti. I subappaltatori autorizzati dal Titolare del trattamento al momento della stipula del contratto sono indicati nell'allegato 3. Inoltre, è possibile consultare i prestatori di servizi dei rispettivi subappaltatori ai seguenti link https://www.vimcar.de/legal/danteschutz/subunternehmer e https://www.avrios.com/it/legal/sub-processors.

(6) Le società collegate del Gruppo Shiftmove sono incaricate come subappaltatori a condizione che siano indicate negli elenchi di cui al § 6 comma 4 del presente accordo.

(7) Il trasferimento del trattamento dei dati a un Paese terzo richiede la preventiva istruzione documentata del Titolare del trattamento (art. 28 comma 3 lett. a RGPD) e può avvenire solo nel rispetto dei requisiti speciali di cui agli artt. 44-49 RGPD.

(8) L'allegato 3 è parte integrante del presente accordo.

§ 7 Diritti degli interessati

(1) L'Incaricato del trattamento è tenuto a supportare il Titolare del trattamento con misure tecniche e organizzative adeguate, ove possibile, per adempiere agli obblighi relativi alle richieste di salvaguardia dei diritti degli interessati di cui agli artt. 12-22 RGPD (art. 28 comma 3 cpv. 2 lett. e RGPD).

(2) Qualora gli interessati abbiano diritto alla portabilità dei dati nei confronti del Titolare del trattamento, l'Incaricato del trattamento deve provvedere a trasmettere a quest'ultimo i dati personali trattati in un formato strutturato, di uso comune e leggibile da dispositivo automatico.

(3) L'Incaricato del trattamento è autorizzato a divulgare, rettificare, cancellare o limitare il trattamento dei dati personali solo previa istruzione documentata del Titolare del trattamento (art. 28 comma 3 cpv. 2 lett. g RGPD).

(4) Se un interessato si rivolge direttamente all'Incaricato del trattamento per far valere i propri diritti ai sensi degli artt. 12-22 RGPD, quest'ultimo inoltrerà tempestivamente la richiesta al Titolare del trattamento.

(5) L'Incaricato del trattamento è autorizzato a fornire informazioni a terzi o a interessati solo previo consenso scritto del Titolare del trattamento.

(6) Il Titolare del trattamento è tenuto a informare gli interessati ai sensi degli artt. 12 e 13 RGPD. Informazioni necessarie in relazione a tale obbligo, di cui solo l'Incaricato del trattamento dispone, saranno messe a disposizione del Titolare del trattamento su richiesta.

(7) Il Incaricato del trattamento assisterà il titolare del trattamento, su sua richiesta, nella fornitura dei dati in un formato strutturato, interoperabile e leggibile da dispositivo automatico e, se necessario, nella loro trasmissione a terzi, nella misura in cui il titolare del trattamento sia chiamato a rispondere in qualità di titolare dei dati degli utenti ai sensi degli articoli 4 e seguenti e dell'articolo 8 del Data Act.

§ 8 Obblighi dell'Incaricato del trattamento

Oltre a rispettare le disposizioni del presente incarico, l'Incaricato del trattamento è tenuto a soddisfare gli obblighi di legge ai sensi degli artt. 28-36 RGPD. A tale proposito, l'Incaricato del trattamento deve in particolare rispettare i seguenti requisiti:

- se l'Incaricato del trattamento è obbligato per legge a nominare per iscritto un responsabile della protezione dei dati ai sensi dell'art. 37 RGPD, § 38 BDSG, l'Incaricato fornirà al Titolare del trattamento i recapiti del responsabile della protezione dei dati per consentire un contatto diretto; in caso di variazione del responsabile della protezione dei dati, il Titolare del trattamento deve esserne immediatamente informato;

- l'Incaricato del trattamento ha nominato

  clever datenschutz GmbH
  E-mail: privacy@shiftmove.com

  come responsabile esterno della protezione dei dati.

(2) L'Incaricato del trattamento supporta il Titolare del trattamento nell'adempimento degli obblighi di cui agli artt. 32-36 RGPD in materia di sicurezza dei dati personali, obblighi di comunicazione in caso di violazioni dei dati, valutazioni d'impatto sulla protezione dei dati e consultazioni preliminari. Ciò include in particolare:

- la garanzia di un livello di protezione adeguato attraverso misure tecniche e organizzative che tengano conto delle circostanze e delle finalità del trattamento, nonché della probabilità e della gravità previste di un'eventuale violazione dovuta a lacune di sicurezza, che consentano l'individuazione immediata di violazioni significative;
- l'obbligo per l'Incaricato del trattamento di informare immediatamente il Titolare del trattamento qualora venga a conoscenza di una violazione dei dati personali (art. 28, comma 3, lett. f, art. 33, comma 2 RGPD);
- l'obbligo di supportare il Titolare del trattamento in relazione al suo dovere di informare l'interessato e di fornirgli senza indugio tutte le informazioni pertinenti al riguardo;
- il supporto al Titolare del trattamento nella valutazione dell'impatto sulla protezione dei dati;
- il supporto al Titolare del trattamento nell'ambito delle consultazioni preventive con l'autorità di vigilanza.

(3) Qualsiasi trasferimento di dati da parte dell'incaricato del trattamento a un paese terzo o a un'organizzazione internazionale deve avvenire esclusivamente nel rispetto dei requisiti legali per il trasferimento di dati a paesi terzi ai sensi dell'art. 44 e seguenti. 44 e segg. GDPR. Al fine di garantire un livello adeguato di protezione dei dati, l'incaricato del trattamento trasferirà i dati a destinatari in paesi terzi solo se esiste una decisione di adeguatezza della Commissione UE per il paese terzo in questione (art. 45 del GDPR), se esistono garanzie adeguate per il trasferimento, come clausole contrattuali standard (art. 46 del GDPR), se esistono regolamenti interni sulla protezione dei dati (art. 47 del GDPR) o altre circostanze eccezionali per il trasferimento dei dati (art. 48 del GDPR). Il responsabile del trattamento acconsente al trasferimento dei dati ai subappaltatori di cui al §6 (5) del presente accordo, che possono avere sede in paesi terzi.

(4) Il Titolare del trattamento assiste il titolare del trattamento nell'adempimento dei suoi obblighi in materia di portabilità dei dati e di cambio di fornitore in conformità con i requisiti del Data Act e fornisce indicazioni sui formati e sulle interfacce supportati ai sensi degli articoli 23-29 del Data Act.

§ 9 Diritti di controllo del Titolare del trattamento, art. 28 comma 3 cpv. 2 lett. h RGPD

(1) L'Incaricato del trattamento si impegna a fornire al Titolare del trattamento, su richiesta scritta ed entro un periodo di tempo ragionevole, tutte le informazioni e gli elementi necessari per effettuare un controllo mediante procedura scritta.

(2) Il Titolare del trattamento ha il diritto di accertarsi, prima dell'inizio del trattamento e a intervalli regolari, del rispetto delle misure tecniche e organizzative attuate dal Incaricato del trattamento.

Ciò avviene principalmente attraverso:

- la richiesta di informazioni al Incaricato del trattamento e/o
- la presentazione di rapporti di verifica indipendenti o certificazioni riconosciute.

a) Controlli in loco in base alle circostanze

Il Titolare del trattamento ha il diritto di effettuare un controllo in loco presso il Incaricato del trattamento se:

- esistono indizi concreti che fanno dubitare della correttezza o della completezza delle relazioni di verifica o delle certificazioni presentate,
- si è verificato un incidente di sicurezza ai sensi dell'art. 33, comma 1, del GDPR in relazione al trattamento dei dati, oppure
- i documenti messi a disposizione non forniscono tutte le prove necessarie.

In questi casi, i controlli in loco devono essere comunicati per iscritto con almeno 14 giorni di calendario di anticipo.

Una riduzione di tale termine è consentita solo in casi eccezionali giustificati, se l'urgenza deriva direttamente dal motivo specifico (ad esempio, in caso di incidente di sicurezza). In tal caso, il Titolare del trattamento deve spiegare in modo comprensibile i motivi della riduzione del termine e, su richiesta, fornirne la prova al Incaricato del trattamento.

b) Controlli in loco senza motivo specifico

Indipendentemente da un motivo specifico, il Titolare del trattamento può effettuare un controllo in loco senza motivo specifico una volta all'anno. Anche i controlli in loco senza

motivo devono essere comunicati per iscritto dal Titolare almeno 14 giorni di calendario prima.

c) Condizioni generali

Il Titolare del diritto di controllo non deve interferire in modo inappropriato con l'attività commerciale del Incaricato del trattamento né essere esercitato in modo abusivo. I costi effettivi dei controlli in loco senza motivo sono a carico del Titolare.

(3) Il Titolare del trattamento è tenuto a redigere un verbale di ogni controllo effettuato. Tutte le discrepanze, i difetti o altre constatazioni significative rilevate nell'ambito del controllo devono essere comunicate al Titolare del trattamento immediatamente, e in ogni caso entro un termine ragionevole dopo la conclusione del controllo, in forma scritta. Il verbale deve essere messo a disposizione del Titolare del trattamento su richiesta.

§ 10 Responsabilità

(1) La responsabilità delle Parti è disciplinata dall'art. 82 RGPD. Resta salva qualsiasi responsabilità dell'Incaricato del trattamento nei confronti del Titolare del trattamento per violazione degli obblighi previsti dal presente accordo o dal Contratto principale.

(2) Le Parti si esonerano reciprocamente dalla responsabilità se una di esse dimostra di non essere in alcun modo responsabile della circostanza che ha causato il danno all'interessato. Si applica il § 10 comma 2 frase 1, in caso di ammenda inflitta a una Parte, laddove l'esenzione viene concessa a condizione che l'altra Parte sia corresponsabile dell'illecito sanzionato dall'ammenda.

§ 11 Annullamento e risoluzione dell'incarico (art. 28 comma 3 cpv. 2 lett. g RGPD)

(1) Se l'Incaricato del trattamento non adempie agli obblighi previsti dalle presenti clausole, il Titolare del trattamento può ordinare all'Incaricato di sospendere il trattamento dei dati personali fino all'adempimento di tali obblighi o alla risoluzione del contratto. L'Incaricato del trattamento dovrà informare tempestivamente il Titolare del trattamento nel caso in cui, per qualsiasi motivo, non sia in grado di rispettare le presenti clausole.

(2) Il Titolare del trattamento ha il diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali in conformità alle presenti clausole se:

- il Titolare del trattamento ha sospeso il trattamento dei dati personali da parte dell'Incaricato del trattamento ai sensi della lett. a) e la conformità alle presenti clausole non è stata ripristinata entro un periodo di tempo ragionevole e in ogni caso entro un mese dalla sospensione;
- l'Incaricato del trattamento viola ripetutamente le presenti clausole o contravviene ai propri obblighi ai sensi del Regolamento generale sulla protezione dei dati;

- l'Incaricato del trattamento non rispetta una decisione vincolante del tribunale competente o delle autorità di vigilanza responsabili in relazione ai suoi obblighi derivanti dalle presenti clausole o dal Regolamento generale sulla protezione dei dati.

(3) L'Incaricato del trattamento avrà il diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali ai sensi delle presenti clausole se il Titolare del trattamento esige che le sue istruzioni vengano eseguite pur essendo stato informato dall'Incaricato che quest'ultime violano i requisiti legali vigenti ai sensi della clausola 7.1 lett. b.

(4) Al termine della fornitura dei servizi di elaborazione, l'Incaricato del trattamento dovrà, a discrezione del Titolare del trattamento, cancellare o restituire tutti i dati personali, a meno che non vi sia un obbligo legale di conservazione degli stessi. Oppure il Titolare del trattamento richiede l'accesso ai sensi del punto 2.1.5 delle Condizioni Generali.

(5) In tal caso, l'Incaricato del trattamento dovrà confermare al Titolare del trattamento in forma testuale, indicando la data e senza ulteriori richieste, di aver restituito o distrutto o cancellato in modo sicuro tutti i supporti di memoria e gli altri documenti fornitigli dal Titolare e di non aver quindi conservato i suoi dati.

(6) La documentazione utile a dimostrare il corretto trattamento dei dati deve essere conservata dall'Incaricato del trattamento oltre la scadenza del contratto, in conformità ai rispettivi periodi di conservazione.

§ 12 Disposizioni finali

(1) I supporti di memoria e i set di dati forniti rimangono proprietà del Titolare del trattamento.

(2) Se una o più disposizioni del presente accordo non sono valide, non viene meno la validità delle restanti disposizioni. Nel caso in cui una o più disposizioni non siano valide, le Parti contraenti sostituiranno immediatamente la disposizione non valida con una il più possibile analoga alla disposizione non valida in termini economici e di protezione dei dati.

(3) Le Parti contraenti concordano che l'esercizio del diritto di ritenzione da parte dell'appaltatore ai sensi del § 273 BGB (Codice civile tedesco) è escluso per quanto riguarda i dati da trattare e i relativi supporti di memoria.

(4) Non esistono accordi collaterali orali tra le parti. Qualsiasi modifica, integrazione o risoluzione del presente accordo richiede la forma scritta per la sua validità, dalla quale si può derogare solo per iscritto. Il requisito della forma scritta è soddisfatto mediante una firma apposta con almeno una firma elettronica semplice registrata tramite software di firma elettronica. Alla firma elettronica è riconosciuto pieno valore probatorio.

(5) Nel caso in cui altri accordi al momento della stipula del presente contratto contengano disposizioni divergenti o contraddittorie, prevarrà il contenuto del presente contratto.

(6) I seguenti allegati costituiscono parte integrante dell'accordo:

- Allegato 1 "Informazioni sul trattamento"
- Allegato 2 "Misure tecniche e organizzative"
- Allegato 3 "Subappaltatori"

Società:	
Indirizzo	
Data:	
Luogo:	
Nome:	
Firma del Titolare del trattamento	

Società:	Shiftmove GmbH
Indirizzo	Warschauer Str. 57, 10243 Berlin
Data:	15.09.2025
Luogo:	Berlin
Nome:	i.V. John Maik Ryssel
Signed by: i.V. John Maik Ryssel 4ABB00F788844C5...	
Firma dell'Incaricato del trattamento	

Allegato 1

Informazioni sul trattamento

Le informazioni riportate di seguito riguardanti l'oggetto e la finalità del trattamento, le tipologie di trattamento, le categorie di persone interessate e le categorie di dati personali trattati si riferiscono all'intera gamma potenziale di funzionalità dei servizi offerti dal Responsabile del trattamento. Sono vincolanti esclusivamente quelle finalità, tipologie di trattamento, categorie di interessati e categorie di dati che risultano dal contratto principale, inclusa la relativa Order Form concordata, e che sono necessarie per i prodotti e le funzioni effettivamente ordinati dal Titolare del trattamento.

a) Oggetto e finalità del trattamento

L'oggetto dell'incarico è la fornitura di uno o più dei seguenti servizi come Software as a Service:

- Software per la gestione della flotta (Avrios) con le seguenti finalità:
  - Gestione di veicoli e conducenti
  - Gestione delle multe
  - Gestione delle carte carburante
  - Gestione dei sinistri
  - Controllo delle patenti di guida
  - Elaborazione di resoconti e analisi

- Localizzazione in tempo reale e documentazione del percorso (Vimcar Fleet Geo) con le seguenti finalità:
  - Localizzazione in tempo reale dei veicoli
  - Documentazione del percorso dei veicoli
  - Notifica di geo-fencing per i veicoli

- Registro di bordo elettronico con le seguenti finalità:
  - Documentazione del percorso dei veicoli
  - Esportazione dei dati del registro di bordo

b) Tipo di trattamento

Nell'ambito dell'incarico, l'Incaricato del trattamento effettuerà i seguenti tipi di trattamento ai sensi dell'art. 4 n. 2 RGPD: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento, modifica, recupero, consultazione, trasferimento, limitazione, cancellazione e distruzione dei dati.

c) Categorie di interessati e dati personali

Durante la fornitura dei servizi, i dati personali delle seguenti categorie di soggetti possono essere regolarmente trattati:

1) Conducenti (ex e attuali dipendenti e loro coniugi e familiari a carico, attuali appaltatori nonché candidati e futuri dipendenti)
2) Utenti (utenti [diversi dai conducenti] autorizzati dal Cliente a utilizzare i servizi)
3) Terzi (committenti, partner commerciali, fornitori, consulenti, rappresentanti, liberi professionisti e/o subappaltatori del Cliente [persone fisiche])

d) Tipo di dati trattati

Quando si utilizzano i nostri prodotti, vengono trattate le seguenti categorie di dati, a seconda dell'ambito e dell'uso individuale:

Gestione della flotta Avrios:

- Mansioni e commenti
- Informazioni sulle multe (destinatario, importo, foto)
- Data di inizio e di fine
- Informazioni sul veicolo (emissioni di CO2, rapporti sui danni, targa, numero di telaio)
- Fotografie (fotografie di patenti e fototessere)
- Informazioni sulle patenti di guida
- Informazioni di contatto (numero di telefono, numero di fax, numero di cellulare, indirizzo e-mail)
- Storico delle comunicazioni (storico delle e-mail con fornitori, prestatori di servizi, compagnie assicurative, ecc.)
- Dati anagrafici (nome, cognome, indirizzo, genere, data e luogo di nascita, lingua, nazionalità, permesso di soggiorno, stato civile, dati dei parenti, numero di identificazione nazionale)
- Dati gestionali dell'azienda (ID interno, centro di costo, organizzazione, reparto, sede, settore e sottosettore, struttura di reporting)
- Informazioni sulla pianificazione salariale (benefit relativi alle auto aziendali), capitolati di servizio e informazioni correlate (diritto all'auto aziendale e relativa classe)
- Informazioni sulla carta carburante (fornitore, costi, data, prodotto)
- Risultati dei test della normativa antinfortunistica

- Dati sui dispositivi e sull'utilizzo delle tecnologie informatiche

Vimcar Fleet Geo:

- Nome, cognome
- Indirizzo e-mail, numero di telefono, numero di cellulare
- Dati del registro di bordo
- Dati di viaggio
- Localizzazione in tempo reale e documentazione del percorso
- VIN (numero di identificazione del veicolo)
- Parametri di prova per il controllo automatizzato della patente di guida (facoltativi se si utilizza il controllo della patente di guida)
- Dati tecnici del veicolo (ad es. stato di riparazione), fotografie dei veicoli (facoltative se si utilizza la gestione dei sinistri)
- Dati sui dispositivi e sull'utilizzo delle tecnologie informatiche

Vimcar Registro di bordo:

- Nome, cognome
- Indirizzo e-mail, numero di telefono, numero di cellulare
- Dati del registro di bordo
- Dati di viaggio
- Punto di partenza e di arrivo dei viaggi
- Chilometri percorsi
- Categorizzazione dei viaggi privati e di lavoro
- Dati di contatto e indirizzo
- VIN (numero di identificazione del veicolo)
- Parametri di prova per il controllo automatizzato della patente di guida (facoltativi se si utilizza il controllo della patente di guida)
- Dati tecnici del veicolo (ad es. stato di riparazione), fotografie dei veicoli (facoltative se si utilizza la gestione dei sinistri)
- Dati sui dispositivi e sull'utilizzo delle tecnologie informatiche

Allegato 2

Misure tecniche e organizzative ai sensi dell'art. 32 del GDPR. 32 (1) GDPR

1. Misure per garantire la riservatezza

1.1 Controllo degli ingressi

Ha lo scopo di impedire alle persone non autorizzate di accedere fisicamente ai sistemi di elaborazione dati. Misure per la sicurezza degli edifici e dei locali.

- Concetto di sicurezza dell'edificio (documentato)
- Sistema di chiusura
- Finestre e porte antieffrazione
- Servizio di sicurezza esterno
- Sistema di allarme
- Collegamento tra sistema di allarme e servizio di sicurezza/polizia
- Barriere luminose/rilevatori di movimento
- Collegamento dei rilevatori di movimento al servizio di sicurezza/polizia
- Sorveglianza TVCC
- Concetto di controllo degli accessi
- Controllo biometrico degli accessi
- Verifica delle persone al gatekeeper/alla reception
- Registrazione degli accessi dei visitatori / libro dei visitatori / badge dei visitatori
- Supervisione personale delle persone esterne nelle aree di sicurezza
- Badge identificativi
- Carte elettroniche con codice di accesso/trasponder di accesso
- Zone di sicurezza (riunioni dei visitatori, sale server, posti di lavoro, ricerca)
- Esistenza di una panoramica delle autorizzazioni per le zone di sicurezza
- Utilizzo di porte a chiusura automatica quando le zone vengono attraversate
- Carte di autorizzazione (per le singole zone)
- Regolamenti chiave
- Ingresso protetto separato per gli arrivi e le partenze
- Accesso separato e protetto alla sala server
- Accesso separato e protetto al centro informatico
- Scelta accurata del personale addetto alle pulizie
- Istruzioni di lavoro/linee guida relative alla chiusura dei locali quando si lascia/finisce il lavoro

1.2 Controllo degli accessi

Finalizzato a prevenire l'accesso e l'utilizzo non autorizzato dei sistemi di elaborazione dati. Sicurezza del sistema.

- Concetto di sicurezza basato sui ruoli/ assegnazione dei diritti degli utenti
- Creazione di profili utente
- Gestione delle autorizzazioni
- Evitare gli identificatori di gruppo
- Processo documentato per l'assegnazione dei diritti quando i nuovi dipendenti entrano a far parte dell'organizzazione.
- Processo documentato per la revoca dei diritti quando i dipendenti cambiano reparto
- Processo documentato per la revoca dei diritti quando i dipendenti lasciano l'azienda
- Assegnazione funzionale e/o limitata nel tempo delle autorizzazioni agli utenti
- Uso di password individuali
- Accesso con nome utente e password
- Accesso con dati biometrici
- Password BIOS separata
- Blocco automatico dello schermo protetto da password dopo l'inattività (screen saver)
- Schermate di privacy per la visualizzazione di eventuali immagini non autorizzate
- Politica sulle password con requisiti minimi di complessità della password:
    - Minimo 8 caratteri
    - Minimo 12 caratteri per le password di amministrazione locale
    - Maiuscole e minuscole, caratteri speciali, numeri (di cui almeno 4 criteri)
    - Prevenzione di password banali (ad esempio, password1, password2, 123456, qwerty).
    - Cronologia delle password (nessun riutilizzo delle ultime password)
    - Prevenzione della PW dopo una corrispondenza positiva con i dizionari
    - Limitazione dell'input di alcuni caratteri speciali per prevenire le iniezioni SQL.
    - Procedura di reset della PW adeguatamente sicura
- Ciclo di modifica delle password:
- Intervallo di tempo tra i tentativi di login
- I tentativi di accesso falliti vengono visualizzati agli utenti
- Blocco automatico degli account utente dopo più inserimenti errati di PW
- Blocco delle password dopo un incidente di sicurezza e riassegnazione
- Blocco delle password in caso di sospetta violazione
- Implementazione in gran parte automatica (tecnica) della politica delle password
- Autenticazione a due o più fattori per i processi ad alto rischio
- Salvataggio delle password nel browser solo con la master password
- L'accesso ai siti web è gestito in modo restrittivo
- Altro: (ad esempio, utilizzo di Fido2)
- Hashing delle password memorizzate con metodi di hashing aggiornati:
    - Metodo di hashing utilizzato:

    - Gli hash sono “salati” e/o “pepati”.
- Crittografia delle reti
    - Algoritmi di crittografia utilizzati: SSH, HTTPS, TLS 1.2+,
- Blocco delle apparecchiature di elaborazione dati (ad es. gabbia chiusa per i server).
- Disattivazione dell'avvio automatico dei supporti esterni.
- Controllo del programma e procedure di rilascio per le nuove installazioni
- Impedire l'esecuzione di software scaricato i cui sorgenti sono contrassegnati come insicuri.
- Impedire l'esecuzione automatica di programmi provenienti da download temporanei.
- Utilizzo di sistemi di prevenzione delle intrusioni
- Utilizzo di tecnologie VPN
- Utilizzo di software antivirus: server
- Utilizzo di software antivirus: client
- Utilizzo di un firewall software
- Utilizzo di un firewall hardware
- Raccolta centralizzata degli avvisi di malware
- Modifica delle informazioni di autenticazione predefinite dopo l'installazione del software/il primo login
- Gestione centrale dei dispositivi
- Gestione dei dispositivi mobili
- Per gli smartphone: accesso solo dopo l'autenticazione
- Per smartphone: Utilizzo di metodi di accesso biometrici solo con memorizzazione esclusivamente locale dei modelli biometrici (all'interno di chip sicuri)
- Per smartphone: fonti sicure per le app, le app sono testate e approvate
- Conservazione dei dati personali/dei supporti di dati in armadi di sicurezza con serratura o in locali protetti separatamente.
- Politica sull'home office / telelavoro
- Politica sull'utilizzo privato delle apparecchiature o esclusione dell'utilizzo privato
- Altre misure:
    - Password diverse per servizi diversi o SSO
    - Utilizzo di un gestore di password

1.3 Controllo degli accessi

Deve impedire attività non autorizzate nei sistemi di elaborazione dati al di fuori delle autorizzazioni concesse.

- Utilizzo di un concetto di autorizzazione
- Uso minimo di account di amministratore
- Ruoli amministrativi diversi in base al concetto di minor privilegio (utenti, firewall, backup ecc.)
- Superutente (ad es. root in Linux) non utilizzato per quanto possibile.
- Regolamentazione che vieta di navigare in Internet o di leggere/inviare e-mail utilizzando i privilegi di amministratore.

- Utilizzo di dispositivi finali di amministrazione propri (connessione di rete dedicata)
- Separazione tra approvazione dell'autorizzazione (organizzativa) e assegnazione dell'autorizzazione (tecnica).
- Invio di dati telemetrici ai produttori disattivato
- Regolamento per il ripristino dei dati dai backup (chi, quando, su richiesta di chi)
- Conservazione dei backup dei dati (ad es. nastri, CD) in una cassaforte protetta dall'accesso.
- Revisione regolare dei ruoli e delle autorizzazioni
- Limitazione dell'interrogazione libera e incontrollata dei database
- Accesso parziale ai database e alle funzioni (lettura, scrittura, esecuzione)
- Valutazione regolare dei log (file di log)
- Limitazione temporale delle possibilità di accesso
- Disattivazione dei servizi standard del server non utilizzati
- Registrazione a livello di firewall per rilevare gli accessi non autorizzati tra le reti
- Notifiche automatiche quando si sospetta un'elaborazione non autorizzata
- Registrazione degli accessi di manutenzione remota
- Registrazione degli accessi ai file
- Registrazione delle cancellazioni di file
- Registrazione delle modifiche ai file
    - Filtro SPAM
- Rilevamento delle intrusioni (IDS)
    - Software di gestione delle informazioni e degli eventi di sicurezza (SIEM)
- Prevenzione delle intrusioni (IPS)
- Accesso limitato ai file di log (solo Log Admin)
- Archiviazione dei file di log su un server LogFile dedicato
- Archiviazione criptata dei dati
- algoritmi di crittografia utilizzati:
    - AES (128/256 bit)
    - 3DES
    - RSA (1024/2048 bit)
    - EC (256 bit)
    - Altro: AES 256 AWS a riposo Verschlüsselung
- Funzione di hash utilizzata:
    - SHA2 (256, 384, 512 bit)
    - SHA3
    - bcrypt
- Altri metodi:
    - Gli hash sono “salati” (salt) o “pepati” (pepper)
- Autenticazione a due fattori per la manutenzione del server web
- Certificati SSL solo da fonti affidabili
- Distruzione controllata dei dati:
    - Smaltimento dei supporti di dati - cancellazione sicura dei supporti di dati (DIN 66399)
    - Distruggidocumenti (Cross-Cut, mindestens Stufe 3, DIN 66399)

    - Contenitori metallici sigillati (i cosiddetti bidoni della spazzatura per la protezione dei dati)
    - Algoritmo di Peter Gutmann - sovrascrittura di 35 volte
    - Distruzione fisica (ad es. trituratore per particelle di dimensioni fino a max. 1000 millimetri quadrati)
    - Smagnetizzazione tramite distruzione termica (riscaldamento della superficie del disco magnetico oltre la temperatura di Curie del rivestimento utilizzato)
    - Smagnetizzazione per mezzo di un degausser
- Connessione di filiali o uffici domestici solo tramite connessioni VPN con autenticazione del certificato del cliente
- Utilizzo della WLAN solo su router attuali con meccanismi di accesso efficaci
- Accesso ospite WLAN senza accesso alla rete interna
- Politica di distruzione dei dati
- Politica di pulizia della scrivania
- Controllo della posta elettronica in arrivo tramite anti-malware
- Concetto di sicurezza per la gestione di stampanti, fotocopiatrici, ecc.
- Altre misure:
    - Archiviazione delle chiavi tramite moduli di sicurezza hardware

2. 2 Misure per garantire l'integrità

2.1 Controllo del trasferimento

Garantire la sicurezza dei dati durante la trasmissione elettronica e il trasporto dei dati e la verificabilità del trasferimento.

- Come vengono trasmessi i dati tra il controllore e le terze parti?
    - Connessione VPN
    - Protocollo di trasferimento sicuro dei file (sftp)
    - Connessione Citrix
- Crittografia della posta elettronica:
    - SMIME
    - OpenPGP
    - Invio di e-mail con file ZIP crittografati
- Per i messenger: crittografia del trasporto e del contenuto
- Scambio di dati tramite connessione https
- Protocollo di crittografia utilizzato:
    - TLS 1.2
    - TLS 1.3
- Algoritmi di crittografia utilizzati:
    - AES (128/256 bit)
    - 3DES

    - RSA (1024/2048 bit)
    - Diffie-Hellmann
- Utilizzo della procedura di firma
- Procedura di firma utilizzata:
    - RSA
    - ElGamal
    - DSA
- Firma digitale delle macro
- Nessuna trasmissione di dati personali (ad es. indirizzo di posta elettronica) tramite richiesta HTTP GET, in quanto tali dati vengono memorizzati nei file di log del server web e possono essere deviati dai tracker dei siti web utilizzati.
- Per HTTPS: utilizzo di certificati client
- Richieste criptate ai servizi DNS
- Regolamentazione dell'uso dei servizi cloud (compresa la strategia di uscita)
- Gestione documentata dei supporti di dati, controllo dell'inventario
- Crittografia dei record di dati riservati
- Crittografia dei supporti di dati mobili (ad es. dischi rigidi di laptop, dischi rigidi esterni, chiavette USB)
- Divieto di trasportare borse e altri bagagli e telefoni cellulari nelle aree di sicurezza.
- Regolamento per la creazione di copie di registri di dati
- Esecuzione di copie di backup dei supporti di dati che devono essere trasportati
- Documentazione degli uffici a cui è destinata la trasmissione e dei mezzi di trasmissione
- Raccolta diretta, servizio di corriere, scorta di trasporto
- Controllo di completezza e correttezza

2.2 Controllo degli ingressi

Lo scopo è quello di garantire che sia possibile rintracciare se, chi e quando i dati personali sono stati inseriti nei sistemi di elaborazione dati, modificati o cancellati.

- Registrazione tecnica dell'inserimento, della modifica e della cancellazione dei dati.
- Valutazione manuale o automatizzata dei log
- Autorizzazioni differenziate per gli utenti:
    - Nomi di utenti individuali, nessun gruppo di utenti
    - Assegnazione dei diritti di inserimento, modifica e cancellazione dei dati in base a un concetto di autorizzazione
    - Accesso al campo per i database
- Definizione organizzativa delle responsabilità di inserimento
- Impegno alla segretezza dei dati
- Concetto di log che va oltre lo standard OS
- Server di log dedicato
- Regolamentazione delle autorizzazioni di accesso ai server di log (LogAdmin)
- Regolamentazione dei periodi di conservazione per scopi di verifica/prova.

3. Misure per garantire la disponibilità e la resilienza

3.1 Controllo della disponibilità

Progettato per proteggere i dati dalla distruzione o dalla perdita accidentale.

- Sistemi di allarme antincendio nelle sale server
- Rilevatori di fumo nelle sale server
- Porte antincendio
- Sistemi antincendio senza acqua nelle sale server
- Sensori d'acqua nelle sale server
- Protezione da fulmini e sovratensioni
- Sale server climatizzate
- Sale server in compartimento antincendio separato
- Stoccaggio dei sistemi di backup in locali separati e in un compartimento antincendio separato
- Sale server non sotto o accanto a servizi igienici
- Accesso alle sale server limitato al solo personale necessario
- Segnale di allarme in caso di accesso non autorizzato alle sale server
- Stoccaggio dei supporti di archiviazione nelle condizioni di stoccaggio necessarie (aria condizionata, requisiti di protezione, ecc.)
- estintori a CO2 nelle immediate vicinanze delle sale server
- Sistema UPS (gruppo di continuità)
- Generatore di corrente
- Armadi ignifughi
- Cassaforte per la protezione dei dati
- Concetto di protezione e backup dei dati documentato
- Esecuzione di backup dei dati e creazione di copie di sicurezza secondo il principio 3-2-1
- Archivio di emergenza (outsourcing dei dati)
- Test regolari per il ripristino dei dati
- Almeno un sistema di backup non può essere criptato da codice maligno
- Mirroring dei dischi rigidi (ad es. RAID)
- Partizioni separate per sistema operativo e dati
- Piano di emergenza in atto (standard BSI 200-4)
- Revisione regolare del piano di emergenza attraverso test ed esercitazioni di emergenza.
- Garantire la leggibilità tecnica a lungo termine dei supporti di memorizzazione di backup.

3.2 Resilienza (resilienza e controllo dei guasti)

Deve consentire ai sistemi di far fronte ai cambiamenti legati al rischio e di dimostrare tolleranza e capacità di compensazione di fronte alle interruzioni.

- Alimentazione ridondante
- Connessione dati ridondante
- Aria condizionata ridondante
- Disponibilità di data center di backup (stand-by a caldo o a freddo?): Freddo
- altri sistemi/procedure ridondanti:
- Utilizzo di una soluzione SAN (Storage Area Network) ad alta disponibilità.
- Team di risposta alle emergenze informatiche (CERT)
- Uso del bilanciamento del carico
- Delimitazione dei componenti critici
- Esecuzione di test di penetrazione
- Irrigidimento del sistema (disattivazione dei componenti non necessari)
- Attivazione immediata e regolare degli aggiornamenti software e firmware disponibili.
- Controllo regolare della configurazione dei firewall
- Sensibilizzazione regolare dei dipendenti (almeno annualmente)
- Il processo per la segnalazione immediata degli incidenti all'IT è noto a tutti i dipendenti.

4. Misure per il riesame, la valutazione e l'analisi regolari

4.1 Procedure di controllo

Garantire l'efficacia delle misure di sicurezza dei dati

- Gli elenchi dei trattamenti (art. 30 I e II DSGVO) vengono aggiornati annualmente.
- Notifica di nuove/modificate procedure di trattamento dei dati al responsabile della protezione dei dati
- Notifica delle procedure di trattamento dei dati nuove/modificate al responsabile della sicurezza informatica.
- I processi per la segnalazione di nuove/modificate procedure sono documentati
- Revisione e valutazione periodica del software utilizzato
- I concetti e la documentazione sono rivisti regolarmente (ciclo PDCA)
- Revisione dell'efficacia delle misure di sicurezza adottate almeno una volta all'anno.
- Esecuzione di test di sicurezza sulle applicazioni web secondo le procedure di buona pratica (ad esempio, OWASP Testing Guide).
- Se durante la suddetta revisione vengono riscontrati dei risultati, le misure di sicurezza vengono adeguate in base al rischio.
- Esiste un processo per rispondere alle violazioni della sicurezza (attacchi) e ai malfunzionamenti del sistema (gestione della risposta agli incidenti).

- Documentazione degli incidenti di sicurezza
- Certificazioni di sicurezza (ISO 27001, BSI IT-Grundschutz, ISIS12 ecc.)
- Utilizzo di informazioni sulla sicurezza (analisi in tempo reale; gestione dei log, SIEM, NBAD, network forensics).

4.2 Controllo degli ordini

Garantire che i dati elaborati per conto dei fornitori di servizi (subappaltatori) siano trattati solo in conformità alle istruzioni del committente.

- Progettazione del contratto in conformità ai requisiti di legge (art. 28 DSGVO)
- Registrazione centrale dei fornitori di servizi esistenti (gestione uniforme dei contratti).
- Controlli precontrattuali presso la sede dell'appaltatore prima dell'inizio del contratto
- Controlli regolari presso la sede dell'appaltatore dopo l'inizio del contratto (durante la durata del contratto)
- Ispezioni in loco presso i locali dell'appaltatore
- Revisione del concetto di sicurezza dei dati dell'appaltatore
- Revisione dei certificati di sicurezza informatica dell'appaltatore.
- L'appaltatore ha nominato un responsabile della protezione dei dati

4.3 Controllo della separazione

I dati raccolti per scopi diversi devono essere trattati separatamente.

- Separazione dei client (capacità multi-client del sistema utilizzato).
- Separazione fisica dei dati (ad es. sistemi o supporti di dati diversi).
- Separazione logica dei dati (ad esempio, in base al numero di clienti o di clienti).
- Backup dei dati dei clienti su supporti separati (senza dati di altri clienti).
- Concetto di autorizzazione che tenga conto dell'elaborazione separata dei dati dei clienti da quelli di altri clienti.
- Separazione dei sistemi di sviluppo, test e produzione
- Assegnazione dei record di dati agli attributi di scopo
- Per i dati pseudonimizzati: Separazione del file di assegnazione e memorizzazione su un sistema diverso.

4.4 Altri tipi di gestione della protezione o della sicurezza dei dati

- Struttura organizzativa appropriata per la sicurezza delle informazioni con ruoli chiaramente definiti
- Nomina di un responsabile della sicurezza informatica
- Utilizzo di un software di gestione della protezione dei dati

- Responsabile della protezione dei dati nominato
- Processo documentato per la gestione degli incidenti di sicurezza informatica
- Processo documentato per la gestione degli incidenti relativi alla protezione dei dati
- Responsabilità chiare per la gestione degli incidenti di protezione dei dati e di sicurezza
- Processo documentato per garantire i diritti degli interessati
- Archiviazione centrale di politiche/processi/istruzioni procedurali accessibili a tutti i dipendenti
- Le linee guida/processi/istruzioni procedurali sono comunicate all'interno dell'azienda e conosciute da tutti i dipendenti.
- I fornitori di servizi esterni sono tenuti al segreto, se necessario.
- Disposizioni per la cancellazione effettiva dei dati sull'hardware ritirato dal produttore o dal fornitore di servizi.
- Formazione regolare sulle linee guida e sui processi di sicurezza

Allegato 3

Subappaltatori

Il Titolare del trattamento ha autorizzato l'utilizzo dei seguenti subappaltatori:

1

Nome: Vimcar GmbH

Indirizzo: Warschauer Str. 57, 10243 Berlino, Germania

Contatti: datenschutz@vimcar.com

Paese terzo: No

Finalità:

- Fornitura e sviluppo dei sistemi SaaS Vimcar registro di bordo e Vimcar Fleet Geo
- Assistenza clienti
- Spedizione

2.

Nome: Avrios International AG

Indirizzo: Riesterstr. 6, 8002 Zurigo, Svizzera

Contatti: privacy@avrios.com

Paese terzo: Sì

Garanzia: Decisione di adeguatezza della Commissione UE, art. 45 RGPD

Finalità:

- Fornitura del sistema SaaS di gestione della flotta Avrios
- Assistenza clienti