

Matrice delle Responsabilit  Condivise

SIK SISTEMI S.r.l. vs. Clienti – Prodotti DDD Manager, DDD Police, Centraline DDD Box, Terminali di Scarico

Versione 1.1 – Documento Pubblico – Conformit  ISO/IEC 27001:2022, ISO/IEC 27017, ISO/IEC 27018 e GDPR

1. Informazioni sul Documento

Titolo	Matrice Responsabilit� Condivise – SIK SISTEMI vs Clienti
Prodotti trattati	DDD Manager, DDD Police, Centraline DDD Box, Terminali di Scarico (DDD Terminal)
Versione	1.1
Data emissione	21/05/2026
Data revisione	19/05/2026
Redatto da	[Responsabile SGSI / Resp. IT – Gianluca Roveda, resp. R&D]
Approvato da	[DPO / Legale Rappresentante – Yuri Merli, Legale rappresentante]
Classificazione	Documento Pubblico – Distribuzione esterna autorizzata
Standard di riferimento	ISO/IEC 27001:2022 (SGSI) – ISO/IEC 27017:2015 (Servizi cloud) – ISO/IEC 27018:2019 (PII in public cloud)
Riferimenti normativi	Reg. UE 2016/679 (GDPR) – D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018 – L. 300/1970 art. 4 (Statuto dei Lavoratori) – Reg. UE 165/2014 – Reg. CE 561/2006 – D.D. 215/2016 – art. 174 Codice della Strada

2. Scopo e principio del documento

Il presente documento definisce la ripartizione delle responsabilit  operative, normative e in materia di protezione dei dati personali tra SIK SISTEMI S.r.l. e i propri clienti, con riferimento ai prodotti e servizi erogati.

Il modello adottato si ispira al principio di responsabilit  condivisa (Shared Responsibility Model) secondo cui alcune responsabilit  sono integralmente in capo a SIK SISTEMI, altre sono interamente del cliente, e altre ancora sono condivise tra le due parti in ambiti distinti. Il documento attua il controllo CLD.6.3.1 di ISO/IEC 27017.

I clienti di SIK SISTEMI si suddividono in due categorie principali:

- **Aziende di autotrasporto** (clienti DDD Manager, DDD Box, DDD Terminal): utilizzano i prodotti per adempiere agli obblighi di scarico, archiviazione e analisi dei dati tachigrafici previsti dal Reg. UE 165/2014 e dal Reg. CE 561/2006.
- **Organi di controllo su strada** – Polizia Stradale e Locale (clienti DDD Police): utilizzano il software e l'hardware fornito per effettuare controlli sui dati tachigrafici in modo rapido, equo e conforme alla normativa.

3. Legenda Tipologie di Responsabilità

Tipo	Significato
SIAK SISTEMI	La responsabilità è integralmente in capo a SIAK SISTEMI S.r.l. Il cliente non ha obblighi specifici per questo ambito.
Condiviso	La responsabilità è divisa: SIAK SISTEMI e il cliente hanno ciascuno un ambito specifico di competenza sullo stesso aspetto.
Cliente	La responsabilità è integralmente in capo al cliente. SIAK SISTEMI fornisce strumenti ma non interviene.

Nota: Le righe evidenziate con fondo color arancio chiaro nella sezione 4 indicano voci **nuove o sostanzialmente reVISIONATE** rispetto alla versione 1.0 del documento.

4. Localizzazione dei dati e sub-fornitori

SIAK SISTEMI dichiara le seguenti informazioni rilevanti ai sensi degli artt. 7.5.1 e 9.3.3 di ISO/IEC 27018:

Voce	Informazione
Localizzazione dati	Tutti i dati personali e operativi sono archiviati e trattati nello Spazio Economico Europeo, su infrastruttura Amazon Web Services regione eu-west-1 (Dublino, Irlanda).
Sub-responsabili attivi	Amazon Web Services Inc. – fornitore di infrastruttura cloud (IaaS/PaaS) – certificato ISO/IEC 27001, 27017, 27018, SOC 2 Type II.
Notifica modifiche sub-resp.	Modifiche all'elenco dei sub-responsabili sono comunicate al Cliente con preavviso scritto di almeno 30 giorni, con facoltà di opposizione entro 20 giorni (cfr. art. 17.7 del contratto Remote Assistance).
Trasferimenti extra-SEE	Non sono previsti trasferimenti di dati al di fuori dello SEE. Eventuali variazioni saranno comunicate con preavviso non inferiore a 60 giorni e accompagnate dalle garanzie ex artt. 44 e ss. GDPR (es. SCC).
Strumenti per audit del cliente	Su richiesta scritta del Cliente con preavviso minimo di 30 giorni e non più di una volta all'anno, SIAK rende disponibili: (i) certificati ISO vigenti; (ii) sintesi non confidenziale del più recente penetration test; (iii) attestazioni del sub-fornitore cloud.

5. Matrice delle Responsabilità per Prodotto

La tabella seguente riporta, per ciascun prodotto e ambito funzionale, il tipo di responsabilità e le azioni specifiche richieste a ciascuna parte. Le righe contrassegnate dal marker NUOVO sono state aggiunte nella versione 1.1.

Ambito / Funzionalità	Tipo	Responsabilità SIAK SISTEMI	Responsabilità Cliente	Riferimenti normativi e ISO
DDD MANAGER – Piattaforma web gestione dati tachigrafici (clienti: aziende di autotrasporto)				
Piattaforma web: disponibilità e infrastruttura	SIAK SISTEMI	Garantisce l'erogazione del servizio web, la disponibilità della piattaforma, gli aggiornamenti software, la manutenzione dei server di archiviazione e la disponibilità dell'accesso da PC, tablet e smartphone. I livelli di servizio puntuali sono definiti in apposito allegato SLA (in fase di definizione).	Dispone di una connessione internet funzionante. Non è responsabile di eventuali interruzioni del servizio imputabili all'infrastruttura SIAK SISTEMI.	ISO 27001 A.5.30 – ISO 27017 CLD.9.5.1
Archiviazione file DDD su server	SIAK SISTEMI	Conserva i file DDD su server sicuri e dedicati nell'ambiente AWS eu-west-1. Garantisce la conservazione per il periodo concordato (2 anni Light/Silver, 5 anni Gold). Assicura backup periodici su sistemi separati e integrità dei dati.	Non è responsabile della conservazione fisica dei file sul proprio hardware locale, in quanto la conservazione è delegata a SIAK SISTEMI.	Reg. UE 165/2014 art. 36 – ISO 27001 A.8.13 – GDPR art. 32
Integrazione con servizi terzi di scarico/trasmisione dati	Condiviso	Gestisce la ricezione e l'archiviazione dei file DDD trasmessi da servizi terzi integrati con DDD Manager (Nextcloud, Volvo Dynafleet, Webfleet, Jaltest, Satelicom...). I dati, una volta ricevuti, sono conservati e gestiti sui server SIAK SISTEMI.	È responsabile della corretta configurazione e gestione del servizio terzo di scarico/trasmisione, del consenso all'integrazione e della verifica che i dati trasmessi siano completi e integri.	ISO 27001 A.5.19/5.20 – ISO 27017 CLD.6.3.1
Anagrafiche conducenti e veicoli	Condiviso	Fornisce lo strumento per l'inserimento e la gestione delle anagrafiche. Garantisce la sicurezza e la riservatezza dei dati inseriti tramite controlli di accesso e cifratura at-rest.	È responsabile dell'inserimento accurato, dell'aggiornamento e della correttezza delle anagrafiche di conducenti e veicoli nel sistema. Quale Titolare, garantisce la liceità del trattamento.	GDPR artt. 5, 24 – ISO 27018 A.7.2.1
Notifiche scadenze (patenti, CQC, scarichi, calibrature)	Condiviso	Genera e invia le notifiche automatiche configurate (scadenze patenti, CQC, revisioni, calibrazioni, scadenze scarico). Mantiene il sistema di notifiche sempre aggiornato.	È responsabile di agire sulle notifiche ricevute: provvedere alle revisioni, agli scarichi entro le scadenze, al rinnovo delle certificazioni dei conducenti.	Reg. UE 165/2014 – D.D. 215/2016
Generazione report (attività, infrazioni, scadenziari)	Condiviso	Produzione reportistica finalizzata al controllo dei conducenti, buste paga e adempimento obblighi Reg. CE 561/2006, sulla base dei dati presenti nell'archivio.	È responsabile della lettura e comprensione dei report generati, della contestazione delle infrazioni ai conducenti entro i termini, della conservazione delle lettere infrazione firmate per almeno 1 anno.	Reg. CE 561/2006 – D.D. 215/2016 art. 7
Accesso alla piattaforma – credenziali	Condiviso	Fornisce le credenziali di accesso e provvede alla loro disattivazione su segnalazione del cliente. Garantisce la sicurezza dell'autenticazione lato server (cifratura delle password, controlli sui tentativi falliti, logging degli accessi).	È responsabile della custodia e della riservatezza delle credenziali di accesso, della gestione degli utenti abilitati, della revoca degli accessi non più autorizzati e dell'utilizzo di password robuste.	ISO 27001 A.5.16/A.8.5
Correttezza e completezza dei dati analizzati	Cliente	Elabora i dati ricevuti dai dispositivi di scarico secondo gli algoritmi di calcolo aggiornati alla normativa vigente. Non verifica la completezza degli scarichi effettuati dal cliente.	È responsabile di garantire che tutti gli scarichi siano effettuati nei tempi previsti dalla legge e che i dati caricati in piattaforma siano completi e non alterati.	Reg. UE 165/2014 – D.D. 215/2016

Ambito / Funzionalità	Tipo	Responsabilità SIAK SISTEMI	Responsabilità Cliente	Riferimenti normativi e ISO
Utilizzo dei report a fini legali e sanzionatori	Cliente	Mette a disposizione la generazione di report redatti ai sensi della normativa. Non è parte in causa in eventuali procedimenti sanzionatori.	È responsabile dell'utilizzo dei report ai fini della contestazione agli autisti, della firma e conservazione delle ricevute, e delle eventuali decisioni aziendali conseguenti.	Codice Civile – D.D. 215/2016
DDD POLICE – Software e hardware (tablet) per il controllo su strada (clienti: organi di Polizia Stradale e Locale)				
Software di analisi su strada – erogazione e aggiornamento	SIAK SISTEMI	Sviluppa, mantiene e aggiorna il software DDD Police, garantendo l'allineamento con la normativa vigente (Reg. UE 165/2014, 561/2006, CdS). Fornisce supporto tecnico e legale da remoto agli agenti.	Non è responsabile degli aggiornamenti software. Gli aggiornamenti avvengono automaticamente.	ISO 27001 A.8.25 – A.8.32
Lettura e analisi dei dati del tachigrafo in sede di controllo	Condiviso	Fornisce lo strumento per la lettura dei file DDD e la generazione dei report di controllo. Il software guida l'agente attraverso le fasi di verifica.	È responsabile dell'esecuzione materiale del controllo su strada, dell'inserimento corretto dei dati del conducente e del veicolo, della corretta interpretazione dei report generati e della verifica delle infrazioni segnalate dal software.	Reg. UE 165/2014 – CdS art. 174
Generazione fac-simile di verbale e ciclo sanzionatorio	Cliente	Fornisce la funzionalità di generazione di un fac-simile di verbale precompilato con i dati rilevati. SIAK non è responsabile del contenuto dell'atto eventualmente emesso.	La gestione dell'intero ciclo sanzionatorio è responsabilità esclusiva dell'agente: decisione di sanzionare, verifica e validazione dei dati precompilati, redazione e firma dell'atto ufficiale, notifica al trasgressore e tutti gli effetti amministrativi e legali conseguenti.	CdS – L. 689/1981
Conservazione dei dati del controllo	Condiviso	Conserva i dati di ogni sessione di controllo nel cloud per il periodo impostato per quel controllo (default 12 mesi, modificabile dall'agente). Garantisce la sicurezza e la riservatezza dei dati durante il periodo di conservazione.	Imposta il periodo di conservazione per ogni singolo controllo. È responsabile dell'eliminazione esplicita dei dati che non intende conservare e della conservazione degli atti ufficiali secondo le disposizioni interne del proprio comando.	GDPR art. 5(1)(e) – ISO 27018 A.11.1
Fornitura e configurazione hardware (tablet)	SIAK SISTEMI	Fornisce il tablet preconfigurato con il software DDD Police installato e sempre aggiornato. Garantisce la compatibilità hardware/software e si occupa della configurazione iniziale del dispositivo prima della consegna.	È responsabile della custodia del dispositivo ricevuto, del suo corretto utilizzo in sede di controllo e della segnalazione a SIAK SISTEMI di eventuali danni o malfunzionamenti.	ISO 27001 A.7.9 – A.8.1
Aggiornamenti software DDD Police sul tablet	SIAK SISTEMI	Rilascia e distribuisce gli aggiornamenti del software DDD Police (nuove versioni, allineamenti normativi, correzioni). Garantisce che il tablet riceva gli aggiornamenti software.	Non deve modificare, disinstallare o alterare il software presente sul tablet.	ISO 27001 A.8.32
Sicurezza del dispositivo e protezione dati sul tablet	Condiviso	Applica controlli di sicurezza sul dispositivo: non archivia dati personali dei conducenti controllati sul dispositivo in modo permanente; cifratura del filesystem; possibilità di wipe remoto in caso di furto/smarrimento se segnalato.	È responsabile della custodia fisica del tablet, della prevenzione di accessi non autorizzati e della segnalazione immediata a SIAK SISTEMI in caso di smarrimento o furto del dispositivo, per consentire l'eventuale cancellazione remota dei dati.	ISO 27001 A.7.9 – A.8.1 – GDPR art. 32
Accesso alla piattaforma – credenziali e gestione sessione	Cliente	Fornisce le credenziali di accesso iniziali al software DDD Police sul tablet. Non è responsabile della gestione della sessione da parte dell'agente.	È responsabile della custodia e riservatezza delle proprie credenziali di accesso, di non condividerle con personale non autorizzato, e di eseguire il logout al termine di ogni sessione di	ISO 27001 A.5.16 – A.8.5

Ambito / Funzionalità	Tipo	Responsabilità SIAK SISTEMI	Responsabilità Cliente	Riferimenti normativi e ISO
			controllo.	
CENTRALINE DDD BOX – Scarico automatico da remoto (accessorio di DDD Manager)				
Fornitura e installazione hardware centralina DDD Box	Condiviso	Fornisce la centralina DDD Box certificata e compatibile con i tachigrafi digitali comprensiva di cavi. Fornisce supporto all'installazione.	È responsabile dell'installazione fisica della centralina sul veicolo (o dell'incarico a officina autorizzata).	Reg. UE 165/2014
Trasmissione automatica file DDD	SIAK SISTEMI	Gestisce la ricezione automatica dei file DDD trasmessi dalla centralina verso i server SIAK SISTEMI. Garantisce la connettività della rete e il corretto recapito dei dati.	Non è responsabile della trasmissione, che avviene automaticamente. Deve garantire che la centralina sia alimentata e operativa sul veicolo.	ISO 27001 A.8.20/A.8.21
Disponibilità dati aggiornati in DDD Manager	SIAK SISTEMI	Garantisce che i file ricevuti dalla centralina vengano elaborati e resi disponibili nell'archivio DDD Manager del cliente entro i tempi tecnici di elaborazione.	Verifica periodicamente che i dati della flotta vengano regolarmente aggiornati in piattaforma e segnala a SIAK SISTEMI eventuali anomalie o assenze prolungate di dati.	Reg. UE 165/2014 art. 36
Manutenzione e guasto della centralina	Condiviso	Fornisce supporto tecnico da remoto per diagnosticare malfunzionamenti. Gestisce la sostituzione del dispositivo in caso di guasto.	Segnala tempestivamente a SIAK SISTEMI eventuali anomalie della centralina. Durante il periodo di guasto, è responsabile di garantire lo scarico dati con modalità alternative (chiavetta).	Reg. UE 165/2014
Tracciamento posizione veicolo (GPS) — vedi NOTA art. 4 L. 300/1970 più sotto	Condiviso	La centralina può rilevare e trasmettere dati di geolocalizzazione del veicolo. SIAK SISTEMI tratta tali dati come Responsabile del trattamento e applica misure di sicurezza adeguate (cifatura in transit e at-rest, controlli di accesso).	È Titolare del trattamento per i dati GPS dei propri veicoli e conducenti. È responsabile di informare i conducenti del tracciamento (art. 13 GDPR), di acquisire la base giuridica appropriata e di soddisfare gli obblighi dell'art. 4 L. 300/1970 (accordo sindacale o autorizzazione ITL).	GDPR artt. 6, 13 – L. 300/1970 art. 4 – ISO 27018 A.7.5
Tempi di guida in tempo reale	Condiviso	Calcola e presenta in tempo reale i tempi di guida e riposo del conducente nei limiti tecnici del sistema, a supporto della pianificazione dei viaggi. La responsabilità di SIAK SISTEMI si esaurisce con la presentazione dei dati all'utente: non invia notifiche automatiche di infrazione.	È responsabile di verificare la correttezza dei dati visualizzati e di utilizzarli esclusivamente a scopo di pianificazione. Non deve basare decisioni sanzionatorie sui dati in tempo reale senza una verifica completa dei file DDD.	Reg. CE 561/2006
Carta azienda per lo scarico remoto	Condiviso	Custodisce la carta azienda del cliente inserita nelle apparecchiature di scarico SIAK SISTEMI e la restituisce al cliente su richiesta.	È responsabile di richiedere una nuova carta azienda alla Camera di Commercio in caso di guasto, scadenza o necessità di sostituzione. La richiesta di restituzione della carta azienda deve essere effettuata formalmente a SIAK SISTEMI.	Reg. UE 165/2014
Integrità e custodia della centralina DDD Box	Cliente	Fornisce la centralina funzionante e omologata. Non è responsabile di danni, manomissioni o guasti derivanti da un utilizzo improprio o da interventi non autorizzati sul dispositivo.	È responsabile dell'integrità fisica della centralina installata sul veicolo. Deve evitare manomissioni, interventi non autorizzati o rimozioni del dispositivo. In caso di guasto o manomissione segnala tempestivamente e gestisce lo scarico dati con modalità alternative fino al ripristino del servizio.	Reg. UE 165/2014 – Codice Penale art. 437
TERMINALI DI SCARICO – Terminale fisso autonomo (accessorio di DDD Manager)				

Ambito / Funzionalità	Tipo	Responsabilità SIAK SISTEMI	Responsabilità Cliente	Riferimenti normativi e ISO
Fornitura hardware terminale fisso (DDD Terminal)	Condiviso	Fornisce il terminale fisso omologato, lo configura per la connessione con l'account DDD Manager del cliente e garantisce assistenza tecnica.	È responsabile dell'installazione fisica del terminale in sede, della messa a disposizione dei conducenti e della segnalazione di guasti.	Reg. UE 165/2014
Scarico autonomo carte conducente da parte degli autisti	Condiviso	Il terminale acquisisce automaticamente i dati dalla carta conducente inserita e li trasmette all'archivio DDD Manager. SIAK SISTEMI garantisce il corretto funzionamento del processo.	È responsabile di comunicare ai propri conducenti la procedura di utilizzo del terminale, di assicurare che effettuino lo scarico nei termini obbligatori (ogni 28 giorni) e di vigilare sul rispetto della procedura.	Reg. UE 165/2014
Invio dati a DDD Manager senza intermediari	SIAK SISTEMI	Garantisce che i file DDD acquisiti dal terminale vengano inviati direttamente e in modo sicuro all'archivio DDD Manager del cliente, tramite canale cifrato, senza passaggi manuali.	Non è richiesto alcun intervento manuale. Il cliente deve verificare periodicamente che i dati degli autisti risultino presenti e aggiornati nell'archivio.	ISO 27001 A.8.20/A.8.24
Disponibilità del terminale per i conducenti	Cliente	Non è responsabile dell'organizzazione interna del cliente né della disponibilità oraria del terminale ai conducenti.	È responsabile di garantire che il terminale sia accessibile ai conducenti anche fuori dagli orari d'ufficio o in sedi non presidiate, e di organizzare le procedure interne affinché ogni autista effettui lo scarico nei termini.	Reg. UE 165/2014 – Statuto org. interna
Integrità e custodia del terminale di scarico	Cliente	Fornisce il terminale funzionante e configurato. Non è responsabile di danni, manomissioni o guasti derivanti da utilizzo improprio o interventi non autorizzati.	È responsabile dell'integrità fisica del terminale installato in sede. Deve evitare manomissioni o interventi non autorizzati sull'hardware. In caso di guasto o danneggiamento segnala tempestivamente a SIAK SISTEMI e garantisce lo scarico dati con modalità alternative fino al ripristino del dispositivo.	Reg. UE 165/2014
AMBITI TRASVERSALI – Sicurezza, privacy, gestione incidenti (applicabili a tutti i prodotti) – NUOVA SEZIONE v1.1				
Gestione delle violazioni di dati personali (data breach)	Condiviso	Notifica al Cliente, in qualità di Titolare, qualsiasi violazione di dati personali entro 48 ore dalla conoscenza dell'incidente (cfr. art. 17.6 contratto). Fornisce: natura della violazione, categorie e numero approssimativo di interessati, conseguenze probabili, misure adottate.	Quale Titolare, valuta l'obbligo di notifica al Garante (entro 72 ore ex art. 33 GDPR) e di comunicazione agli interessati (art. 34 GDPR), sulla base delle informazioni fornite da SIAK SISTEMI.	GDPR artt. 33, 34 – ISO 27018 A.10.1 – ISO 27001 A.5.24/5.25/5.26
Gestione delle richieste degli interessati (DSAR)	Condiviso	Assiste il Titolare nel rispondere alle richieste degli interessati di cui agli artt. 15-22 GDPR (accesso, rettifica, cancellazione, portabilità, limitazione, opposizione). Mette a disposizione strumenti tecnici e dati nei tempi richiesti.	Quale Titolare, gestisce direttamente il rapporto con l'interessato, valuta la richiesta, dispone le azioni necessarie e fornisce risposta nei termini di legge (1 mese, prorogabile).	GDPR artt. 12-22 – ISO 27018 A.16.1
Logging e accesso del cliente ai propri log	Condiviso	Conserva i log degli accessi alla piattaforma e delle attività amministrative per almeno 6 mesi. Garantisce integrità e disponibilità dei log per audit, sicurezza e gestione incidenti. Su richiesta scritta, fornisce estratti dei log per i dati di pertinenza del Cliente.	Può richiedere accesso ai log che lo riguardano per finalità di sicurezza, audit interno o investigazione di incidenti, con preavviso e modalità che garantiscano la riservatezza degli altri clienti.	ISO 27001 A.8.15/A.8.16 – ISO 27017 CLD.12.4.5
Esportazione e cancel-	Condiviso	Su richiesta del Cliente, esporta i dati in formato strutturato e	Richiede formalmente l'esportazione entro la data di cessazio-	ISO 27017 CLD.8.1.5 – ISO 27018 A.11.1 –

Ambito / Funzionalità	Tipo	Responsabilità SIAK SISTEMI	Responsabilità Cliente	Riferimenti normativi e ISO
lazione dati a fine rapporto		leggibile entro 60 giorni. Cancella i dati dai sistemi di produzione attivi entro 30 giorni dall'esportazione (o dalla cessazione se non richiesta). Le copie di backup non sono oggetto di cancellazione puntuale per ragioni tecniche (immutabilità, cicli di rotazione, eventuali archiviazioni offline): i dati restano confinati nei supporti di backup, non sono ripristinabili in produzione, sono trattati solo per disaster recovery e vengono naturalmente sovrascritti secondo i cicli ordinari. Rilascia attestazione di avvenuta cancellazione dai sistemi attivi su richiesta.	ne. È responsabile della corretta conservazione dei dati esportati e dell'eventuale comunicazione ai propri interessati.	GDPR art. 28(3)(g) – EDPB Guidelines on the right to erasure
Diritto di audit del cliente	Condiviso	Rende disponibili: (i) certificati ISO/IEC 27001, 27017, 27018 e relativo SoA; (ii) sintesi non confidenziale del più recente penetration test; (iii) attestazioni di conformità del sub-fornitore cloud (AWS). Su richiesta scritta con preavviso minimo 30 giorni, non più di una volta all'anno.	Può richiedere documentazione probatoria delle misure di sicurezza adottate. In caso di violazione di dati che lo coinvolga, può richiedere un audit specifico a proprie spese.	GDPR art. 28(3)(h) – ISO 27017 + ISO 27018 A.A.1.1
Personale autorizzato, NDA e formazione privacy	SIAK SISTEMI	Designa formalmente per iscritto tutto il personale dipendente, collaboratore o consulente con accesso a dati del Cliente come soggetto autorizzato al trattamento. Acquisisce NDA firmato. Eroga formazione periodica in materia di protezione dati e sicurezza delle informazioni.	Riceve, su richiesta, evidenza delle policy adottate da SIAK per il personale autorizzato.	ISO 27001 A.6.2/A.6.3/A.6.6 – ISO 27018 A.10.1 – GDPR art. 28(3)(b)
Finalità del trattamento dei dati personali	SIAK SISTEMI	Tratta i dati personali del Cliente esclusivamente per le finalità documentate dal Cliente e per gli adempimenti di legge connessi alla fornitura del servizio. Esclude espressamente attività di marketing, profilazione o uso dei dati per finalità proprie diverse da quelle previste.	Definisce e documenta le finalità del trattamento. Quale Titolare, mantiene il pieno controllo sulla destinazione d'uso dei dati.	ISO 27018 A.7.2.1 – A.A.2.1 – GDPR art. 28(3)(a)
Livelli di servizio	SIAK SISTEMI	Adotta le migliori pratiche di settore per garantire la disponibilità e la continuità del servizio SaaS su infrastruttura cloud. I livelli di servizio puntuali (disponibilità mensile, RTO, RPO, tempi di risposta supporto) saranno definiti in un apposito allegato SLA, attualmente in fase di definizione tra le Parti. Le metriche effettivamente registrate sono rendicontate su richiesta del Cliente.	Riceve, su richiesta, report sulle metriche di disponibilità. Una volta sottoscritto l'allegato SLA, ne accetta i livelli e le esclusioni ivi previste.	ISO 27001 A.5.30 – ISO 27017 CLD.9.5.1

6. Ruoli GDPR per Prodotto

I prodotti SIAK SISTEMI trattano dati personali (dati di conducenti: ore di guida/riposo, infrazioni, dati identificativi, posizione GPS ove applicabile). Di seguito la ripartizione dei ruoli ai sensi del Reg. UE 2016/679.

Prodotto	Ruolo SIAK	Ruolo Cliente	Dati personali coinvolti
----------	------------	---------------	--------------------------

Prodotto	Ruolo SIAK	Ruolo Cliente	Dati personali coinvolti
DDD Manager	Responsabile del trattamento (art. 28 GDPR)	Titolare del trattamento (art. 4(7) GDPR): determina finalità e mezzi del trattamento dei dati dei propri conducenti.	Dati dei conducenti: ore guida/riposo, infrazioni, dati anagrafici, informazioni sui veicoli, scadenze carte conducenti.
DDD Police	Fornitore di strumento e archiviazione dei dati. Responsabile del trattamento ex art. 28 per l'archiviazione cloud.	Titolare del trattamento: l'organo di controllo tratta i dati del conducente controllato nell'esercizio delle proprie funzioni istituzionali.	Dati del controllo e del conducente controllato: dati tachigrafo, tempi guida/riposo, infrazioni rilevate.
Centraline DDD Box	Responsabile del trattamento (art. 28 GDPR) per i dati trasmessi ai server SIAK.	Titolare del trattamento: definisce le finalità d'uso, informa i conducenti della localizzazione GPS, gestisce le basi giuridiche e gli adempimenti ex art. 4 L. 300/1970.	Dati conducenti e veicoli: dati tachigrafo, memoria di massa, posizione GPS (ove attivata).
Terminali di Scarico	Responsabile del trattamento per il transito dei dati verso DDD Manager.	Titolare del trattamento: organizza l'accesso al terminale, informa i conducenti, definisce le procedure interne.	Dati carta conducente: ore guida/riposo, identificativo conducente.

7. Revisione del Documento

Il presente documento è soggetto a revisione periodica nelle seguenti circostanze:

- Almeno una volta all'anno nell'ambito del riesame del SGSI (ISO 27001 cl. 9.3).
- In caso di aggiornamenti normativi rilevanti (GDPR, Reg. UE 165/2014, Reg. CE 561/2006, D.D. 215/2016, CdS, L. 300/1970).
- In caso di introduzione di nuovi prodotti, funzionalità significative o modifiche all'elenco dei sub-responsabili.
- A seguito di incidenti di sicurezza che coinvolgano dati personali trattati tramite i prodotti SIAK SISTEMI.

8. Storico Revisioni

Versione	Data	Descrizione modifiche	Autore
1.0	07/04/2025	Prima emissione del documento.	Gianluca Roveda, resp. R&D
1.1	21/05/2026	Revisione complessiva per allineamento a ISO/IEC 27017 e 27018: aggiunti riferimenti normativi nelle voci della matrice; aggiunta sezione 4 (Localizzazione dati e sub-fornitori); aggiunta sezione trasversale su data breach, DSAR, log, esportazione/cancellazione, audit right, NDA personale, finalità trattamento, SLA; aggiunta nota dedicata art. 4 L. 300/1970 per geolocalizzazione GPS; riclassificazione tipo responsabilità per coerenza (Sicurezza tablet, Conservazione dati controllo da "Cliente" a "Condiviso"); aggiunto storico revisioni; compilato form di approvazione.	Gianluca Roveda, resp. R&D

9. Approvazione del Documento

	Redatto da	Approvato da (DPO / Legale Rappresentante)
Nome	Gianluca Roveda	Yuri Merli

	Redatto da	Approvato da (DPO / Legale Rappresentante)
Ruolo	Responsabile R&D	Legale rappresentante
Data	19/05/2026	21/05/2026
Firma	 Signed with Odoo Sign 33981b0881...	 Signed with Odoo Sign ebf320decc...