Allegato 2
(Artt. 8 e 13)

MISURE DI SICUREZZA

In attuazione del principio contenuto nell'art. 32 del regolamento UE 2016/679, Regione Piemonte in qualità di Titolare, tenendo conto della tipologia dei dati trattati, dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, contemplando altresì i rischi di varia probabilità e gravità per i diritti e le libertà delle persone, ha individuato le misure di sicurezza ritenute idonee a minimizzare i rischi e garantire la sicurezza del trattamento.
In particolare, la Regione Piemonte, i Responsabili da essa individuati e i soggetti a vario titolo tenuti agli obblighi del regolamento UE 2016/679, impiegheranno nel trattamento dei dati personali le seguenti misure tecniche ed organizzative:

Tipologia di Contromisura	Descrizione sintetica delle principali contromisure adottate
Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa	Sono presenti misure per assicurare l'alta disponibilità dei sistemi e dei servizi di supporto. In particolare: • Le architetture dei sistemi datacenter prevedono opportune ridondanze dei componenti critici nonché procedure per il ripristino in caso di gravi interruzioni • I servizi "as service" sono erogati dai provider di riconosciuta affidabilità e sicurezza • l'adozione di copie di back-up e il ripristino dei dati in tempi certi • installazione di idonei programmi contro il rischio di intrusione e accesso abusivo • segnalazione della presenza di vulnerabilità nei programmi utilizzati e la contemporanea disponibilità delle opportune modifiche, all'aggiornamento, entro un congruo periodo di tempo
Controllo degli accessi	Al fine di mitigare la minaccia di accessi logici non autorizzati, vengono utilizzate utenze nominali e profili di autorizzazione di accesso per ogni singolo soggetto incaricato autorizzato al trattamento o gruppo omogeneo, configurati prima dell'inizio dei trattamenti e con criteri restrittivi. Con riferimento a tali utenze vengono implementate ulteriori misure: • Meccanismo che richiede che la password sia complessa; • Disattivazione delle credenziali di autenticazione del personale in caso venga a cessare la necessità di accesso da parte del soggetto incaricato autorizzato al trattamento o intervenga un'inattività per più di sei mesi; • Blocco delle credenziali in caso di reiterati tentativi di accesso falliti • cautele per assicurare la segretezza della componente riser-

	vata della credenziale e/o la diligente custodia del dispositivo in possesso ad uso esclusivo del soggetto incaricato autorizzato al trattamento; In merito all'eventuale trattamento dei dati personali con strumenti diversi da quelli elettronici, sono previste le seguenti misure: - predisporre un archivio per gli atti e i documenti con dati personali individuando per iscritto i soggetti incaricati autorizzati al trattamento con i relativi profili di accesso ai dati ed ai documenti; - definire le procedure di deposito, custodia, consegna o restituzione e compartimentazione dei dati stessi (ad esempio, un registro e degli armadi separati e chiusi); - l'utilizzo di appositi contenitori con lucchetti o serrature e definire una procedura di gestione delle chiavi.
Crittografia e pseudonimizzazione	La crittografia è utilizzata per proteggere la componente sicura delle credenziali e per la protezione delle transazioni via internet. Ai fini di analisi statistiche sono adottate tecniche di anonimizzazione.
Data Retention	I dati personali verranno conservati in maniera da consentire l'identificazione degli interessati per l'arco temporale massimo di 1 anno al fine di consentire l'eventuale correzione automatica delle rilevazioni inesatte e la risposta a contestazioni sui chilometraggi "addebitati" agli interessati. I dati personali relativi al sistema MOve-IN sono conservati separatamente da dati estranei allo stesso e suddivisi per territorio di competenza.
Gestione degli asset	Occorre mantenere continuamente aggiornato il seguente inventario: 11) Dispositivi autorizzati ad accedere alla rete; 12) Software autorizzati. Con riferimento ai supporti rimovibili, vi è l'obbligo di renderli inutilizzabili o di distruggerli e viene fornito un report finale sullo smaltimento di questi oggetti. In caso di trattamento di "dati particolari", occorre prevedere che: - il riutilizzo dei supporti di memorizzazione sia possibile solamente nel caso in cui le informazioni precedentemente contenute non siano recuperabili; in caso contrario i supporti dovranno essere distrutti; - la memorizzazione dei dati particolari su elenchi, registri o banche dati, avvenga in maniera da non permettere la diretta identificazione dell'interessato, ovvero che la memorizzazione dei dati particolari sia cifrata o in alternativa che vi sia separazione tra i dati particolari e gli altri dati personali che possano permettere l'identificazione dell'interessato
Gestione dei log	La configurazione del sistema permette la raccolta sia dei log delle azioni degli utenti e degli amministratori, sia i log degli eventi transazionali. Le stesse modalità di gestione dei log sono utilizzate anche con riferimento ai DBMS e ai servizi "as service".

Governo della sicurezza e privacy	Il governo della sicurezza e della privacy viene garantito tramite l'adozione di molteplici misure di sicurezza: • Svolgimento di regolari attività di: ✓ Analisi dei rischi ✓ Revisione dei requisiti di sicurezza ✓ Definizione dei piani di trattamento ✓ Verifica di attuazione ed efficacia dei piani di trattamento • Identificazione dei ruoli e delle responsabilità per l'attuazione delle misure di sicurezza e opportuna allocazione delle risorse • Attività formative e di sensibilizzazione in materia di sicurezza e privacy • Comunicazione al Titolare di eventuali situazioni che possano incidere sulla propria idoneità a svolgere l'incarico
Minimizzazione dei dati	Sono state implementate misure appropriate in linea con quanto definito in fase di progettazione per gestire solo i dati personali strettamente necessari.
Qualità dei dati personali trattati	I processi di trattamento prevedono adeguati controlli per assicurare che i dati personali trattati siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità.
Relazioni con gli operatori	Gli operatori selezionati rispettano autorevoli standard qualitativi e di sicurezza. I contratti prevedono l'identificazione delle responsabilità reciproche in merito alla gestione della sicurezza dei dati. All'osservanza di medesimi criteri sono tenuti eventuali subresponsabili nominati. Sono definiti e verificati i livelli di servizio.
Sicurezza delle attività operative	Al fine di garantire la sicurezza delle attività operative vengono implementate molteplici misure di sicurezza: • Procedure che regolamentano il ciclo di vita dei sistemi e dell'infrastruttura, considerando i requisiti di sicurezza nelle prime fasi di progettazione (privacy by design) e sviluppo, in fase di rilascio in esercizio fino alla dismissione; • Profilazione delle utenze sulla base della mansione svolta, garantendo il principio del minimo privilegio e la separazione dei ruoli e controllo degli accessi; • Separazione degli ambienti e divieto di utilizzare dati reali in ambienti di produzione; • Gestione degli incidenti di sicurezza e comunicazione all'Autorità competente e agli interessati; • Gestione degli asset; • Gestione degli operatori; • Gestione della sicurezza fisica; • Assoluto divieto di **diffusione dei dati,** o di **effettuazione di trattamenti ulteriori** rispetto a quelli affidati, salvo a fronte di specifica autorizzazione da parte del Titolare; • Obbligo di massima **riservatezza** in relazione a fatti, informazioni e dati; • Attività di revisione, comprese le ispezioni.

Sicurezza delle comunicazioni	A livello infrastrutturale gli eventuali flussi verso terzi soggetti vengono monitorati e nelle trasmissioni vengono utilizzati canali sicuri. A livello infrastrutturale, inoltre, è presente una segmentazione delle reti.
Sicurezza fisica e ambientale	Per garantire la sicurezza fisica e ambientale, l'accesso fisico agli archivi contenenti dati personali è controllato e vi è bisogno di un'autorizzazione per accedere. Sono presenti, inoltre, una politica di sicurezza fisica che prevede specifici controlli di sicurezza perimetrale e specifiche regole con riferimento alle attrezzature e alle reti utilizzate e una policy di clean desk/screen.
Software Development Lifecycle	La piattaforma tecnologica è stata sviluppata seguendo una politica di software lifecycle che regolamenta gli accessi ai sistemi di sviluppo e la necessità di test di sicurezza per verificare l'assenza di codice malevolo.
Training su sicurezza e privacy	È impartito training sulla sicurezza e privacy in modo da diminuire il rischio di violazione dei dati personali.
Aspetti relativi alla correttezza e trasparenza	Al fine di garantire l'esercizio dei diritti eventualmente applicabili da parte degli Interessati (Capo III del Regolamento UE 2016/679) occorre prevedere le seguenti misure: - Adesione su base meramente volontaria al progetto; - Chiarezza comunicativa nella divulgazione del progetto e successivamente in fase di adesione; - Adeguata e specifica informativa di consenso scritta in linguaggio chiaro e semplice (articolo 13 del Regolamento) fornita all'aderente ex ante alla raccolta dati; - Assistenza di primo e secondo livello; - Pubblicazione sul sito web istituzionale delle frequently asked questions (FAQ); - Comunicazione tempestiva di eventuali istanze ricevute ai sensi degli artt. da 15 a 22 del Regolamento UE 2016/679.

Considerato, infine, che la sicurezza, ed in particolar modo la sicurezza informatica, deve essere necessariamente intesa come un processo, soggetto a costante revisione ed aggiornamento, le misure tecniche ed organizzative sopra considerate saranno oggetto di periodico adeguamento, in ragione dello stato dell'arte disponibile, dei relativi costi di attuazione, nonché dell'eventuale definizione di ulteriori misure di garanzie prescritte ai sensi di legge.