Allegato B

Il presente Allegato Tecnico contiene i profili funzionali e tecnici del RENT anche con riferimento alle garanzie e misure di sicurezza tecnico-organizzative adottate dal Titolare, finalizzate a tutelare i diritti fondamentali dei soggetti i cui dati sono coinvolti nel Trattamento, di seguito «*interessati*». Sono, altresì, descritte le tipologie di dati trattati, le categorie di interessati e le operazioni eseguibili sui medesimi dati.

1. Descrizione modello di funzionamento del RENT

Il trattamento dei dati personali è effettuato nell'ambito della nuova versione informatica del RENT, che costituisce l'elenco informatico di registrazione dei titolari di licenza per il servizio taxi effettuato con autovettura, motocarrozzetta e natante e dei titolari di autorizzazione per il servizio di noleggio con conducente effettuato con autovettura, motocarrozzetta e natante a motore, di cui all'articolo 10-bis, comma 3, primo periodo, del decreto- legge 14 dicembre 2018, n. 135, convertito, con modificazioni, dalla legge 11 febbraio 2019, n. 12.

L'iscrizione al RENT è effettuata a seguito dell'istanza presentata ai sensi dell'articolo 5.

L'accesso alle informazioni e ai dati personali contenuti all'interno del RENT è garantito, previo superamento di una procedura di identificazione e autenticazione informatica, ai soggetti legittimati ad accedere al medesimo RENT ai sensi dell'articolo 4 del decreto.

L'accesso al RENT da parte dei soggetti di cui all'articolo 4 può avvenire attraverso i portali operativi del Dipartimento (Portale dell'Automobilista; Portale del Trasporto), ovvero tramite sistemi gestiti da altri soggetti attraverso l'intermediazione della Piattaforma Digitale Nazionale Dati - di seguito, anche «PDND» o infine attraverso cooperazione con i Sistemi del CED Interforze del Dipartimento della Pubblica Sicurezza. In particolare:

- Gli Utenti personale amministrativo delle Imprese accedono tramite SPID livello 2 o CIE;
- gli Utenti Terzi Delegati accedono tramite SPID livello 2 o CIE;
- gli Utenti personale amministrativo delle Imprese di autoriparazione accedono tramite credenziali istituzionali con «MFA» o SPID livello 2 o CIE;
- gli Utenti personale amministrativo dei Comuni accedono tramite credenziali istituzionali con Multi-Factor Authentication (di seguito, anche «MFA») o SPID livello 2 o CIE. In caso di utilizzo di sistemi proprietari attraverso cooperazione applicativa verrà adottato lo scambio attraverso PDND, con i livelli di sicurezza definiti dalla piattaforma;
- gli Utenti personale amministrativo degli UMC accedono tramite credenziali istituzionali con MFA;
- gli Utenti personale tecnico del CED accedono tramite credenziali istituzionali con MFA;
- gli Agenti di Polizia accedono tramite le modalità di autenticazione poste in essere dal CED Interforze del Dipartimento della Pubblica Sicurezza, con livelli di sicurezza da questo definiti, oppure tramite credenziali istituzionali con MFA.

Nelle more dell'implementazione delle modalità di accesso sopra descritte, , e comunque sino al 31 dicembre 2024, al fine di garantire l'operatività sul RENT a tutti gli utenti sin dal momento del primo rilascio del sistema, agli Utenti personale amministrativo dei Comuni e agli Utenti personale amministrativo delle Imprese di autoriparazione viene garantito l'accesso tramite le credenziali istituzionali rilasciate dal CED.

Ciò posto, si riporta di seguito la descrizione del ciclo di vita dei dati realizzato nell'ambito del RENT:

A. «*Raccolta dei dati*»: in tale fase, le informazioni richieste ai fini dell'iscrizione al RENT, vengono fornite dalle Imprese o da Terzi Delegati in sede di presentazione dell'istanza di iscrizione e sono raccolti tramite l'apposito servizio a ciò dedicato;

B. «*Verifica e Approvazione*»: a seguito della presentazione della richiesta di iscrizione da parte dell'Utente Impresa o Terzo Delegato, il sistema, a valle dell'esito positivo della verifica della consistenza dei dati, approva la stessa;

C. «*Inserimento nel RENT*»: una volta approvata l'istanza di iscrizione, i dati suddetti confluiscono all'interno del RENT;

D. «*Trattamento e Conservazione*»: una volta confluiti all'interno del RENT, i dati sono processati e conservati nel *database* del sistema per il perseguimento delle specifiche finalità del trattamento effettuato nell'ambito del RENT;

E. «*Accesso e Utilizzo*»: i dati sono accessibili agli Utenti previo superamento di una procedura di identificazione e autenticazione informatica, come sopra definito. In particolare, nell'ambito della procedura di accesso al RENT, sono previsti: (*i*) un sistema di *logging* integrato; (*ii*) soluzioni di monitoraggio per tenere traccia delle operazioni del sistema e facilitare l'identificazione di eventuali problemi tecnici;

F. «*Aggiornamento e Manutenzione*»: i dati relativi alle imprese possono essere aggiornati in considerazione dell'inserimento di nuove informazioni e/o di modifica delle informazioni esistenti a cura delle Imprese, dei Terzi delegati, del personale amministrativo degli UMC e del CED;

G. «*Archiviazione e Backup*»: i dati possono essere archiviati in un formato sicuro per scopi di conservazione a lungo termine e *backup*, per prevenire la perdita dei medesimi a causa di guasti tecnici o altri incidenti. A tal fine si prevede di introdurre un sistema a blockchain che ne garantisca immutabilità;

H. «*Cancellazione logica*»: i dati possono essere eliminati mediante cancellazione logica qualora non risultassero più necessari per il perseguimento delle finalità di trattamento, nonché su richiesta dell'Utente interessato.

Per ciascuna delle sezioni previste dall'articolo 3 il RENT presenta le seguenti funzioni (di seguito, anche «Funzioni:

1. «*Richiesta di iscrizione*»;
2. «*Verifica delle richieste di iscrizione*»;
3. «*Anagrafica Impresa*».

In particolare, si precisa che:

- l'Utente Impresa può eseguire le seguenti operazioni:
  - «*Richiesta di iscrizione*»: l'Utente compila i campi e carica la documentazione relativa alla presentazione dell'istanza di iscrizione;
  - «*Anagrafica Impresa*»: l'Utente visualizza i dati del proprio profilo all'interno del quale è abilitato ad effettuare le seguenti operazioni:
    - Censimento dei CF che sono abilitati ad operare in vece dell'Utente in qualità di Terzi Delegati. I CF verranno utilizzati per riconoscere i soggetti al momento del login attraverso SPID;

- Censimento dei CF dei Vettori NCC e dei Conducenti, come definiti nello schema di Decreto del Foglio di Servizio, che possono operare per conto dell'Impresa ai fini dell'esecuzione delle operazioni descritte nell'Allegato Tecnico dello schema di Decreto medesimo;
- Aggiornamento dati;
- Visualizzazione dei provvedimenti di revoca o sospensione adottati nei confronti del medesimo.

Ciò posto, si precisa che è previsto un sistema di notifica automatica nei confronti dell'Utente Impresa, per le comunicazioni relative al RENT.

- l'Utente Terzo Delegato può eseguire le seguenti operazioni:
  - «*Richiesta di iscrizione*»: l'Utente compila i campi e carica la documentazione relativa alla presentazione dell'istanza di iscrizione per conto dell'Utente Impresa;
  - «*Anagrafica Impresa*»: l'Utente aggiorna e modifica i dati del profilo, in seguito alla delega ricevuta a sistema dall'Impresa;

  Si precisa che, terminato il processo di richiesta di iscrizione a cura di un Utente Terzo Delegato, il sistema notifica in via automatica all'Utente Impresa, tramite PEC, l'invio della richiesta di iscrizione, rimandando all'accesso al sistema per la visualizzazione dei relativi dati;
- l'Utente personale amministrativo delle Imprese di autoriparazione può eseguire le seguenti operazioni:
  - «*Anagrafica Impresa*»: l'Utente visualizza i dati per la sola consultazione. Con riferimento alle informazioni relative ai provvedimenti di revoca o sospensione adottati, la visualizzazione è limitata ai soli effetti degli stessi;
- l'Utente personale amministrativo del Comune può eseguire le seguenti operazioni:
  - «*Anagrafica Impresa*»:
    - l'Utente visualizza i dati per la consultazione dei titoli delle Imprese relative al proprio comune;
    - l'Utente può inserire eventuali provvedimenti di revoca o sospensione adottati e gestire eventuali modifiche a valere sugli stessi;
- l'Utente personale amministrativo degli UMC può eseguire le seguenti operazioni:
  - «*Anagrafica Impresa*»: l'Utente visualizza i dati per la sola consultazione. Con riferimento alle informazioni relative ai provvedimenti di revoca o sospensione adottati, la visualizzazione è limitata ai soli effetti degli stessi;
- l'Utente personale tecnico del CED può eseguire le seguenti operazioni:
  - «*Richiesta di iscrizione*»: l'Utente organizza e struttura i dati e manutiene il sistema;
  - «*Verifica delle richieste di iscrizione*»: l'Utente organizza e struttura i dati e manutiene il sistema;
  - «*Anagrafica Impresa*»: l'Utente organizza, struttura, consulta, recupera e, se necessario, cancella i dati e manutiene il sistema;
- l'Utente Agenti di polizia può eseguire le seguenti operazioni:

- «*Anagrafica Impresa*»: l'Utente visualizza i dati per la sola consultazione. Con riferimento alle informazioni relative ai provvedimenti di revoca o sospensione adottati, la visualizzazione è limitata ai soli effetti degli stessi.

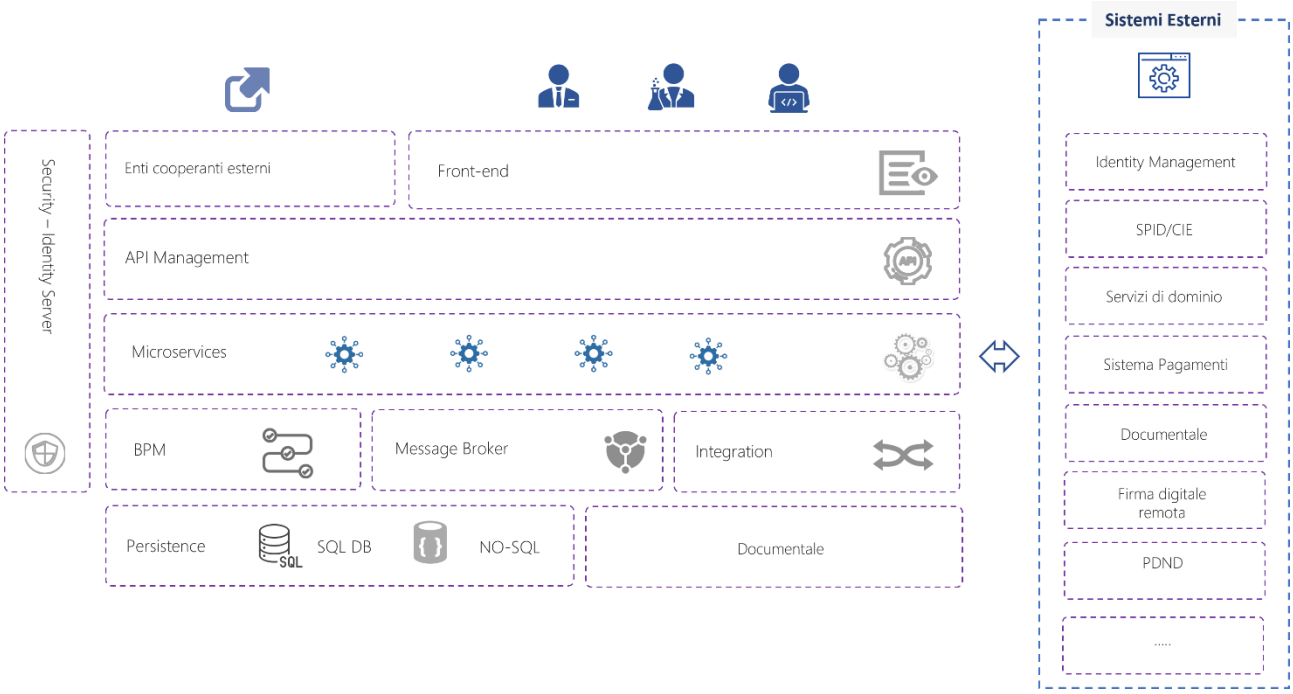
Le operazioni eseguibili dagli utenti all'interno del RENT, ciascuno nell'ambito della propria area di operatività, sono tracciate e monitorate al fine di garantire l'integrità e la correttezza del trattamento dei dati, in conformità alla disciplina vigente. Al riguardo, si precisa che il sistema consente la registrazione delle istanze, la modifica dei profili delle imprese, l'aggiornamento dei dati, nonché la gestione dei provvedimenti di revoca o sospensione.

Il Ministero delle infrastrutture e dei trasporti, in veste di Titolare del trattamento, sottopone agli Interessati l'informativa ai sensi degli articoli 13 e 14 del GDPR, contenente le informazioni in merito al trattamento dei dati eseguito nell'ambito del RENT.

In particolare, l'informativa è fornita attraverso le seguenti modalità:

- Apposizione di *flag* relativo alla presa visione dell'informativa medesima, nei casi in cui la richiesta di iscrizione sia presentata dalle Imprese;
- caricamento dell'informativa firmata dall'Impresa delegante, nei casi di presentazione della richiesta di iscrizione da parte dell'Utente Terzo Delegato.

Di seguito è mostrata l'Architettura Logica con le macro-componenti ed i layer che la caratterizzano.



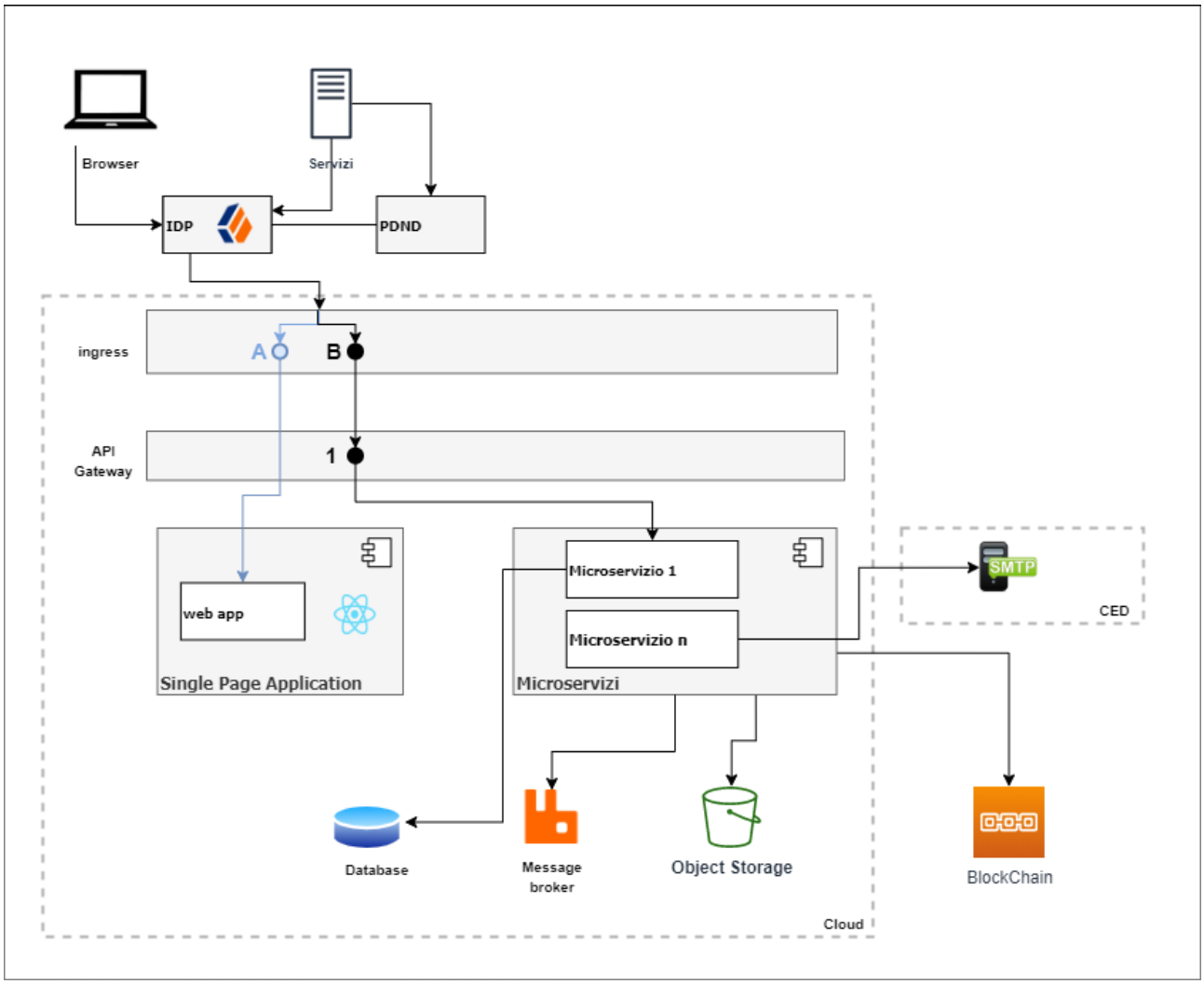
Il layer di identity management è progettato per fornire un'esperienza di accesso sicuro e unico agli utenti, implementando funzionalità di single sign-on (SSO) e integrando protocolli moderni di federazione come lo SPID (Sistema Pubblico di Identità Digitale) e la CIE (Carta d'Identità Elettronica); in tale layer si integrano anche i controlli sui token scambiati con la PDND per la cooperazione applicativa.

Le informazioni ricevute dalla federazione, come ad esempio i dati di autenticazione forniti tramite SPID livello 2 o CIE, vengono quindi verificate dall'applicativo per garantire che gli utenti corrispondano ai requisiti necessari per l'accesso. Nel caso specifico, il sistema verifica se l'utente è un rappresentante legale di

un’impresa di TAXI e NCC (Noleggio Con Conducente) o comunque un utente riconosciuto dalla specifica impresa, ovvero, in caso di mancata approvazione automatica, il personale amministrativo degli UMC o il personale tecnico del CED verificano l’istanza presentata, prima di autorizzare l’effettiva operatività sul sistema RENT per le funzionalità di data entry.

Questo approccio garantisce che solo gli utenti autorizzati, che soddisfano specifici requisiti di identità, possano accedere e utilizzare le funzionalità dell'applicativo, migliorando così la sicurezza e riducendo il rischio di accessi non autorizzati o fraudolenti.

Si riporta di seguito la soluzione specifica adottata per il RENT all’interno dell’architettura logica appena descritta. Questa si avvale di apposite risorse tecnologiche, rappresentate dall’architettura applicativa seguente.



Il *front-end* dell’applicazione è realizzato da una *Single Page Application* (SPA), i cui meccanismi di autenticazione e autorizzazione sono gestiti dall’Identity Portal della Motorizzazione (di seguito, anche «IdP»), che all’atto del login rilascia un *Id_Token.* Lo stesso è verificato dal Gateway che, in caso di *token* valido, ribalta la richiesta ai microservizi *stateless*. I microservizi effettuano RBAC sul profilo dell’utente.

Relativamente alla cooperazione applicativa, questa avverrà tramite l’integrazione della PDND, in cui l’API gateway sarà predisposto per esporre le API opportunamente configurate.

L'*object storage* viene utilizzato come area di archiviazione documentale anche sfruttando le *feature* di cifratura degli strumenti utilizzati; il *Message broker* viene utilizzato per garantire il paradigma di un'architettura *event-driven.*

Le credenziali di accesso al database, al *message broker* e all'*object storage* sono gestite come *secrets*.

Si prevede l'utilizzo di un server SMTP interno al CED e l'integrazione di servizi *Blockchain* per garantire l'immutabilità dei documenti generati ed eventualmente dei dati salvati in archivio.

2. Descrizione delle attività di trattamento dei dati personali

2.1 Tipologie di Dati trattati, in relazione alle specifiche finalità di trattamento e modalità operative di alimentazione

Nell'ambito del RENT sono raccolti e gestiti i dati e le informazioni di cui all'Allegato A.

Nel caso in cui l'iscrizione sia effettuata dal Terzo Delegato per conto dell'Impresa, sono registrate le seguenti informazioni:

- documento di delega che attesta la delega dell'Impresa al soggetto terzo per effettuare la sua iscrizione;
- dichiarazione di visualizzazione dell'informativa *privacy* firmata dal titolare dell'Impresa;
- dichiarazione di veridicità e di conformità all'originale resa dal titolare dell'Impresa;
- *flag* relativo alla dichiarazione di conformità della documentazione allegata alla documentazione esibita dall'Impresa.

Il trattamento dei suddetti dati personali è in ogni caso volto a consentire l'iscrizione degli Interessati all'interno del RENT, quale condizione necessaria per l'esercizio delle proprie, ai sensi del presente decreto.

In particolare, i dati su elencati sono resi accessibili al Titolare del trattamento per il perseguimento delle finalità di propria competenza, quali, in particolare: (*i*) garantire l'iscrizione da parte dell'Imprese nel RENT; (*ii*) il controllo, da parte dei restanti Utenti sopra riportati.

Sono, infine, registrate le informazioni relative all'apposizione da parte dell'Utente Impresa dei *flag* associati alle seguenti dichiarazioni:

- Dichiarazione di veridicità delle informazioni inserite ai sensi del Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, recante «*Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*»;
- presa visione dell'Informativa *privacy* fornita agli Utenti da parte del Titolare ai sensi degli articoli 13 e 14 GDPR.

I dati elencati confluiscono nel RENT tramite compilazione manuale.

2.2 Operazioni eseguibili sui dati e relative modalità di trattamento

Le operazioni eseguibili sui dati contenuti nell'ambito del RENT sono indicate nella tabella sottostante.

Soggetti coinvolti	Tipologia di accesso a sistema	Tipologia dei dati	Operazioni di trattamento
Impresa	SPID livello 2 o CIE	Dati personali, dati professionali; documentazione; stato corrente	Raccolta, registrazione, consultazione, adattamento/modifica
Terzi Delegati	SPID livello 2 o CIE	Dati personali, dati professionali; documentazione; stato corrente dell'Impresa	Raccolta, registrazione, adattamento/modifica
Personale amministrativo delle Imprese di autoriparazione	credenziali istituzionali con MFA o SPID livello 2 o CIE	Dati personali, dati professionali; stato corrente dell'Impresa	Consultazione
Personale amministrativo dei Comuni	credenziali istituzionali con MFA o SPID livello 2 o CIE; nel caso di cooperazione applicativa tramite PDND	Dati personali, dati professionali; stato corrente dell'Impresa	Consultazione e, per i soli provvedimenti, raccolta, registrazione adattamento/modifica
Personale amministrativo degli UMC	Credenziali istituzionali con MFA	Dati personali, dati professionali; stato corrente dell'Impresa	Consultazione
Personale amministrativo del CED	Credenziali istituzionali con MFA	Dati personali, dati professionali; stato corrente dell'Impresa	Organizzazione, strutturazione, conservazione, recupero, consultazione, utilizzo, cancellazione
Agenti di polizia	Autenticazione predisposta dal CED Interforze del Dipartimento della Pubblica Sicurezza; oppure tramite credenziali istituzionali con MFA	Dati personali, dati professionali; stato corrente dell'Impresa	Consultazione

2.3. Tempistiche di conservazione

Ai sensi dell'articolo 5, paragrafo 1, lettera e), del GDPR, al fine di garantire un trattamento corretto e trasparente, i dati delle imprese sono conservati all'interno del RENT fino a 2 anni dalla decadenza della loro iscrizione, per garantire anche oltre tale data la disponibilità delle informazioni ai fini di eventuali accertamenti

di legge. Decorso il periodo di conservazione, i dati personali oggetto di trattamento vengono cancellati in modo irreversibile.

3. Analisi dei rischi

Nella seguente tabella sono descritti i rischi potenziali connessi all'utilizzo del RENT, con indicazione del livello di rischio, calcolato sulla base della gravità e della probabilità di accadimento, e le relative misure preventive adottate per la mitigazione degli stessi.

Tipologia di rischio	Descrizione	Livello di rischio	Misure preventive
Malware, *virus*, *bug* introdotti via internet nel sistema e nelle postazioni di lavoro.	Tale rischio può verificarsi e può comportare la perdita di dati, la violazione della sicurezza, il rallentamento del sistema, il furto di informazioni personali e il danneggiamento dei sistemi.	Medio	• sistemi di *intrusion detection* e *prevention* • gestione sicura delle postazioni di lavoro • sicurezza dell'ambiente operativo
Intrusioni che possano comportare l'accesso illegittimo ai dati personali.	Il *Data Breach* è una violazione della sicurezza, che comporta accidentalmente o in modo illecito la distruzione, perdita, modifica, divulgazione, accesso, copia o consultazione non autorizzate di dati personali trasmessi, conservati o comunque trattati.	Medio	• controllo degli accessi logici ed autenticazione) • minimizzazione della quantità di dati personali • sicurezza del ciclo di vita delle applicazioni e nei progetti • sicurezza dell'ambiente operativo • sicurezza della rete e delle comunicazioni • tracciatura e monitoraggio • controllo degli accessi fisici • gestione degli incidenti di sicurezza e delle violazioni dei dati personali
Rischio di perdita accidentale di dati.	Tale rischio è riconducibile a problemi di funzionamento dei sistemi informatici o a condotte umane non corrette, che possono comportare la perdita o la distruzione accidentale di dati.	Basso	• manutenzione delle apparecchiature • sicurezza dell'ambiente operativo • sicurezza della rete e delle comunicazioni • controllo gestione sicura dell'*hardware*, delle risorse e dei dispositivi • *backup* • procedure previste dal Sistema di Gestione della sicurezza delle informazioni

Tipologia di rischio	Descrizione	Livello di rischio	Misure preventive
			• protezione delle fonti di rischio ambientali
Attacco informatico che renda indisponibile il servizio.	Attacchi DoS o DdoS che vanno a saturare la banda disponibile o le risorse elaborative rendendo indisponibile il servizio.	Medio	• sistemi di *intrusion detection* e *prevention*: • sicurezza della rete e delle comunicazioni • sicurezza del ciclo di vita delle applicazioni e nei progetti
Sabotaggi di apparecchiature, *server*, apparati di reti.	Tali rischi possono verificarsi a seguito di accessi non autorizzati ai sistemi o qualunque azione dannosa che potrebbe portare al furto di dati sensibili o al blocco dei sistemi.	Basso	• controllo degli accessi fisici • gestione degli incidenti di sicurezza e delle violazioni dei dati personali • controllo gestione sicura dell'*hardware*, delle risorse e dei dispositivi • protezione delle fonti di rischio ambientali
Guasti tecnici, quali malfunzionamenti apparecchiature, interruzione alimentazione elettrica, e malfunzionamenti software.	Tali rischi possono verificarsi in mancanza di affidabilità delle apparecchiature e un cattivo comportamento del software può dipendere, da errori presenti nel codice, dall'ambiente esecutivo.	Basso	• controllo gestione sicura dell'*hardware*, delle risorse e dei dispositivi • protezione delle fonti di rischio ambientali

4. Regole tecniche, requisiti, garanzie e misure di sicurezza adottate

Il Ministero delle Infrastrutture e dei trasporti identifica il Responsabile del trattamento dei dati personali, ai sensi dell'articolo 28 del GDPR, tramite appositi atti di nomina, ai fini dell'affidamento dei servizi infrastrutturali, di gestione e sviluppo applicativo del sistema informativo del Ministero medesimo.

In adempimento all'articolo 32 del GDPR, il Ministero delle Infrastrutture e dei trasporti adotta sulle infrastrutture tecnologiche, anche per mezzo del Responsabile del trattamento dei dati personali, le seguenti misure di sicurezza infrastrutturali, oltre a quelle risultanti dalle valutazioni di impatto:

- con riferimento ai sistemi di *intrusion*, *detection* e *prevention*, i servizi esposti del RENT sono protetti da sistemi IDS/IPS che monitorano e bloccano gli attacchi di varia tipologia (es. DoS, DdoS, sfruttamento vulnerabilità, *syn flood*, ecc.);

- con riferimento al controllo degli accessi logici ed autenticazione, in particolare la parte di autenticazione è gestita con un *Identity Portal* IDP federato con SPID mentre la parte di accesso è gestita direttamente dall'infrastruttura dei Portali;
- con riferimento alla gestione sicura delle postazioni di lavoro, le PDL del Ministero delle Infrastrutture e dei Trasporti sono sotto dominio e sotto antivirus, con Endpoint Detection and Response (EDR), e patch di sicurezza, controllate centralmente. Le PDL del Responsabile del trattamento dei dati personali, su cui quest'ultimo opera per la manutenzione dei sistemi, sono sotto dominio e si collegano alla rete del Ministero delle Infrastrutture e dei Trasporti attraverso un client VPN autenticato, tramite MFA, nell'eventualità in cui venga effettuato un collegamento da remoto;
- con riferimento alla manutenzione delle apparecchiature, su tutti gli apparati sono attivati contratti di manutenzione da parte del Ministero delle Infrastrutture e dei Trasporti;
- con riferimento alla minimizzazione della quantità di dati personali, le autorizzazioni e i permessi sono configurati secondo il principio del minimo privilegio, assicurando che gli utenti abbiano accesso solo alle sezioni e alle operazioni strettamente necessarie per le loro funzioni;
- con riferimento alla sicurezza del ciclo di vita delle applicazioni e nei progetti, il *Change Management* effettuato tramite processi in linea con i principi di *Security & Privacy by Design*. Viene effettuato il *patching* periodico della sicurezza dei Sistemi e vengono effettuati dei VA infrastrutturali e dei *Penetration Test* lato applicativo in modalità *Blackbox* con cadenza semestrale;
- con riferimento alla sicurezza dell'ambiente operativo, sono previste le seguenti misure: (i) manutenzione HW e SW di base; (ii) installazione tempestiva degli aggiornamenti di sicurezza distribuiti dal produttore ("*patching*"); (iii) rimozione di servizi, applicazioni e protocolli che non sono utilizzati; (iv) configurazione di Utenti autorizzati con i relativi permessi; (v) configurazione di sistemi di controllo delle risorse per il monitoraggio degli accessi e delle violazioni; (vi) *Change Management* con riferimento sicurezza della rete e delle comunicazioni, la rete è perimetrata e il servizio di accreditamento del RENT è separato a livello III nella parte di *frontend* e di *backend*;
- con riferimento alla tracciatura e al monitoraggio, le applicazioni sono configurate per produrre i *log* necessari a tracciare gli eventi significativi, e una piattaforma di *Log Management* è configurata per raccogliere, interpretare, indicizzare e conservare gli stessi per un anno;
- con riferimento al controllo degli accessi fisici alla sede di Via G. Caraci a Roma, lo stesso è consentito al personale autorizzato, nonché ai visitatori, mediante l'assegnazione (definitiva per il personale fisso e temporanea per gli ospiti) di un *badge* che permette l'accesso al perimetro e, ove configurato, al Palazzo dove è situato il CED;
- con riferimento alla gestione degli incidenti di sicurezza e delle violazioni dei dati personali, il Dipartimento, nell'ambito del suo sistema di gestione della sicurezza delle informazioni, ha definito un processo di gestione degli incidenti e una procedura specifica di *Data Breach* che è adottata qualora l'evento riguardi i dati anche di questo specifico trattamento in esame;
- con riferimento alla gestione sicura dell'hardware, delle risorse e dei dispositivi, i server sono posizionati in un CED e sono dotati di armadi *rack* con serratura, controllo della temperatura con impianto di refrigerazione, sistemi di antincendio oppia linea di alimentazione con UPS (batteria tampone) e gruppo di continuità per garantire la continuità elettrica;
- con riferimento alla protezione delle fonti di rischio ambientali, il CED è dotato di un sistema antiincendio a gas inerti, un sistema di allagamento. Tutti i *server* sono attestati su una doppia linea di alimentazione che in cascata è dotata di un UPS dedicato e un gruppo elettrogeno;

- con riferimento alle procedure previste dal Sistema di Gestione della sicurezza delle informazioni, le stesse sono definite nel Piano di Sicurezza;
- con riferimento al *Backup*, sono utilizzati specifici *tool* e *appliance* per la conservazione (su disco e su nastro) degli stessi;
- con riferimento alla cancellazione sicura, la stessa viene effettuata attraverso *software* specifici;
- con riferimento alle *policy* e alle procedure per la protezione dei dati personali, come definito nel piano della sicurezza, il Ministero delle Infrastrutture e dei trasporti adotta integralmente quanto stabilito dal Codice *privacy* e dal GDPR.