

ALLEGATO F.2

Infrastruttura Cloud e Governance

Capitolato Tecnico — Concessione di Servizi per il Recupero dei Crediti

Partenariato Pubblico Privato ai sensi degli artt. 174 e 193 del D.Lgs. 31 marzo 2023, n. 36

SECAM S.p.A. — CIG BB9E1C45C2

Versione 1.0 — Maggio 2026

Articolo 1 – Premessa e ambito di applicazione

Il presente allegato disciplina i livelli di servizio relativi all'infrastruttura Cloud su cui è erogata la piattaforma tecnologica che il Concessionario è tenuto a garantire per tutta la durata del rapporto concessorio. L'ambito di applicazione comprende: i servizi applicativi front-end e back-end, le componenti di integrazione con i sistemi informativi del Concedente, le pipeline di trattamento e le basi dati, nonché ogni ulteriore componente infrastrutturale funzionale alla continuità operativa del servizio. Le previsioni del presente allegato disciplinano altresì la classificazione degli incident e delle segnalazioni di disservizio.

Articolo 2 – Classificazione degli incident

Ai fini dell'applicazione degli SLA, gli incident sono classificati secondo quattro livelli di severità in funzione dell'impatto sul servizio e sulla continuità operativa del Concedente.

Livello	Denominazione	Definizione
P1	Critical	Piattaforma completamente non disponibile ovvero perdita di dati in atto. Impatto su tutti gli utenti del Concedente.
P2	High	Funzionalità core degradata — a titolo esemplificativo: impossibilità di aprire pratiche, dashboard non accessibile — con impatto su oltre il cinquanta per cento degli utenti.
P3	Medium	Funzionalità non core compromessa o disagio superabile mediante workaround. Impatto parziale e circoscritto.
P4	Low	Disservizio minore senza impatto operativo immediato sulle attività del Concedente.

Articolo 3 – Disponibilità del servizio

3.1 Uptime mensile garantito

Il Concessionario garantisce i seguenti livelli minimi di disponibilità mensile per ciascuna componente della piattaforma, calcolati sul totale dei minuti del mese solare. Le finestre di manutenzione programmata, preventivamente comunicate al Concedente non concorrono al computo del downtime.

Componente	SLA target	Minimo accettabile	Finestra di misura
Piattaforma applicativa (front-end e back-end)	99,5 %	99,0 %	H24, 7 giorni su 7

Articolo 4 – Ripristino del servizio e perdita di dati

4.1 Recovery Time Objective (RTO)

Il Concessionario garantisce i seguenti tempi massimi di ripristino del servizio a seguito di un'interruzione non pianificata, a decorrere dalla segnalazione formale dell'incident mediante apertura del ticket.

Severità	RTO obiettivo	RTO massimo contrattuale
P1 — Critical	2 ore	8 ore
P2 — High	4 ore	16 ore lavorative
P3 — Medium	8 ore lavorative	4 giorni lavorativi

P4 — Low	3 giorni lavorativi	10 giorni lavorativi
-----------------	---------------------	----------------------

4.2 Recovery Point Objective (RPO)

Il Concessionario garantisce i seguenti valori massimi di perdita di dati accettabile, misurati come intervallo temporale tra l'ultimo backup validato e ripristinabile e il momento dell'evento avverso. Il rispetto del RPO è verificato mediante i Disaster Recovery Test di cui al punto 4.3.

Tipologia di dato	RPO obiettivo	RPO massimo contrattuale
Dati pratiche e anagrafiche dei debitori	24 ore	48 ore
Log delle lavorazioni e audit trail	24 ore	48 ore
Dati di reporting e dashboard	48 ore	72 ore
Configurazioni di sistema e parametri applicativi	24 ore	48 ore

4.3 Disaster Recovery Test

Il Concessionario è tenuto ad eseguire almeno un Disaster Recovery Test documentato ogni sei mesi, simulando uno scenario di ripristino completo della piattaforma a partire dai backup disponibili. L'esito del test, comprensivo dei valori di RTO e RPO effettivamente misurati, è trasmesso al Direttore dell'Esecuzione entro cinque giorni lavorativi dal completamento dell'esercitazione. Il mancato svolgimento del test nel termine semestrale è assoggettato alle penali.

Articolo 5 – Sicurezza dell'infrastruttura

5.1 Requisiti tecnici minimi

Il Concessionario adotta e mantiene per tutta la durata del Contratto le seguenti misure di sicurezza tecniche sull'infrastruttura Cloud:

Requisito	Specifica
Cifratura dei dati in transito	Protocollo TLS versione 1.2 come minimo; TLS 1.3 raccomandato
Cifratura dei dati a riposo	Standard AES-256
Autenticazione utenti	Autenticazione a più fattori (MFA) obbligatoria per tutti gli utenti della piattaforma
Autenticazione API	OAuth 2.0 con token JWT; scadenza del token non superiore a sessanta minuti
Localizzazione dei data center	Esclusivamente nel territorio dell'Unione Europea, in conformità al Regolamento (UE) 2016/679
Penetration test	Almeno uno per anno solare, condotto da soggetto terzo indipendente; esito condiviso con il Concedente entro trenta giorni dal completamento

5.2 Gestione delle vulnerabilità e delle patch

Il Concessionario è tenuto ad applicare le patch di sicurezza nei termini seguenti, calcolati a decorrere dalla data di pubblicazione ufficiale della vulnerabilità sul National Vulnerability Database (NVD) o da parte del CERT nazionale competente:

Classificazione CVSS	Termine di applicazione	Termine massimo contrattuale
Critica (CVSS $\geq 9,0$)	72 ore dalla pubblicazione	7 giorni
Alta (CVSS 7,0–8,9)	7 giorni dalla pubblicazione	14 giorni
Media (CVSS 4,0–6,9)	30 giorni dalla pubblicazione	45 giorni
Bassa (CVSS $< 4,0$)	90 giorni dalla pubblicazione	120 giorni

5.3 Notifica delle violazioni dei dati personali

In caso di violazione dei dati personali ai sensi dell'articolo 4, n. 12, del Regolamento (UE) 2016/679, il Concessionario notifica l'evento al Concedente entro quarantotto ore dall'avvenuta conoscenza, con le modalità e i contenuti di cui all'Allegato J della Convenzione.

Articolo 6 – Backup e ridondanza

Il Concessionario adotta e mantiene le seguenti misure di backup e ridondanza dell'infrastruttura per tutta la durata del Contratto e del Periodo di Continuità:

Parametro	Requisito contrattuale
Frequenza backup dati pratiche e lavorazioni	Giornaliera
Frequenza backup configurazioni di sistema	Giornaliera
Conservazione dei backup	Minimo novanta giorni in modalità rolling
Test di ripristino da backup	Con cadenza mensile; log del test trasmesso al Direttore dell'Esecuzione entro cinque giorni lavorativi dal completamento

Articolo 7 – Supporto e gestione degli incident

7.1 Canali e orari di assistenza

Il Concessionario garantisce i seguenti canali e livelli di assistenza in funzione della severità dell'incident, a decorrere dalla Data di Avvio:

Severità	Canale	Orario	Tempo di presa in carico
P1 — Critical	Numero telefonico dedicato H24 e PEC	Orario lavorativo	≤ 30 minuti
P2 — High	Numero telefonico dedicato e ticket system	Orario lavorativo	≤ 2 ore
P3 — Medium	Ticket system	Orario lavorativo	≤ 4 ore lavorative
P4 — Low	Ticket system	Orario lavorativo	≤ 1 giorno lavorativo

7.2 Obblighi di aggiornamento

Per gli incident classificati P1, il Concessionario fornisce aggiornamenti sullo stato del ripristino con cadenza non superiore alle due ore fino alla risoluzione. Alla chiusura di ogni incident P1 e P2, il Concessionario trasmette al Direttore dell'Esecuzione, entro cinque giorni lavorativi, un rapporto di post-incident contenente: descrizione dell'evento, causa

radice individuata, impatto sui dati e sul servizio, azioni correttive intraprese e misure preventive adottate per evitare il ripetersi dell'evento.

7.3 Technical Account Manager

Il Concessionario designa un Technical Account Manager dedicato al Concedente, quale punto di contatto unico per la gestione degli incident P1 e P2, le comunicazioni relative alle manutenzioni programmate e il coordinamento operativo con il Direttore dell'Esecuzione. Il nominativo e i recapiti del Technical Account Manager sono comunicati al Concedente entro dieci giorni dalla Data di Avvio e aggiornati senza indugio in caso di sostituzione.

Articolo 8 – Monitoraggio e reportistica

Il Concessionario mette a disposizione del Direttore dell'Esecuzione, entro dieci giorni dalla Data di Avvio, un accesso in sola lettura agli strumenti di monitoraggio della piattaforma, comprensivo di una status page aggiornata in tempo reale con l'indicazione della disponibilità di ciascuna componente.

Il Concessionario trasmette al Direttore dell'Esecuzione, entro il quinto giorno lavorativo del mese successivo al periodo di riferimento, un report mensile di servizio contenente almeno le seguenti informazioni:

- a) uptime effettivo per ciascuna componente, con evidenza degli eventuali scostamenti rispetto ai valori target;
- b) log degli incident classificati P1 e P2, con indicazione di: data e ora di apertura del ticket, data e ora di ripristino, RTO effettivo, causa radice e azioni correttive intraprese;
- c) riepilogo delle patch applicate nel mese con classificazione CVSS e data di applicazione;
- d) esito dei test di backup eseguiti nel mese.