Contratto per l'acquisizione di servizi ICT di sviluppo, manutenzione e supporto tecnico specialistico – Sistema della Riscossione SET (G15), CIG _____

Misure Tecnico Organizzative per Responsabili Esterni

NATURA DEL TRATTAMENTO	ACQUISIZIONE DI SERVIZI ICT DI SVILUPPO, MANUTENZIONE E SUPPORTO TECNICO SPECIALISTICO – SISTEMA DELLA RISCOSSIONE SET (G15)"
FINALITA' DEL TRATTAMENTO	Sviluppo e manutenzione del software a supporto della riscossione, con riferimento ai moduli software indicati nel capitolato tecnico
TIPOLOGIA DI DATI TRATTATI	Dati personali comuni (dati anagrafici, contabili e fiscali, inerenti possidenze e riscossione, inerenti il rapporto di lavoro, dati inerenti situazioni giudiziarie civili, amministrative, tributarie), nonché dati personali finanziari (dati relativi all'esistenza di rapporti finanziari (coordinate bancarie, consistenze saldi, movimenti, giacenza media, etc.).
CATEGORIE INTERESSATI	Debitori iscritti a ruolo

CARATTERISTICHE DEI SERVIZI PREVISTI NEL CONTRATTO

Il contratto ha come oggetto la manutenzione evolutiva e correttiva del sistema software della riscossione denominato "Acquisizione di servizi ICT di sviluppo, manutenzione e supporto tecnico specialistico – Sistema della Riscossione SET (G15)"

Luogo del trattamento

☐ Il Responsabile utilizza la propria infrastruttura

☐ Il Responsabile utilizza l'infrastruttura IT del Titolare

Quanto segue in questo paragrafo vuole essere una breve sintesi di ciò che è stato descritto nel Capitolato Tecnico, allegato al contratto avente CIG. _____ . Resta inteso che non si intende in alcun modo superare i contenuti nel Capitolato Tecnico stesso.
Per ogni dettaglio o approfondimento relativo alla natura dei servizi previsti nel contratto si rimanda all'allegato citato.

I servizi software oggetto del contratto sono:

- Servizio di Onboarding APM
- Servizio di Application Management (AMS)
- Servizio di Nuovi Sviluppi (NSS)
- Servizio di Assistenza Specialistica (AS)
- Servizio di Supporto agli utenti e Richiesta Informazioni (RI)

Per quanto riguarda il servizio di **Onboarding APM**, questo comprende attività di analisi e descrizione del software che non necessitano di alcun trattamento di dati.

Per quanto riguarda il **servizio di AMS**, questo contempla la Manutenzione Correttiva (MAC). Considerato che un generico intervento di MAC è correlato ad un errore del software su un determinato insieme di dati, la risoluzione di una MAC richiederà la trasmissione dei dati sul quale si è rilevato l'errore software

stesso. Questi dati non potranno essere anonimizzati in quanto l'operazione di renderli anonimi potrebbe compromettere la possibilità di risolvere l'intervento di MAC.

Il processo sottostante alla gestione di una MAC è articolabile nei seguenti passaggi:

1. A seguito di un problema del software il personale di AdeR rileva l'insieme di dati sui quali si è manifestato;
2. I dati sono estratti tramite l'impiego di opportuni software;
3. Si apre un ticket al Fornitore del servizio con allegati i dati estratti di cui al punto 2;
4. La trasmissione dei dati da AdeR al Fornitore avviene su canale criptato;
5. Il Fornitore riceve i dati e il ticket per l'intervento di MAC e provvede a installarli sul proprio sistema;
6. I passi da 2 a 5 potranno essere ripetuti più volte, anche su richiesta del Fornitore, qualora si rendesse necessario trasmettere altri dati su cui si manifesta lo stesso problema software;
7. Il Fornitore deve sempre avere informazione circa coloro della propria organizzazione che accedono a quei dati specifici;
8. Quando AdeR riterrà concluso l'intervento di MAC, il Fornitore dovrà cancellare tutti i dati relativi.

Per quanto riguarda il **servizio NSS**, questo contempla la manutenzione evolutiva (MEV) e nuovi sviluppi software (NS). Allo scopo di sviluppare le funzioni commissionate da AdeR al Fornitore, AdeR preventivamente avrà consegnato dei dati di prova resi pseudo anonimi per quanto riguarda i dati anagrafici, codice fiscale, rapporti di lavoro, ecc.

Il collaudo unitario e quello d'integrazione, eseguiti sui sistemi del Fornitore, saranno comunque effettuati sugli stessi dati pseudo anonimi.

Il collaudo di accettazione del software sarà eseguito sui sistemi di AdeR a cura del personale di AdeR e su dati reali (non pseudo anonimi). Personale del Fornitore potrà assistere ai collaudi di accettazione da remoto o presso le sedi di AdeR.

In caso il collaudo di accettazione dovesse rilevare problemi software, sarà eseguita la stessa procedura già vista per gli interventi di MAC nell'ambito del servizio di AMS.

Il servizio di AS ed il servizio di RI comprendono un insieme integrato di attività che garantisce supporto per tutte le necessità afferenti alle esigenze specifiche di AdeR come, ad esempio, studi su specifici argomenti, analisi e ricerche, realizzazione quadri di sintesi.

Comprendono inoltre le attività di ripristino dei sistemi oggetto del capitolato di gara a fronte di errori di manovra di operatori o utenti, o più in generale analisi di situazioni di errore ingenerati da programmi software.

Nel caso di ripristino dei sistemi come anche l'analisi delle situazioni di errore, gli addetti del Fornitore dovranno accedere direttamente ai dati reali sul sistema di produzione di AdeR.

L'accesso ai dati di produzione (quindi i dati reali e non resi pseudo anonimi), potrà avvenire presso le sedi di AdeR, come anche da sedi del Fornitore remote. Resta inteso che l'accesso del Fornitore ai sistemi di produzione di AdeR sarà sempre intermediato dagli operatori di AdeR e che quindi l'addetto del Fornitore accederà alle informazioni come "Amministratore di sistema".

In generale potrebbe essere richiesto un accesso ai dati di produzione, allo scopo di fornire una spiegazione più precisa e dettagliata.

L'accesso alle informazioni sui sistemi di produzione sarà regolamentato esattamente secondo quanto già specificato per il servizio di AMS.

I vari servizi possono combinarsi tra loro determinando diversi accessi del Fornitore ai dati di produzione allo scopo di risolvere un qualche problema. A titolo di esempio quanto segue rappresenta un possibile scenario di composizione dei vari servizi previsti nel contratto:

1. I tecnici di AdeR rilevano un comportamento giudicato anomalo di un modulo software e a questo scopo attivano una richiesta di informazioni presso il Fornitore;

2. Il Fornitore richiede di accedere ai dati di produzione per risolvere la richiesta;
3. AdeR gestisce l'accesso del Fornitore ai dati di produzioni inerenti alla richiesta di informazioni specifica; l'accesso del Fornitore potrà avvenire anche da una sede del Fornitore stesso;
4. A seguito degli approfondimenti durante l'ispezione dei dati di produzione potrebbe sorgere la necessità di attivare una AS, dalla quale seguirebbero più accessi del Fornitore ai dati di AdeR; tutti gli accessi sarebbero comunque supervisionati da AdeR e limitati alla situazione in esame;
5. Infine, le ulteriori indagini eseguite dal Fornitore nell'ambito dell'AS potrebbero determinare il rilascio di un programma in grado di risolvere i problemi sul database (da eseguirsi a cura di AdeR con il supporto del Fornitore), come anche si potrebbe rilevare un problema del software e quindi l'apertura di un intervento di MAC.

Sulla base dei servizi e dello scenario descritto, nei paragrafi che seguono sono declinate le Misure Tecnico Organizzative per Responsabili Esterni.

ORGANIZZAZIONE DELLA SICUREZZA DELLE INFORMAZIONI
Obiettivo: Stabilire un quadro di riferimento gestionale per intraprendere e controllare l'attuazione e l'esercizio della sicurezza delle informazioni all'interno dell'organizzazione.

1. Prevedere la definizione all'interno dell'organizzazione di specifici ruoli e responsabilità per la gestione della privacy (per es. privacy officer) e per la gestione della sicurezza dei dati (per es. CISO o figure equivalenti).
2. Prevedere adeguate misure di sicurezza per proteggere dati, informazioni acceduti, elaborati o memorizzati tramite siti di telelavoro (al di fuori delle sedi di lavoro).

Output
- Il Responsabile fornisce, a richiesta, specifiche sulla propria organizzazione producendo l'organigramma, il funzionigramma, l'elenco degli incarichi/ nomine con evidenza delle figure e gli uffici preposti alla sicurezza dei dati personali.
- Nel caso venga attuato il telelavoro, operatività sugli ambienti tecnici da parte dei propri dipendenti nell'ambito delle attività previste da contratto, il Responsabile si impegna a documentare le misure messe in opera per garantire la sicurezza. A titolo di esempio potranno essere indicate le misure fisiche adottate, delle comunicazioni, degli accordi di licenza, delle procedure operative e di audit delle attività svolte.

SICUREZZA DELLE RISORSE UMANE
Obiettivo: Assicurare che il personale e i collaboratori comprendano le proprie responsabilità e siano adatti a ricoprire i ruoli per i quali sono presi in considerazione.

3. Prevedere l'erogazione di formazione specifica, per il personale del Responsabile e per eventuali Sub-Contractor, in materia di trattamento dei dati – GDPR -, con particolare focus in relazione agli specifici trattamenti inerenti al contratto, ponendo in rilievo l'obbligo di riservatezza e di non divulgazione delle informazioni, sua durante le fasi di trattamento, sia successivamente, alla scadenza del rapporto contrattuale.

Output
- Il Responsabile fornisce, a richiesta, documentazione attestante la formazione in materia di sicurezza delle informazioni e dei dati personali in particolare, producendo evidenza dei Piani di formazione previsti o già attuati in materia e gli esiti dei corsi attuati. Per quest'ultimo aspetto, a titolo di esempio, indica la percentuale di copertura del personale coinvolto nelle attività previste dal contratto.

GESTIONE DEGLI ASSET
Obiettivo: Identificare gli asset dell'organizzazione e definire adeguate responsabilità per la loro protezione.

4. Definire e gestire un inventario dei Dati Personali di AdeR e dei relativi elementi di sicurezza.
5. Distruggere in modo sicuro le informazioni sensibili e il software in licenza prima del riutilizzo o dello smaltimento delle apparecchiature.

Output

- Il Responsabile fornisce, a richiesta, documentazione attestante la modalità con la quale gestisce la dismissione dei supporti non più necessari e che contengono informazioni riservate.

CONTROLLO DEGLI ACCESSI
Obiettivo: Limitare l'accesso alle informazioni ed ai servizi di elaborazione delle informazioni.

6. Proteggere e controllare l'accesso, anche in lettura, ai sistemi contenenti Dati Personali di AdeR.
7. Assegnare a ciascun soggetto autorizzato al trattamento credenziali sicure di autenticazione personali per accedere ai sistemi ed agli applicativi per trattare i dati di cui AdeR è Titolare.
8. Qualora fosse prevista la nomina di Amministratori di Sistema, per l'assegnazione delle credenziali privilegiate (Amministratori di sistema), rispettare il provvedimento del Garante del 27 novembre 2008, nonché quanto indicato nell'allegato privacy al contratto.

Output

- Il Responsabile fornisce, a richiesta, l'elenco degli utenti abilitati all'ambiente tecnico evidenziando le utenze di amministratori di sistema.
- Inoltre, a richiesta, sono fornite indicazioni relative al sistema di gestione password, a titolo di esempio riporta le modalità di definizione della password, le modalità di revisione e rimozione dei diritti di accesso ed il profilo di accesso assegnato ai singoli utenti.

SICUREZZA FISICA E AMBIENTALE
Obiettivo: Prevenire l'accesso fisico non autorizzato, danni e disturbi alle informazioni dell'organizzazione e alle strutture di elaborazione delle informazioni.

9. Definire, implementare e documentare le misure di sicurezza fisica all'interno dei locali e delle aree di lavoro del progetto.
10. Definire ed implementare politiche per il corretto utilizzo degli strumenti elettronici che includano anche indicazioni per la protezione dei dati in essi contenuti durante l'utilizzo ed in caso di furto, danneggiamento o malfunzionamento.
11. Definire implementare e documentare una politica di controllo accessi alle aree protette (Sede/i della società, sale CED, uffici, ecc.)

Output

- Il Responsabile fornisce, a richiesta, indicazione rispetto alle misure assolte in materia sicurezza fisica delle aree in cui sono svolte le attività di progetto ed in relazione al corretto utilizzo degli strumenti elettronici (Disciplinare). A titolo di esempio, indica le precauzioni intraprese rispetto alla protezione dei dispositivi fisici e dell'edificio in cui gli stessi sono collocati (reception, tornelli con badge, presenza sistemi di sicurezza perimetrale).

SICUREZZA DELLE ATTIVITÀ OPERATIVE
Obiettivo: Assicurare che le attività operative delle strutture di elaborazione delle informazioni siano corrette e sicure.

12. Condividere con AdeR la descrizione degli ambienti di sviluppo, test e altro tipo usati nell'ambito del contratto (in termine di numero macchine, configurazione software, configurazioni di rete, policy di sicurezza, ecc.)
13. Implementare controlli adeguati di sicurezza per le workstation che trattano Dati Personali di AdeR.
14. Implementare e portare a termine piani di azioni derivanti da audit, test e verifiche sulla sicurezza
15. Implementare, gestire e documentare una politica per la produzione, la conservazione e l'accesso ai file di log delle applicazioni e dei sistemi che trattano dai del presente contratto.
16. Definire, implementare e documentare politiche di backup delle informazioni in accordo con le specifiche contenute negli allegati tecnici.
17. Cancellare in modo sicuro i Dati Personali di AdeR in accordo con gli standard stabiliti nel Supplemento per il Trattamento dei Dati Personali (DPA) e comunque alla conclusione degli interventi di AMS, come indicato nel paragrafo "CARATTERISTICHE DEI SERVIZI PREVISTI NEL CONTRATTO".
18. Cancellare i file temporanei delle transazioni

Output
Le precedenti TOM si intendono dispositive in materia dei dati personali oggetto di trattamento nell'ambito del contratto, pertanto che il Responsabili documenti tramite uno specifico output.
In particolare dovrà essere data evidenza dei seguenti eventi:

- Acquisizione dei dati personali di produzione correlati all'intervento di AMS richiesto da AdeR;
- Evidenza della distruzione dei dati di cui al punto precedente alla conclusione dell'intervento di AMS.

SICUREZZA DELLE COMUNICAZIONI
Obiettivo: Assicurare la protezione delle informazioni nelle reti e nelle strutture per l'elaborazione delle informazioni a loro supporto.

19. Definire, implementare e documentare i seguenti controlli per assicurare la protezione dei dati oggetto del contratto che viaggiano su rete:
    - Definire una politica di controllo accessi e di utilizzo della rete.
    - Perseguire la sicurezza dei canali di trasmissione dati, sia sulla rete interna all'organizzazione, sia all'esterno (cifratura dei protocolli di rete HTTPS, FTPS, ecc.).

Output

- Il Responsabile fornisce, a richiesta, indicazione rispetto le misure assolte in materia sicurezza delle comunicazioni previste nell'esecuzione del contratto. A titolo di esempio riporta le eventuali procedure operative per la gestione delle reti, controlli a garanzia della riservatezza e della integrità dei dati in transito, le modalità di monitoraggio, eventuale presenza di NDA che riflettono la volontà del Responsabile di proteggere le informazioni e la modalità di aggiornamento e revisione periodica degli stessi.

ACQUISIZIONE, SVILUPPO E MANUTENZIONE DEI SISTEMI
Obiettivo: Assicurare che la sicurezza delle informazioni sia parte integrante di tutto il ciclo di vita dei sistemi informativi. In particolare questo include anche i requisiti specifici per i sistemi informativi che forniscono servizi attraverso reti pubbliche.

20. Memorizzare e archiviare la documentazione di progetto in un repository protetto e sicuro
21. Creare e mantenere una lista delle procedure operative di sicurezza.
22. Definire, implementare e documentare processi, regole e procedure per garantire la sicurezza dei dati personali oggetto del contratto nell'ambito di tutto il ciclo di vita dei sistemi informativi e degli applicativi, dalla progettazione alla dismissione; mantenendo al riguardo registrazione delle approvazioni, rendendole disponibili.
23. Mantenere registrazione delle approvazioni dei documenti sulla sicurezza dei dati e sulla privacy (DS&P) e renderla disponibile per scopi di report/audit.
24. Creare e aggiornare i documenti sulla sicurezza dei dati e sulla privacy (DS&P) nei tempi stabiliti e revisionarli su base periodica.

Output

- Il Responsabile fornisce, a richiesta, indicazione rispetto le misure assolte in materia di sviluppo dei sistemi nell'ambito del contratto. A titolo di esempio, indica le precauzioni intraprese rispetto alla protezione dei dati nelle fasi di raccolta dei requisiti, rispetto le politiche di sviluppo sicuro adottate e alle modalità di controllo dei cambiamenti di sistema, indica l'assolvimento della sicurezza nell'ambiente di sviluppo e l'attenzione alla attuazione di test di sicurezza e accettazione. Indica, inoltre, le protezioni adottate per la trattazione dei dati di test.
- Tracciare tutti i passaggi di assolvimento dei principi di privacy by design e by default.

RELAZIONI CON I FORNITORI
Obiettivo: Assicurare la protezione degli asset dell'organizzazione accessibili da parte dei fornitori.

25. Definire e monitorare livelli di servizio (SLA) per i Subresponsabili (sub-processors) corrispondenti a quelli riportati nel presente documento contratto (in termine di numero macchine, configurazione software, configurazioni di rete, policy di sicurezza, ecc.).

26. Garantire l'uso esclusivo di tutti gli ambienti usati nell'ambito di contratto per le sole finalità di ADER.
27. Registrare e monitorare le attività di sistema come stabilito nell'allegato tecnico.
28. Stipulare accordi scritti con tutti gli altri Subresponsabili del Trattamento (sub-processor) per imporre loro gli stessi obblighi stabiliti nel Supplemento per il Trattamento dei Dati Personali (DPA), in particolare per fornire sufficienti garanzie nell'attuare misure tecniche e organizzative adeguate.
29. (Definire e monitorare livelli di servizio (SLA) per i Subresponsabili (sub-processors) corrispondenti a quelli riportati nel presente documento contratto (in termine di numero macchine, configurazione software, configurazioni di rete, policy di sicurezza, ecc.).
30. Garantire l'uso esclusivo di tutti gli ambienti usati nell'ambito di contratto per le sole finalità di AdeR.

GESTIONE DEGI INCIDENTI RELATIVI ALLA SICUREZZA DELLE INFORMAZIONI
Obiettivo: Assicurare un approccio coerente ed efficace per la gestione degli incidenti relativi alla sicurezza delle informazioni, incluse le comunicazioni relative agli eventi di sicurezza ed ai punti di debolezza.

31. Definire, implementare e documentare un processo di gestione degli incidenti di sicurezza per assicurare: una immediata comunicazione, una rapida analisi d'impatto ed efficaci azioni correttive (e preventive).
32. (data breach) informare per iscritto, senza ingiustificato ritardo, AdeR specificando prontamente le violazioni dei dati subiti e le relative procedure messe in atto per contenere il rischio.

ASPETTI RELATIVI ALLA SICUREZZA DELLE INFORMAZIONI NELLA GESTIONE DELLA CONTINUITÀ OPERATIVA
Obiettivo: La continuità della sicurezza delle informazioni dovrebbe essere integrata nei sistemi per la gestione della continuità operativa dell'organizzazione.

33. Garantire e assicurare la sicurezza delle informazioni anche attraverso le necessarie attività sulle basi dati per assicurare la continuità del servizio, in riferimento a quanto previsto dal contratto

CONFORMITÀ
Obiettivo: Evitare violazioni a obblighi cogenti o contrattuali relativi alla sicurezza delle informazioni e di qualsiasi requisito di sicurezza.

34. Garantire l'adeguatezza delle misure tecniche previste per assicurare la continuità operativa dei servizi erogati.
35. Analizzare periodicamente i rischi di progetto relativi al trattamento dei dati personali e averne evidenza in caso di audit da parte di AdeR.
36. Implementare un processo di gestione dei rischi.
37. Documentare e gestire i rischi di progetto e di trattamento dei dati in accordo con il processo di gestione dei rischi.
38. Implementare procedure per la prevenzione delle minacce per ridurre al minimo il rischio di violazioni della sicurezza.
39. Il Titolare si riserva di procedere agli audit per la verifica in tema di protezione dati. Il Responsabile si impegna a produrre la documentazione, eventualmente richiesta, nel rispetto del principio di accountability previsto nel regolamento (UE) 2016/679.