Appendice alla nomina di Responsabile esterno del trattamento dei dati personali per il Contratto per i Servizi di gestione operativa dei processi dell'amministrazione del personale (Payroll) Cig. XXXX

## Misure Tecnico Organizzative per Responsabili Esterni

| | |
|---|---|
| NATURA DEL TRATTAMENTO | Gestione operativa dei processi dell'amministrazione del personale (Payroll) |
| FINALITA' DEL TRATTAMENTO | instaurazione e gestione amministrativa del rapporto di lavoro |
| TIPOLOGIA DI DATI TRATTATI | Personali; relativi alla salute; bancari; appartenenza sindacale; disabilità |
| CATEGORIE INTERESSATI | Dipendenti e loro familiari e/o collaboratori terzi (autonomi od occasionali) |

### 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 Agenzia delle Entrate - Riscossione 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.

Proteggere e controllare l'accesso, anche in lettura, ai sistemi contenenti Dati Personali di Agenzia delle Entrate - Riscossione.

6. 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 Agenzia delle Entrate - Riscossione è Titolare.
7. 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.

**CRITTOGRAFIA**

**Obiettivo:** Assicurare un uso corretto ed efficace della crittografia per proteggere la riservatezza, l'autenticità e/o l'integrità delle informazioni.

5. Assicurare, se previsto, l'uso della crittografia per proteggere i dati, ovvero anonimizzare i dati personali.

**Output**

- Il responsabile fornisce evidenza dei criteri adottati per la crittografia o l'anonimizzazione dei dati.

**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.

6. Definire, implementare e documentare le misure di sicurezza fisica all'interno dei locali e delle aree di lavoro del progetto.
7. 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.
8. 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.

9. Condividere con Agenzia delle Entrate - Riscossione 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.).
10. Implementare controlli adeguati di sicurezza per le workstation che trattano Dati Personali di Agenzia delle Entrate - Riscossione.
11. Implementare e portare a termine piani di azioni derivanti da audit, test e verifiche sulla sicurezza.
12. 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 dati del presente contratto.
13. Definire, implementare e documentare politiche di backup delle informazioni in accordo con le specifiche contenute negli allegati tecnici.
14. Cancellare in modo sicuro o restituire i Dati Personali di Agenzia delle Entrate - Riscossione in accordo con gli standard stabiliti nel Supplemento per il Trattamento dei Dati Personali (DPA).
15. 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 è richiesto che il Responsabile documenti tramite specifici output le attività intraprese.

**SICUREZZA DELLE COMUNICAZIONI**

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

16. 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.

17. Memorizzare e archiviare la documentazione di progetto in un repository protetto e sicuro

18. Creare e mantenere una lista delle procedure operative di sicurezza.

19. 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.
20. Mantenere registrazione delle approvazioni dei documenti sulla sicurezza dei dati e sulla privacy (DS&P) e renderla disponibile per scopi di report/audit.
21. 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.

22. 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.).
23. Garantire l'uso esclusivo di tutti gli ambienti usati nell'ambito di contratto per le sole finalità di Agenzia delle Entrate - Riscossione.
24. Registrare e monitorare le attività di sistema come stabilito nell'allegato tecnico.
25. 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.
26. (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.).
27. Garantire l'uso esclusivo di tutti gli ambienti usati nell'ambito di contratto per le sole finalità di Agenzia delle Entrate - Riscossione.

**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.

28. 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).
29. In caso di una violazione dei dati personali (data breach) informare per iscritto, senza ingiustificato ritardo, Agenzia delle Entrate – Riscossione e 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.

30. 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.

31. Garantire l'adeguatezza delle misure tecniche previste per assicurare la continuità operativa dei servizi erogati.

32. Analizzare periodicamente i rischi di progetto relativi al trattamento dei dati personali e averne evidenza in caso di audit da parte di Agenzia delle Entrate - Riscossione.
33. Implementare un processo di gestione dei rischi.
34. Documentare e gestire i rischi di progetto e di trattamento dei dati in accordo con il processo di gestione dei rischi.
35. Implementare procedure per la prevenzione delle minacce per ridurre al minimo il rischio di violazioni della sicurezza.
36. 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.