

Servizi di supporto specialistico di Responsabile della Protezione dei Dati (RPD)/ Data Protection Officer (DPO)

SCHEDA SERVIZIO

Contesto di riferimento

Trentino Digitale S.p.A nella sua operatività, pone in essere trattamenti di dati personali (come definiti dal Regolamento (UE) 2016/679 –GDPR- del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, di seguito GDPR) rientranti nella Titolarità propria ed in quella dei soggetti giuridici pubblici e privati con cui intrattiene rapporti di acquisizione o di fornitura di servizi;

Conformemente a quanto previsto del suddetto regolamento ai sensi dell'art. 37 ha nominato un Responsabile interno della Protezione dei Dati (di seguito RPD). A seguito di nuova organizzazione aziendale e al fine di valorizzare le competenze interne la Società assegna al Dirigente Responsabile interno della Protezione dei Dati nuovo incarico e intende quindi affidare ad Operatore specializzato il servizio di Responsabile della Protezione dei Dati Personali (RPD) o Data Protection Officer (DPO) ed i servizi connessi alla funzione detta ai sensi dell'art. 39 del citato Regolamento UE n. 679/2016, da svolgersi in conformità alla normativa di riferimento.

I servizi oggetto dell'incarico riguardano il supporto specialistico da erogare tramite la figura designata di Responsabile esterno della Protezione dei dati (RPD) o Data Protection Officer (DPO), il quale deve avere un'approfondita conoscenza della normativa e delle prassi in materia di privacy, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento, e conoscenze in campo Informatico e di sicurezza informatica.

Il settore di riferimento in cui opera la società, le sue caratteristiche e la relativa struttura organizzativa sono reperibili al seguente link www.trentinodigitale.it.

In particolare si evidenzia quanto segue:

- *Organizzazione aziendale e Privacy: con riferimento all'organizzazione adottata dalla società per garantire la corretta applicazione delle disposizioni normative in materia di Privacy, si evidenzia che:*
 - *Ai Dirigenti, responsabili di strutture organizzative, sono stati delegati specifici compiti e funzioni (rif. d.l. 101/2018, art. quaterdecies) a garanzia che vengano adottate/attuare all'interno delle singole Strutture tutte le misure necessarie ed indispensabili al rispetto e al monitoraggio delle disposizioni in materia di Privacy.*
 - *La Struttura organizzativa 'Processi, certificazioni e privacy' (in staff alla Presidenza), ha il compito di:*
 - *supportare il Titolare nel coordinare le altre Strutture al fine di garantire la corretta attuazione del Codice Privacy all'interno dell'azienda ;*
 - *supportare il Titolare o i Dirigenti delegati al trattamento, negli adempimenti operativi conseguenti all'applicazione del codice Privacy;*
 - *collaborare con il DPO, mettendo in atto le disposizioni dallo stesso impartite.*
 - *Le Strutture dedicate alla sicurezza informatica, Chief Information Security Officer e il Security Operations Center hanno il compito rispettivamente, la prima di definire le politiche di sicurezza per proteggere gli asset informatici, di identificare i rischi di*

sicurezza a cui sono potenzialmente soggette le informazioni e i sistemi individuando misure idonee a mitigarli, di assicurare lo sviluppo del sistema di gestione della sicurezza informatica e relativa certificazione ISO 27001, la seconda di proteggere gli asset informatici da possibili attacchi esterni).

- La Struttura 'Legale e Affari societari' (in staff alla Presidenza), garantisce il servizio di assistenza e consulenza legale
- Certificazioni. Con riferimento al sistema di gestione della sicurezza delle informazioni, la Società è certificata ISO/IEC 27001:2013. Con riferimento al sistema di gestione della qualità la Società è certificata UNI EN ISO 9001:2015 per l'ambito "Progettazione, sviluppo ed erogazione di servizi ICT".
- Adeguamenti al GDPR: la società ha provveduto a riallineare i processi interni a quanto previsto del GDPR, a titolo esemplificativo non esaustivo: gestione offerte e contratti, approvvigionamenti, formazione, gestione delle richieste di assistenza, gestione delle segnalazioni di malfunzionamento, gestione dei Data Breach, gestione dell'esercizio dei diritti degli interessati, gestione della progettazione e dello sviluppo di servizi/applicazioni, gestione del passaggio in esercizio di nuovi servizi/ applicazioni o nuove release/componenti..). La società ha i Registri delle attività di trattamento, il Registro delle violazioni, ha aggiornato le informative agli interessati, ha definito la metodologia per la valutazione del rischio e dell'impatto, ha predisposto standard di riferimento (ad esempio: contrattualistica per la nomina a responsabile e a sub responsabile, informative, riscontro alle richieste da parte degli interessati ecc.)
- E' in corso l'analisi per l'identificazione e l'implementazione di un sistema informativo a supporto del sistema di gestione della Privacy.

Oggetto dell'incarico

Formano oggetto dell'incarico i servizi di RPD/DPO, da svolgere in autonomia ed indipendenza riferendo al vertice gerarchico del Titolare/Responsabile del trattamento, come previsto dall'art.39 del Regolamento, finalizzati a:

- *informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento, nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;*
- *sorvegliare l'osservanza del Regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;*
- *fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;*
- *cooperare con l'autorità di controllo;*
- *fungere da punto di contatto per l'Autorità di Controllo per questioni connesse al trattamento, tra cui la consultazione preventiva, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.*

Potrà inoltre svolgere ulteriori compiti purché non comportino situazioni di incompatibilità, quali a titolo di esempio esemplificativo e non esaustivo:

- *fornire assistenza sulle informative agli interessati e sull'aggiornamento dei registri,*
- *fornire assistenza nell'analisi del rischio e nella valutazione dell'impatto;*
- *fornire pareri in caso di richieste da parte degli interessati,*
- *fornire pareri in caso di violazione dei dati personali (data breach),*
- *fornire pareri e consulenza su richiesta del titolare, del responsabile del trattamento e dell'Ufficio Privacy su temi in materia di protezione dei dati, predisporre un piano annuale delle attività da fare, un piano annuale per la formazione dei dipendenti e un piano annuale per le visite di controllo, formare i dipendenti e condurre le visite di controllo.*

Caratteristiche della Posizione e modalità di esecuzione dell'incarico.

L'incarico per servizi professionali di RPD/DPO, saranno da svolgere in autonomia ed indipendenza rapportandosi direttamente con il Titolare/Responsabile, conformemente a quanto previsto dall'art.38 del Regolamento. Pur mantenendo l'autonomia e l'indipendenza di cui sopra, il RPD/DPO dovrà operare in stretta collaborazione e in affiancamento, senza vincolo di subordinazione, con la struttura competente in materia di Privacy della società (Processi, Certificazioni e Privacy)

Al fine di meglio interagire con le figure aziendali è obbligatoria la presenza presso la sede della Committente almeno due volte alla settimana per un minimo di 4 ore a giornata; in caso di visite ispettive promosse dall'autorità di Controllo, di controlli da parte di Titolari, di violazione dei dati personali, il RPD/DPO dovrà assicurare la presenza presso la sede della Società entro un termine massimo di 4 ore dalla richiesta formulata per iscritto da parte della Committente.

Conformemente a quanto previsto nell'oggetto dell'incarico Il RPD/DPO sarà tenuto a fornire consulenza e assistenza, produrre pareri scritti e verbali, produrre documentazione aggiornata nonché produrre la relazione annuale per dar atto al Titolare della attività svolta e degli eventi più significativi.

In caso di pareri e consulenza scritta il RPD/DPO dovrà produrli nei termini definiti contrattualmente dalla data di richiesta formulata per iscritto da parte della Committente.