Amministratore Unico: Ing. Renato Cipollini
Montecatini Terme lì: 24/08/2018
Prot. n° 94/2018

**PROCEDURA DI OFFERTA PER L'AFFIDAMENTO DEL SERVIZIO DI CONSULENZA FINALIZZATI A GARANTIRE L'ADEGUAMENTO DELLA MONTECATINI PARCHEGGI & SERVIZI S.P.A. AL REGOLAMENTO EUROPEO 679/2016 SULLA PROTEZIONE DEI DATI PERSONALI, DA AGGIUDICARSI SECONDO IL CRITERIO DELL'OFFERTA ECONOMICAMENTE PIU' VANTAGGIOSA EX ART. 95 comma 2 e 10- bis DEL D.LGS 50/2016 e s.m.i..**

## OGGETTO DEL SERVIZIO

Oggetto del presente Capitolato è l'affidamento del servizio, in materia di trattamento e protezione dei dati personali, per la messa a norma ed il conseguente rispetto degli adempimenti e obblighi previsti dal regolamento europeo (di seguito GDPR 2016/679), nonché dell'affidamento dell'incarico di Data Protection Officer (Responsabile della protezione dei dati di seguito RPD/DPO) a Soggetto esterno in possesso dei requisiti previsti dal citato GDPR 2016/679. Adempimento primario sarà l'analisi dello stato attuale dell'impianto esistente (assetto organizzativo, regole aziendali, trattamenti etc.) L'affidatario (di seguito: "Affidatario") è tenuto anche a fornire servizi di supporto normativo/giuridico/amministrativo/organizzativo e di formazione, al fine di permettere alla Montecatini Percheggi & servizi (di seguito: "MP" o "Azienda") di adeguarsi agli adempimenti previsti dalla normativa privacy vigente.

## ATTIVITA' RICHIESTE – REQUISITI DI AMMISSIONE A PENA DI ESCLUSIONE

Le attività richieste sono rappresentate da tre linee di attività distinte: **Prima Linea** (Preliminare), **Seconda Linea** (Successiva) e **Terza Linea** (Finale). La fase preliminare tende ad individuare tutte quelle attività richieste al fine di effettuare gli adempimenti e gli obblighi previsti dal nuovo regolamento europeo. La fase successiva riguarda l'individuazione del DPO/RDP attraverso i requisiti e i compiti richiesti. La fase finale è orientata alla formazione del personale. Per tutte le predette attività di consulenza dovrà essere garantita l'assistenza on site, secondo le modalità che saranno concordate, per un numero di giornate congrue rispetto alla finalità di pieno adeguamento della MP al nuovo GDPR ed alla vigente normativa privacy e, pertanto, alla realizzazione delle attività elencate nei punti precedenti. Pertanto, ciascun Candidato dovrà presentare il proprio piano di lavoro nel quale saranno elencate le attività da svolgere e le relative tempistiche (cronoprogramma). La Prima Linea di attività dovrà concludersi entro il 30.11.2018.

**Prima Linea di attività**: Definizioni delle Attività preliminari richieste

In questa prima fase, come anzidetto, si richiede all'Affidatario di effettuare tutte quelle attività preliminari volte a definire un modello adeguato di funzionamento della data protection, nonché

tutte quelle attività volte a porre in essere tutti i necessari adempimenti previsti per le Società Pubbliche/Partecipate/Controllate, quale l'adozione del Registro dei trattamenti dei dati personali, in specie:

- analisi finalizzata alla raccolta di tutte le informazioni sull'organizzazione aziendale, alla verifica del livello di conformità alla nuova normativa in materia di protezione dei dati ed alla misurazione del livello di esposizione dei rischi associati al trattamento dei dati;
- analisi e valutazione di tutta la documentazione che impatti sul trattamento dei dati (es.: i contratti con i fornitori che trattano dati);
- analisi e valutazione dei processi e delle procedure di gestione dei sistemi informativi, degli strumenti per la gestione della sicurezza informatica e dei sistemi di controllo esistenti all'interno dell'Azienda;
- individuazione e mappatura dei trattamenti effettuati, analisi delle tipologie dei dati trattati, delle finalità per cui sono trattati, dei termini di conservazione dei dati, delle categorie degli interessati e classificazione del rischio privacy, anche dei dati non strutturati. In particolare, l'Affidatario dovrà effettuare la mappatura dei processi aziendali, dei trattamenti, svolgere interviste con il necessario grado di profondità nell'organizzazione aziendale al fine di predisporre il Registro dei Trattamenti dei dati personali. Il Registro dei trattamenti dovrà avere i contenuti minimi di cui all'art. 30 del GDPR 2016/679 e dovrà contenere una descrizione generale delle misure di sicurezza tecniche ed organizzative di cui all'art. 32 del GDPR 2016/679. Il Registro dei Trattamenti dovrà essere predisposto su apposito applicativo, da definire, strutturato in maniera tale da poter essere aggiornato e messo a disposizione dall'Affidatario in favore della MP. Il registro dovrà essere strutturato in maniera tale da consentire le successive attività di risk assestment e impact assestment;
- elaborazione, redazione od aggiornamento/revisione di tutta la documentazione/modulistica affinché risulti completa ed aggiornata secondo la nuova normativa (es. testi delle informative e dei moduli per il consenso al trattamento dei dati, etc.);
- elaborazione, redazione o revisione delle clausole contrattuali standard da inserire nei testi dei contratti, degli atti e dei disciplinari di gara;
- definizione dell'organigramma privacy finalizzato alla distribuzione dei ruoli e delle responsabilità interni all'azienda ai fini del trattamento dati e definizione dei flussi informativi tra le diverse figure coinvolte nel modello organizzativo di data protection;
- redazione di linee guida aziendali che contengano istruzioni operative e organizzative per tutte le figure aziendali coinvolte in materia di data protection (ad es. Manuale per l'adeguamento privacy);
- valutazione dei rischi e definizione delle politiche di sicurezza: attività di valutazione, individuazione dei rischi ed attuazione di tutte le misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare che i trattamenti siano effettuati conformemente al GDPR;
- attività di valutazione d'impatto sulla protezione dei dati (DPIA "Data Protection Impact Assessment"), l'Affidatario deve assistere la MP nell'individuare tutti quei trattamenti dai quali possa derivare un rischio elevato per la libertà e per i diritti degli utenti interessati, nell'individuare i rischi derivanti da tali trattamenti e gli strumenti più idonei per contrastarli (misure tecniche e organizzative da adottare e implementare);
- predisposizione e implementazione del processo di gestione e comunicazione Data Breach con conseguente stesura e attivazione del Registro di Violazione dei dati;
- individuazione e monitoraggio nuove pratiche operative (monitorare pratiche organizzative per identificare nuovi processi o modificare quelli esistenti, al fine di garantire l'attuazione della Privacy by design);

- predisposizione e implementazione dei processi per la gestione delle richieste di accesso ai dati personali oggetto di gara e di esercizio degli altri diritti da parte degli interessati (es.trasportabilità dei dati ed oblio);
- predisposizione e definizione del Remediation Plan: individuazione delle azioni correttive tecniche ed organizzative, atte a ridurre i gap individuati e le relative priorità, con particolare riferimento alla sicurezza informatica ed alle misure organizzative e tecniche adeguate da implementare;
- predisposizione/aggiornamento della regolamentazione aziendale in tema di trattamento dei dati personali (a titolo esemplificativo e non esaustivo: predisposizione di protocolli interni che regolamentano il corretto utilizzo di internet, posta elettronica e social network da parte dei dipendenti e/o collaboratori, il corretto utilizzo da parte dei dipendenti e/o collaboratori dei device aziendali, della realizzazione e diffusione delle riprese audio-video all'interno delle strutture aziendali da parte degli utenti, dell'utilizzo di firme grafometriche);
- analisi del sistema di videosorveglianza e proposta di aggiornamento alla normativa vigente.

**Seconda Linea di attività:** Affidamento del DPO/RDP. Compiti e Requisiti

Oltre alle attività indicate nei punti precedenti, si riportano i compiti del DPO/RDP, da Voi incaricato, previsti dall'art. 39 del GDPR, di seguito indicati (a titolo non esaustivo):

- redigere un piano di lavoro;
- informare e fornire consulenza in merito agli obblighi vigenti relativi alla protezione dei dati; il servizio di consulenza assolve altresì alla finalità di rispondere a singoli quesiti istituzionali in materia di privacy;
- sorvegliare l'osservanza della nuova normativa in materia, nonché delle politiche del Titolare del trattamento relative alla protezione dei dati personali;
- supportare la MP nella gestione documentale prodotta sulla protezione dei dati, ai fini di esibizione a terzi, tesa a dimostrare in modo oggettivo e trasparente le attività poste in essere per la compliance al GDPR, in linea con il principio di accountability;
- cooperare e fungere da punto di contatto con l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 del GDPR 2016/679 ed effettuare, se del caso, consultazioni relativamente ad ogni altra questione;
- facilitare l'accesso, da parte dell'autorità di controllo, ai documenti e alle informazioni necessarie per l'adempimento dei suoi compiti, nonché ai fini dell'esercizio dei suoi poteri di indagine, correttivi, autorizzativi e consultivi. In ogni caso il DPO può consultare l'autorità di controllo con riguardo a qualsiasi altra questione;
- rappresentare un punto cardine per gli interessati in merito al trattamento dei loro dati personali e/o sensibili e all'esercizio dei diritti, comunicando con gli interessati in modo efficiente;
- cooperare e supportare il Responsabile della Trasparenza nella valutazione delle richieste di accesso agli atti, che comportino riflessi sulla protezione dei dati personali, nell'ottica di contemperare il diritto di accesso al diritto di riservatezza dei dati trattati;
- considerare debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo: il DPO deve definire un ordine di priorità nell'attività svolta e concentrarsi sulle questioni che presentino maggiori rischi in termini di protezione dei dati, senza trascurare di sorvegliare altri trattamenti associati ad un livello di rischio inferiore;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del GDPR 2016/679 e supportare il titolare

nell'esecuzione delle attività necessarie per effettuare la valutazione d'impatto e l'eventuale riesame;

- garantire la propria partecipazione nei casi in cui il Titolare coinvolga il DPO in questioni attinenti la protezione dei dati, sin dalla fase di progettazione di dette attività e comunque garantire la propria pronta reperibilità secondo le esigenze della MP;
- riferire direttamente all'Amministratore Unico riguardo alle indicazioni e raccomandazioni fornite nel quadro delle sue funzioni, nonché un reporting riferito al livello di conformità al GDPR;
- redigere e trasmettere all'Amministratore Unico una relazione annuale delle attività svolte;
- supportare la MP nella predisposizione e gestione di specifici audit privacy sia interni che esterni;
- programmare l'attività di formazione ed aggiornamento annuale dei dipendenti della MP, per le problematiche e la legislazione concernente la materia del trattamento dei dati;
- evadere i quesiti in materia di privacy richiesti dalla MP entro il termine massimo di 7 (sette) giorni (di calendario). Nell'adempimento dei propri compiti, il DPO dovrà attenersi al segreto e alla riservatezza. I dati di contatto del DPO sono pubblicati e comunicati alle pertinenti autorità di controllo affinché possa essere contattato sia dagli interessati che dalle autorità di controllo in modo facile e diretto.

Il DPO dovrà svolgere il proprio ruolo dedicando alla MP un tempo adeguato rispetto ai compiti previsti e assegnati, utilizzando le risorse umane e strumentali interne alla propria struttura. Il DPO si rapporta con l'Amministratore Unico. Al DPO è consentito l'accesso a tutte le strutture aziendali al fine di acquisire notizie, informazioni e documenti necessari per lo svolgimento dei propri compiti anche mediante interviste al personale. L'accesso alle strutture aziendali sarà preceduto, di norma, da apposita comunicazione ai responsabili della struttura medesima.

Alla luce di quanto esposto il DPO deve possedere:

- alte qualità professionali, tra le quali, competenze giuridiche ed in particolare avere un'approfondita conoscenza in materia di Privacy, sia della vigente normativa sia del nuovo GDPR, nonché delle prassi nazionali ed europee in materia di tutela, protezione e trattamento dei dati;
- conoscenze in materia di organizzazione delle Società partecipate/controllate;
- adeguata conoscenza delle norme e delle procedure amministrative applicabili;
- capacità di promuovere una cultura di protezione dei dati all'interno dell'organizzazione dell'Azienda e, dunque, sotto il profilo delle qualità personali, deve possedere elevati standard deontologici, quali la correttezza, lealtà ed integrità di condotta;
- competenze in materia di risk management e di analisi dei processi.
- Il DPO non deve trovarsi in situazione che potrebbe anche potenzialmente configurare un conflitto di interessi.

**Terza linea di attività**: la Formazione

In questa terza linea si chiede all'Affidatario di effettuare l'attività di formazione del personale dipendente e/o dei collaboratori coinvolti nel modello organizzativo di Data Protection, con la previsione di corsi di diverso livello per le figure interessate; La formazione proposta sarà articolata al termine della Seconda Linea di attività di cui ai precedenti punti. I destinatari del corso saranno max. 14 partecipanti. L'evento avrà la durata minima di 6 ore per gruppi omogenei e dovrà prevedere, oltre ad una sintesi del contesto giuridico di riferimento, l'illustrazione delle azioni attuate e da attuare da parte della MP, ai fini di compliance GDPR, nonché l'illustrazione di casi pratici/esercitazioni volte a coinvolgere e sensibilizzare i Destinatari del corso. Nel corso degli eventi sarà presentato il DPO, il quale dovrà illustrare i propri compiti ed il tipo di supporto che può fornire agli interessati. L'evento formativo in aula sarà ripetuto una seconda volte nell'arco dei 18 mesi.

La MP, al fine di agevolare l'attività dei canditati a presentare un'offerta conforme alle richieste sopra citate, ha incaricato il Rag. Stefano Forcieri a fornire tutte le specifiche del caso propedeutiche ad una stesura dell'offerta la più puntuale possibile.

Tutte le Attività di analisi del contesto Aziendale, attuazione degli interventi correttivi nonché la formazione del personale, saranno svolti presso la sede della Società Montecatini Parcheggi & servizi Via E. Toti 10/14 Montecatini Terme. La MP metterà a disposizione dell'Affidatario tutti gli strumenti e le strutture necessarie alle finalità del presente Capitolato.

**L'OFFERTA DOVRA' PERVENIRE ENTRO LE ORE 13.00 DEL GIORNO 14 SETTEMBRE 2018 TRAMITE POSTA CERTIFICATA**: info@pecmontecatiniparcheggi.com
.

L'Amministratore Unico
Ing. Renato Cipollini