AFFIDAMENTO DELLE ATTIVITA' RELATIVE AL SERVIZIO SULLA PROTEZIONE DEI DATI PERSONALI E DATA PROTECTION OFFICER (DPO) AI SENSI DEL REGOLAMENTO EUROPEO EU 2016/679 PER IL PERIODO 20 MAGGIO 2018-19 MAGGIO 2021

CAPITOLATO TECNICO

Premessa

Il Regolamento (UE) 2016/679 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 (Regolamento generale sulla protezione dei dati)» (di seguito RGPD), in vigore dal 24 maggio 2016, e applicabile a partire dal 25 maggio 2018, introduce la figura del Responsabile dei dati personali DPO (in italiano RDP) (artt. 37-39).

Il Regolamento prevede l'obbligo per il titolare del trattamento di designare, secondo quanto indicato e stabilito all'art. 37, paragrafo 1, lett. a) un soggetto come RDP comunicandolo al Garante per la Privacy.

Le disposizioni del Regolamento prevedono che la figura del RPD possa anche essere coperta in base a un contratto di servizi (art. 37, paragrafo 6) purché assolva tutti i compiti che l'incarico richiede. La funzione di RPD può quindi essere esercitata in base a un contratto di servizi stipulato con una persona fisica o giuridica esterna all'azienda titolare del trattamento.

Nel caso della azienda società di servizi quale fornitore esterno, questa assolve i compiti stabiliti per il RPD mediante un team operante sotto l'autorità di un contatto principale, l'effettivo RDP, designato e "responsabile" per il singolo cliente. All'interno del team RPD si potranno associare competenze e capacità individuali con una chiara ripartizione dei compiti affinché il contributo fornito da più soggetti consenta di rendere il servizio più efficiente. È indispensabile che ciascun soggetto appartenente al fornitore esterno soddisfi tutti i requisiti applicabili come fissati nel RGPD nella Sezione 4.

OGGETTO DEL SERVIZIO

Il servizio ha per oggetto l'affidamento di consulenza e supporto in materia di protezione dei dati personali per la Funzione Esternalizzata di Data Protection Officer (Responsabile della protezione dei dati).

Nel mese di Marzo 2018 Adir ha conseguito la certificazione volontaria secondo lo schema di certificazione ISDP10003:2015 **in accordo con la norma EN ISO/IEC 17065:2012. La conoscenza e/o eventuale certificazione da parte del Candidato DPO su tale schema o schemi conformi a quanto stabilito dall'art. 43 del Regolamento EU 2016/679.**

Il servizio potrà essere svolto da un Team di professioni secondo quanto descritto in premessa, ovvero da un singolo professionista.

ATTIVITA' PRINCIPALI

Le attività del Data Protection Officer

Fase preliminare

- analisi finalizzata all'identificazione degli obiettivi, alla raccolta delle informazioni, alla verifica del livello di conformità alla normativa in materia di protezione dei dati, misurazione del livello di esposizione dei rischi associati al trattamento dei dati;
- Verifica della mappatura dei trattamenti dei dati personali effettuati con strumenti cartacei, elettronici e/o informatici, analisi della tipologia dei dati trattati, delle finalità per cui sono trattati e degli interessati (registro dei trattamenti) e classificazione del rischio privacy, anche dei dati non strutturati;

LE ASSICURAZIONI DI ROMA • MUTUA ASSICURATRICE ROMANA • Iscritta alla Sez. I dell'Albo delle Imprese istituito presso l'IVASS, al n. 1.00040 Fondo di Garanzia statutario € 16.000.000,00 i.v. • Autorizzata all'esercizio assicurativo con D.M. 26/11/1984 in G. U. n. 357 del 31/12/1984 suppl. ord. 79 e con Provv. ISVAP n. 2602 del 28/3/2008 in Boll. ISVAP, Anno III n. 3 • Registro delle Imprese di Roma n. 1567/71 • C.C.I.A.A. di Roma n. 340805 C. F. 01089780587 P. IVA 00960361004 • Sede legale: Italia - 00153 Roma, Lungotevere R. Sanzio, 15 • Tel. 06/5878.1 • Fax 06/5878237 • adir@pec.it • www.adir.it

- Verifica delle "valutazioni di impatto" (Data Protection Impact Assessment - DPIA), particolarmente per quelle considerate "obbligatorie" dalla normativa, e individuazione delle misure idonee atte a garantire le prescrizioni della norma, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento;
- Verifica della procedura di gestione degli incidenti/data breach e conseguente attivazione del registro di violazione dei dati;
- individuazione delle misure organizzative e tecniche che consentano di avere un controllo continuo sulla conformità alla normativa;
- strategia di gestione dei rischi privacy.

Fase successiva

- riesame/aggiornamento delle "valutazioni di impatto" (DPIA) e rischi privacy in allineamento alle evoluzioni interne e/o alle direttive dell'Autorità Garante Privacy (Garante), nuove leggi, regolamenti etc.;
- attivazione del registro dei trattamenti eseguiti dalle terze parti;
- predisposizione/aggiornamento della regolamentazione aziendale in tema di trattamento dei dati personali;
- elaborazione, redazione od aggiornamento dei moduli per il consenso, delle informative sul trattamento dei dati personali, degli atti di nomina dei responsabili, degli incaricati;
- consulenza sugli obblighi derivanti dal GDPR e dalle ulteriori disposizioni legislative, provvedimenti e linee guida del Garante e conseguente aggiornamento del sistema privacy;
- strutturazione di un organigramma privacy finalizzato alla distribuzione delle responsabilità interne all'azienda del trattamento dati;
- analisi del sistema di videosorveglianza e aggiornamento alla normativa vigente.

Per le predette attività di consulenza deve essere garantita la presenza on site secondo modalità da concordarsi con la committenza, quantificata nella misura minima di 160 ore/annue

Resta inteso che, eventuali ore di presenza on site non utilizzate nel primo anno per esigenze di AdiR, incluse quelle riferite ai primi due mesi, saranno godute dalla Società nel periodo contrattuale successivo.

Qualora nel corso dell'esecuzione del contratto si rendesse necessario ricorrere all'assistenza on site per un numero di ore superiore a quello minimo complessivamente previsto (o a quello complessivo migliorativo indicato nell'offerta tecnica), sarà corrisposto il costo orario pari a quello indicato nell'offerta economica.

ATTIVITA' DI DATA PROTECTION OFFICER (DPO)

Oltre alle attività indicate al precedente punto, al DPO, quale responsabile della protezione dei dati, competono le seguenti prestazioni previste dall'art. 39 del GDPR (a titolo esemplificativo e non esaustivo):

- redigere un piano di lavoro;
- informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento dei dati in merito agli obblighi vigenti relativi alla protezione dei dati;
- sorvegliare l'osservanza della normativa vigente in materia nonché delle politiche del titolare o del responsabile del trattamento relative alla 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;
- assistere il titolare o responsabile del trattamento nel controllo del rispetto a livello interno del regolamento europeo n. 679/2016;
- garantire attività di informazione, consulenza e indirizzo nei confronti del titolare, del responsabile e del personale che partecipa ai trattamenti e alle connesse attività di controllo;

LE ASSICURAZIONI DI ROMA • MUTUA ASSICURATRICE ROMANA • Iscritta alla Sez. I dell'Albo delle Imprese istituito presso l'IVASS, al n. 1.00040 Fondo di Garanzia statutario € 16.000.000,00 i.v. • Autorizzata all'esercizio assicurativo con D.M. 26/11/1984 in G. U. n. 357 del 31/12/1984 suppl. ord. 79 e con Prov. ISVAP n. 2602 del 28/3/2008 in Boll. ISVAP, Anno III n. 3 • Registro delle Imprese di Roma n. 1567/71 • C.C.I.A.A. di Roma n. 340805 C. F. 01089780587 P. IVA 00960361004 • Sede legale: Italia - 00153 Roma, Lungotevere R. Sanzio, 15 • Tel. 06/5878.1 • Fax 06/5878237 • adir@pec.it • www.adir.it

- cooperare e fungere da punto di contatto con l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva ed effettuare, se del caso, consultazioni relativamente ad ogni altra questione: il DPO facilita 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;
- fungere da punto di contatto per gli interessati in merito al trattamento dei loro dati personali e all'esercizio dei diritti, comunicando con gli interessati in modo efficiente;
- considerare debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo;
- riferire riguardo alle indicazioni/raccomandazioni fornite nel quadro delle sue funzioni;
- fornire il reporting riguardo al livello di conformità al GDPR;
- redigere una relazione annuale delle attività svolte;
- programmare l'attività di formazione ed aggiornamento annuale degli operatori della Società, in accordo con la stessa, sulle problematiche e la legislazione concernente la materia del trattamento dei dati;
- evadere i quesiti di natura legale in materia di privacy richiesti dalla committenza entro il termine massimo di 7 (sette) giorni.

Nell'adempimento dei propri compiti, il DPO dovrà attenersi al segreto e alla riservatezza: tali vincoli non precludono la possibilità per il DPO di contattare e chiedere chiarimenti all'autorità di controllo.
Per garantire le prestazioni previste dal presente articolo e dalle disposizioni in materia, il DPO, pur potendosi avvalere di un team (staff tecnico), funge da contatto principale; per tale ragione è necessaria una chiara ripartizione dei compiti.
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.

Requisiti del Responsabile della protezione dati (DPO)

Il DPO deve possedere:

- Comprovata conoscenza della normativa e delle prassi nazionali ed europee in materia di protezione dei dati, compresa un'approfondita conoscenza del GDPR;
- Attestati di partecipazioni a corsi di formazione professionale che attestino la comprovata esperienza in campo Data Protection.
- Comprovata esperienza Tecnico Organizzativo in campo Data Protection;
- Aver Svolto nell'ultimo anno, almeno le seguenti attività:
  - Audit di prima, seconda o terza parte in campo Data Protection;
  - Servizi di Pre-assessment in campo Privacy relativamente alla compliance al Regolamento EU 2017/679;
- Servizi di Pre-Audit per enti di certificazione di parte terza accreditati Accredia conformemente alla norma ENISO/IEC 17065/2012 avranno titolo preferenziale.
- conoscenza specifica dei settori di attività Assicurative, delle norme e procedure amministrative applicabili.
- **Conoscenza e/o eventuali certificazioni secondo lo schema di certificazione ISDP1003:2015 o conformi a quanto stabilito dall'art. 43 del Regolamento Eu 206/679 avrà titolo preferenziale in quanto la committente ha conseguito la suddetta certificazione per la protezione dei Dati personali.**

Esperienza richiesta al DPO e al Team (staff tecnico)

LE ASSICURAZIONI DI ROMA • MUTUA ASSICURATRICE ROMANA • Iscritta alla Sez. I dell'Albo delle Imprese istituito presso l'IVASS, al n. 1.00040 Fondo di Garanzia statutario € 16.000.000,00 i.v. • Autorizzata all'esercizio assicurativo con D.M. 26/11/1984 in G. U. n. 357 del 31/12/1984 suppl. ord. 79 e con Provv. ISVAP n. 2602 del 28/3/2008 in Boll. ISVAP, Anno III n. 3 • Registro delle Imprese di Roma n. 1567/71 • C.C.I.A.A. di Roma n. 340805 C. F. 01089780587 P. IVA 00960361004 • Sede legale: Italia - 00153 Roma, Lungotevere R. Sanzio, 15 • Tel. 06/5878.1 • Fax 06/5878237 • adir@pec.it • www.adir.it

Il team, selezionato per consapevolezza e attenzione alla problematica, dovrà essere messo a disposizione secondo Regolamento e in ragione delle competenze e le conoscenze specialistiche pertinenti all'incarico per sensibilità, complessità e quantità dei dati e delle informazioni trattate dalla committente.

Il team RDP avrà quindi:

- Attestati di partecipazioni a corsi di formazione professionale che attestino la comprovata esperienza in campo Data Protection.
- conoscenza della normativa e delle prassi nazionali ed europee in materia di protezione dei dati, compresa un'approfondita conoscenza del RGPD;
- integrità ed elevati standard deontologici;
- aggiornamento adeguato e continuo alla problematica inerente la Privacy;
- familiarità con le operazioni di trattamento svolte del cliente;
- conoscenza dello specifico settore di attività e dell'organizzazione del titolare;
- conoscenza approfondita delle norme e procedure amministrative applicabili dal titolare del trattamento;
- familiarità con tecnologie informatiche e misure di sicurezza dei dati;
- formazione permanente;
- capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione del titolare per dare attuazione a elementi essenziali quali:
  - i principi fondamentali del trattamento
  - i diritti degli interessati
  - la protezione dei dati sin dalla fase di progettazione e per impostazione predefinita
  - i registri delle attività di trattamento
  - la sicurezza dei trattamenti
  - la notifica e comunicazione delle violazioni di dati personali.
  - **Offerta tecnica**

Per attestare il profilo professionale dell'operatore economico invitato alla procedura, è necessario allegare:

A1) Curriculum vitae (CV), esclusivamente in formato Europass, con precisazione del titolo di studio, numero di anni di esperienza, descrizione esperienze, profilo professionale, competenze ed eventuali iscrizioni ai registri Accreditati ACCREDIA.

A2) Eventuale Certificazione che attesta il possesso dei "requisiti professionali di Responsabile Protezione dei Dati" secondo la norma UNI 11697:2017 e relativi attestati di frequenza, con verifica dell'apprendimento finale, di Corsi di Aggiornamento .

A3) Dichiarazione prodotta, come da fac-simile allegato **"Elenco dettagliato degli AUDIT di prima, seconda o terza parte secondo lo schema ISDP10003:2015;**

A4) Eventuale certificazione su schemi di Audit riconosciuti conformemente alla norma EN ISO/IEC 17065/2012

Sarà obbligatorio, in caso di aggiudicazione preliminare, fornire per la relativa documentazione a comprova di quanto dichiarato.

Eventuali Certificazioni secondo lo schema ISDP10003:2015

B) l'impegno ad effettuare eventuali sopralluoghi settimanali aggiuntivi rispetto al numero minimo indicato nel presente Capitolato, indicandone il numero.

La mancata presentazione della documentazione attestata alle lettere A e B implicherà l'esclusione dell'operatore economico alle successive fasi di valutazione.

Si precisa che non verrà assegnato alcun punteggio agli incarichi incompleti e/o poco chiari o ove sia assente la documentazione a comprova dell'incarico svolto.

Si precisa altresì che non verranno considerate valide le figure professionali che non produrranno in parte o tutta la documentazione richiesta.

La descrizione/documentazione tecnica dovrà essere formulata esclusivamente in lingua italiana.
La gara sarà aggiudicata secondo il criterio dell'offerta economicamente più vantaggiosa a seguito di graduatoria redatta tra le offerte ritenute tecnicamente idonee e sottoposte a verifica di congruità, con riferimento ai punteggi calcolati sulla base dei seguenti criteri:

Offerta tecnica: massimo punteggio complessivo 70 (settanta), articolata nei seguenti sub-punteggi:

Requisiti Tecnici	**Massimo punteggio**	**Criteri di assegnazione dei punteggi tecnici**
Iscrizione a Registri conformi alla norma **EN ISO/IEC 17065:2012** (requisiti minimi essenziali)	**10**	Il punteggio verrà attribuito in base al numero di certificazioni rilasciate da Enti Accreditati Accredia. Verrà attribuito un punteggio pari a 2 punti a certificato fino ad un massimo di 10 punti.
Elenco dettagliato degli Audit di prima e seconda parte, come previsto al precedente punto A3) del paragrafo "Offerta Tecnica", per un massimo di 10 Audit	**20**	Verrà attribuito un punteggio pari a 2 punti per ogni Audit dichiarato fino ad un massimo di 20 punti. Ai fini della graduatoria di gara, il punteggio finale totale del suddetto requisito, sarà determinato dalla somma dei punteggi assegnati.

LE ASSICURAZIONI DI ROMA • MUTUA ASSICURATRICE ROMANA • Iscritta alla Sez. I dell'Albo delle Imprese istituito presso l'IVASS, al n. 1.00040 Fondo di Garanzia statutario € 16.000.000,00 i.v. • Autorizzata all'esercizio assicurativo con D.M. 26/11/1984 in G. U. n. 357 del 31/12/1984 suppl. ord. 79 e con Provv. ISVAP n. 2602 del 28/3/2008 in Boll. ISVAP, Anno III n. 3 • Registro delle Imprese di Roma n. 1567/71 • C.C.I.A.A. di Roma n. 340805 C. F. 01089780587 P. IVA 00960361004 • Sede legale: Italia - 00153 Roma, Lungotevere R. Sanzio, 15 • Tel. 06/5878.1 • Fax 06/5878237 • adir@pec.it • www.adir.it

Elenco dettagliato degli Audit o pre-audit di **terza parte**, come previsto al precedente punto A3) del paragrafo "Offerta Tecnica", per un massimo di 10 Audit	**20**	Verrà attribuito un punteggio pari a 2 punti per ogni Audit dichiarato fino ad un massimo di 20 punti. Ai fini della graduatoria di gara, il punteggio finale totale del suddetto requisito, sarà determinato dalla somma dei punteggi assegnati.
Per il Team tecnico di supporto al DPO eventuali certificazioni sullo schema ISDP10003:2015 o equivalenti ma conformi alla normativa EN ISO/IEC 17065/2012 e UNI 11697:2017	**10**	Il punteggio sarà attribuito per ogni certificazione e comprovata conoscenza dello schema di certificazione che il Team di supporto al DPO avrà, relativamente alla certificazione volontaria che AdiR ha scelto di ottenere. Verrà attribuito un punteggio di due per ogni persona del Team di supporto certificata nelle norme o schemi identificati fino ad un massimo di 10.
Numero dei sopralluoghi aggiuntivi rispetto a quelli minimi richiesti	**10**	Fermo restando il numero minimo richiesto di 160/ore annue per presenza on-Site per ciascun sopralluogo dichiarato in più dal partecipante, verrà attribuito un punteggio pari a 2 punti fino ad un massimo di 10 punti.
TOTALE	**70**	

AdiR non procederà all'apertura dell'offerta economica degli operatori economici la cui offerta tecnica non abbia raggiunto, prima della riparametrazione come di seguito rappresentato, un punteggio minimo di 35 (trentacinque) punti.

Successivamente per ciascuno dei criteri sopra previsti, si procederà a riparametrare i sub-punteggi attribuiti riportando il valore 1 al concorrente che avrà conseguito il sub-punteggio migliore e quindi ri-proporzionando ad esso il valore dei sub- punteggi conseguiti dagli altri concorrenti. Una volta ultimata l'assegnazione dei sotto-punteggi a tutti i concorrenti, si procederà con la riparametrazione della somma degli stessi rispetto al punteggio massimo di 70 (somma dei sub-punteggi massimi dei parametri).

Di conseguenza il punteggio massimo sopra previsto, pari a 70, verrà attribuito al concorrente che avrà conseguito l'offerta più alta e ai restanti verrà assegnato il punteggio in proporzione al migliore, secondo la seguente formula:

Px = Pi/Pmax*70
dove
Pi = punteggio attribuito alla i-esima offerta
Pmax = massimo punteggio conseguito tra le offerte

LE ASSICURAZIONI DI ROMA • MUTUA ASSICURATRICE ROMANA • Iscritta alla Sez. I dell'Albo delle Imprese istituito presso l'IVASS, al n. 1.00040 Fondo di Garanzia statutario € 16.000.000,00 i.v. • Autorizzata all'esercizio assicurativo con D.M. 26/11/1984 in G. U. n. 357 del 31/12/1984 suppl. ord. 79 e con Provv. ISVAP n. 2602 del 28/3/2008 in Boll. ISVAP, Anno III n. 3 • Registro delle Imprese di Roma n. 1567/71 • C.C.I.A.A. di Roma n. 340805 C. F. 01089780587 P. IVA 00960361004 • Sede legale: Italia - 00153 Roma, Lungotevere R. Sanzio, 15 • Tel. 06/5878.1 • Fax 06/5878237 • adir@pec.it • www.adir.it

Px = punteggio tecnico da assegnare al partecipante alla gara in esame

Offerta economica: massimo punteggio 30 (trenta)
L'importo proposto per gli incarichi di Responsabile Protezione dei Dati (DPO), nonché per i servizi richiesti di cui ai punti precedenti, a partire dal 20 Maggio 2018, dovrà essere esplicitato al netto del contributo previdenziale e dell'IVA al 22%.
Al partecipante che avrà offerto la percentuale di sconto più alta, verrà attribuito il punteggio massimo sopra indicato, ossia 30 punti.
Agli altri partecipanti verrà attribuito un punteggio determinato in proporzione al rapporto tra la migliore offerta di cui sopra e la propria offerta, secondo la seguente formula:

Xn = P1/Pn * 30

Dove:
Xn = punteggio da assegnare al partecipante alla gara in esame
P1 = migliore offerta economica presentata
Pn = offerta economica del partecipante alla gara in esame
Il massimo punteggio ottenibile è pertanto pari a 100 punti.
L'assegnazione del punteggio complessivo finale sarà pari alla sommatoria del punteggio attribuito all'offerta tecnica (massimo 70) ed all'offerta economica (massimo 30).

Si segnala che la congruità delle offerte presentate sarà valutata sulle offerte che presentino sia i punti relativi al prezzo, sia la somma dei punti relativi agli altri elementi di valutazione, entrambi pari o superiori ai quattro quinti dei corrispondenti punti massimi previsti nella presente RdO.
Qualora l'offerta dovesse risultare anormalmente bassa a seguito dell'applicazione del suddetto criterio, AdiR procederà con la richiesta agli operatori economici interessati di giustificazione dell'offerta alle condizioni e termini indicati all'art. 97 del Codice degli Appalti.

LE ASSICURAZIONI DI ROMA • MUTUA ASSICURATRICE ROMANA • Iscritta alla Sez. I dell'Albo delle Imprese istituito presso l'IVASS, al n. 1.00040 Fondo di Garanzia statutario € 16.000.000,00 i.v. • Autorizzata all'esercizio assicurativo con D.M. 26/11/1984 in G. U. n. 357 del 31/12/1984 suppl. ord. 79 e con Provv. ISVAP n. 2602 del 28/3/2008 in Boll. ISVAP, Anno III n. 3 • Registro delle Imprese di Roma n. 1567/71 • C.C.I.A.A. di Roma n. 340805 C. F. 01089780587 P. IVA 00960361004 • Sede legale: Italia - 00153 Roma, Lungotevere R. Sanzio, 15 • Tel. 06/5878.1 • Fax 06/5878237 • adir@pec.it • www.adir.it