**PROCEDURA DI GARA APERTA**

**per l'affidamento del servizio di Responsabile della Protezione dei Dati personali esterno e servizi ad esso connessi ai sensi dell'art. 37 del Regolamento UE 679/2016**

# CAPITOLATO PRESTAZIONALE E DESCRITTIVO

## I. Contesto di riferimento

Il 14 aprile 2016 il Parlamento e il Consiglio Europeo hanno approvato in via definitiva il Regolamento in materia di Protezione dei Dati Personali (di seguito "GDPR" o "Regolamento"), entrato in vigore il 25 maggio 2016. Decorso un periodo di transizione, pari a due anni, dal 25 maggio 2018 le disposizioni in esso contenute sono divenute direttamente applicabili in tutta l'Unione Europea a chiunque raccolga, processi o, in generale, tratti dati personali di una «persona fisica» che si trova nell'Unione Europea. L'Italia ha risposto positivamente al Regolamento attraverso il D.Lgs. 101/2018 che sancisce i criteri d'interazione tra il Regolamento Europeo e la precedente normativa nazionale relativa alla Protezione dei Dati Personali introdotta con il D.lgs. 196/2003.

L'attuale quadro normativo inquadra ANPAL (di seguito "Agenzia") come Titolare del trattamento dei dati rispetto alle proprie attività istituzionali con impatto sulla materia.

Al fine di ottemperare agli obblighi in carico al Titolare del Trattamento, ANPAL ha intrapreso un percorso di Adeguamento finalizzato a mettere in atto le misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che i trattamenti di Dati Personali effettuati all'interno dell'Agenzia avvengano in conformità alla normativa vigente in materia di protezione dei dati personali.

Con riferimento al suddetto percorso di adeguamento, è necessario specificare che l'indirizzamento e la gestione degli aspetti connessi alla protezione dei Dati Personali risulta particolarmente articolata poiché il D. Lgs 150/2015 conferisce all'Agenzia il ruolo di coordinamento della rete dei servizi per le politiche attive del lavoro e pertanto, in virtù del suddetto compito istituzionale, l'Agenzia interagisce con i seguenti soggetti pubblici e privati facenti parte della rete dei servizi per le politiche attive del lavoro:

a) le strutture regionali per le Politiche Attive del Lavoro di cui all'articolo 11 del D.Lgs 150/2015;

b) INPS, in relazione alle competenze in materia di incentivi e strumenti a sostegno del reddito;

c) INAIL, in relazione alle competenze in materia di reinserimento e di integrazione lavorativa delle persone con disabilità da lavoro;

d) le Agenzie per il lavoro di cui all'articolo 4 del decreto legislativo 10 settembre 2003, n. 276, i soggetti autorizzati allo svolgimento delle attività di intermediazione ai sensi dell'articolo 6 del medesimo decreto legislativo e i soggetti accreditati ai servizi per il lavoro ai sensi dell'articolo 12 del D.Lgs. 150/2015;

e) i fondi interprofessionali per la formazione continua di cui all'articolo 118 della legge 23 dicembre 2000, n. 388;

e) i fondi bilaterali di cui all'articolo 12, comma 4, del decreto legislativo n. 276 del 2003;

h) l'Istituto per lo sviluppo della formazione professionale dei lavoratori (ISFOL) e Italia Lavoro S.p.A.;

i) il sistema delle Camere di commercio, industria, artigianato e agricoltura, le università e gli istituti di scuola secondaria di secondo grado.

In aggiunta, l'indirizzamento e la gestione degli aspetti connessi alla protezione dei Dati Personali risulta particolarmente critica a causa delle significativa dipendenza dal punto di vista tecnico dal Ministero del Lavoro e delle Politiche sociali, con cui sussiste una stretta relazione che si esprime, tra gli altri, nell'avvalimento ancora in vigenza dei servizi connessi all'esercizio e manutenzione dell'infrastruttura IT, ossia dei sistemi / risorse / archivi a supporto del trattamento di Dati Personali.

Lo svolgimento delle attività previste dal percorso di adeguamento alla normativa in materia di protezione dei dati personali hai previsto il coinvolgimento di ogni singola Divisione/Struttura di ANPAL attraverso degli incontri mirati a sensibilizzare ciascun attore circa le tematiche Privacy e ad identificare tutte le attività di trattamento di Dati Personali eseguite da ciascuna Divisione/Struttura.

In particolare, il percorso di adeguamento normativo si è concretizzato nella realizzazione, tra l'altro, della seguente documentazione:

- Registro delle Attività di Trattamento ex art. 30 del GDPR;
- Processi e relative procedure operative in termini di Data Privacy, ivi inclusi il processo di Gestione delle Istanze degli interessati, il processo di gestione dei Data Breach e il processo per la realizzazione della valutazione di impatto sulla protezione dei dati;

- Informative sul trattamento dati rese da ANPAL ai sensi degli artt. 13 e seguenti del GDPR (e.g. beneficiari iniziative e misure di politica attiva, dipendenti, etc.);
- Modello Organizzativo per gestire le tematiche Privacy, che definisce i ruoli e le responsabilità di tutti gli attori coinvolti nelle attività di trattamento dei dati personali, nonché il flusso di comunicazione interno da seguire nel corso delle singole attività con impatto sui dati personali;
- Modello di accordo sul trattamento dei dati personali da sottoscrivere con tutti i soggetti terzi che forniscano ad ANPAL servizi / prodotti che implichino il trattamento di Dati Personali per conto dell'Agenzia stessa ex art. 28 del GDPR;
- Piano di Formazione base per tutti i soggetti interni autorizzati ai trattamenti di Dati Personali;
- Attività di "Pre-DPIA", finalizzata ad identificare i trattamenti afferenti a ciascuna Divisione/Struttura di ANPAL che presentino un "rischio elevato" per gli interessati;
- Realizzazione dell'attività di DPIA ex art. 35 del GDPR sui trattamenti a "rischio elevato".

Oltre alle attività summenzionate poste in essere dall'Agenzia nell'ambito del percorso di adeguamento normativo, il Regolamento UE 679/2016 individua tra gli obblighi in capo al Titolare del Trattamento quello di designare il responsabile della protezione dei dati, in quanto l'Art. 37 comma 1 recita che il Titolare del trattamento designa sistematicamente un Responsabile della Protezione dei Dati (di seguito anche "*Data Protection Officer*" o, per brevità, "DPO"), ogniqualvolta il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico.

Il Gruppo dell'articolo 29 per la tutela dei dati (WP29, sostituito dal Comitato europeo per la protezione dei dati) ritiene che la classificazione di un'autorità pubblica o di un organismo pubblico deve essere determinata in base al diritto nazionale. Di conseguenza, le autorità pubbliche e gli enti includono le autorità nazionali, regionali e locali, ma il concetto, ai sensi delle leggi nazionali applicabili, comprende anche una serie di altri organismi. Considerato che l'Agenzia rientra in tali casi, la designazione di un DPO è obbligatoria.

Ai sensi dell'Art. 37 comma 6, il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.

Quando la funzione del DPO è esercitata da un fornitore esterno, un gruppo di persone che lavorano per questo soggetto può efficacemente svolgere i compiti di DPO come team, sotto la responsabilità di una figura coordinatrice, poiché il WP suggerisce che per motivi di chiarezza giuridica e di buona organizzazione si raccomanda di avere una chiara ripartizione

dei compiti all'interno del team DPO designando sempre una figura di riferimento.

In tali circostanze a ciascuno dei suoi membri aventi ruolo di DPO si applicano le disposizioni di cui agli Articoli 37, 38 e 39 del GDPR, inclusi il requisito di assenza di conflitti di interessi e la garanzia che non siano attuate penalizzazioni (risoluzione del contratto di servizi o rimozione di un membro dell'organizzazione esterna) a causa dello svolgimento delle attività di DPO.

## II. Oggetto dell'appalto

Con particolare riferimento al quadro normativo attuale e al contesto di riferimento della scrivente Agenzia, il supporto richiesto riguarda lo svolgimento del servizio di Responsabile della Protezione dei Dati personali esterno e servizi ad esso connessi ai sensi dell'art. 37 del Regolamento UE 679/2016. Nel dettaglio, i servizi oggetto di affidamento verteranno, esemplificativamente, sulle seguenti attività che secondo il disposto dell'Articolo 39 del Regolamento UE 679/2016 sono intese come le attività generalmente demandate alla figura di DPO, volte a promuovere la cultura della protezione dei dati e l'implementazione degli elementi essenziali del regolamento:

- Sorvegliare le evoluzioni normative, sia a livello nazionale sia internazionale, in materia di protezione dei dati personali e comunicarle prontamente al Titolare del trattamento;
- Monitorare l'osservanza della scrivente Agenzia alla normativa vigente in materia di protezione dei dati personali eseguendo delle analisi di dettaglio "a campione" per verificare l'aggiornamento continuo delle procedure e della documentazione adottate dal titolare in materia di data protection. In particolare, i piani di verifica hanno ad oggetto la correttezza delle procedure e della documentazione adottata da ANPAL, la validità dell'analisi dei rischi eseguita dai singoli Delegati interni dei trattamenti, nonché la verifica sull'efficacia e sull'adeguatezza delle misure di sicurezza implementate;
- Fornire supporto al Titolare per la definizione dei contenuti dei corsi di formazione rivolti a Delegati interni del trattamento e agli autorizzati nonché monitorare l'effettiva organizzazione ed erogazione dei suddetti corsi;
- Assicurare la tenuta, la conservazione e l'aggiornamento del Registro delle attività di trattamento redatto dalla Scrivente ai sensi dell'Art. 30 del Regolamento UE 679/2016, nonché verificare la correttezza e completezza delle informazioni riportate nel Registro circa i trattamenti di dati personali eseguiti dal personale autorizzato di ANPAL;
- Supportare l'Agenzia nella gestione ed analisi del Data Breach attraverso la presa in carico delle seguenti attività:

  - Collaborazione con i DPO di eventuali Contitolari o Responsabili del trattamento nella gestione del Data Breach;
  - Notifica del Data Breach all'Autorità di Controllo e agli interessati;
  - Monitoraggio del processo di gestione del breach in ottica continuous improvement;
  - Monitoraggio e controllo della tenuta del Data Breach Inventory.
- Supportare il Titolare nell'integrazione nei processi interni dei principi di Privacy By Design e Privacy By Default, nonché di security by design in fase di progettazione, evoluzione o verifica di applicativi utilizzati nell'ambito del trattamento di dati personali e monitorare l'effettiva implementazione degli stessi;
- Supportare, ove richiesto, il Titolare del Trattamento nell'attività di valutazione di impatto sulla protezione dei dati personali (DPIA) ai sensi dell'art. 35 del GDPR. I contributi che saranno richiesti in tale attività, esemplificativamente, consisteranno in:
  - Supporto nella definizione e miglioramento continuo della metodologia di *data protection impact assessment* al fine di essere sempre allineati ai migliori standard internazionali / prassi di settore;
  - Supporto nell'applicazione della metodologia ai singoli casi d'uso;
  - Sorveglianza circa l'effettivo e corretto svolgimento delle singole DPIA e dell'effettiva attuazione delle misure di sicurezza identificate nel corso della valutazione d'impatto;
- Cooperare con l'Autorità di controllo al fine di agevolare l'accesso della stessa ai documenti e alle informazioni relative ai trattamenti effettuati, nonché fungere da "punto di contatto" per l'Autorità medesima in riferimento a questioni specifiche, tra cui la consultazione preventiva di cui all'art. 36 del Regolamento;
- Svolgere le eventuali attività di consultazione all'Autorità che dovessero rendersi opportune in merito ad ulteriori tematiche relative alla tutela dei dati personali;
- Fungere da "punto di contatto" tra gli Interessati (Data Subject) e l'Agenzia, garantendo che le richieste degli stessi, se legittime, siano evase e riscontrate nei modi e nei tempi indicati dal GDPR;
- Formulare pareri per le richieste provenienti da parte delle singole Divisioni/Strutture coinvolte nei trattamenti di dati personali;
- Fornire supporto nella formulazione di pareri / note tecniche per le richieste provenienti da parte dei soggetti facenti parte della rete dei servizi per le politiche attive del lavoro;
- Fornire supporto nell'elaborazione nella sottoscrizione degli Accordi relativi la Contitolarità/Responsabili Esterni con i soggetti facenti parte della rete dei servizi per le politiche attive del lavoro (e.g. Regioni).

## III. Composizione del Gruppo di lavoro e competenze richieste

Per l'esecuzione del servizio in affidamento l'Operatore dovrà mettere a disposizione un Gruppo di Lavoro (di seguito anche "Team DPO") composto dalle seguenti figure:

- **Data Protection Officer**, responsabile della fornitura e coordinatore del Team DPO;
- **Data Protection Specialist;**
- **ICT Security Expert**.

Le risorse da impiegare nell'esecuzione del servizio in affidamento dovranno rispondere ai requisiti previsti dai profili di seguito descritti, da intendersi a tutti gli effetti come requisiti minimi.

Detto gruppo di lavoro offerto dovrà rispettare (per numerosità e qualificazione specifica delle risorse) la configurazione riportata nel presente paragrafo.

**1) Data Protection Officer**: n. 1 risorsa, per 8 giornate mese (media tendenziale), per complessive 192 giornate lavoro.

Tale figura dovrà essere in possesso dei seguenti requisiti:

- laurea o laurea magistrale in ingegneria gestionale / informatica o in discipline giuridico-economiche, oppure titoli pertinenti di livello analogo;
- esperienza professionale di almeno 5 anni, di cui almeno 4 anni con riferimento alla materia della protezione dei dati personali ed almeno 1 anno con riferimento ai servizi e alle attività oggetto del presente Capitolato regolamentare dal GDPR;
- conoscenza specialistica approfondita della normativa vigente in materia di protezione dei dati tra cui, in particolare, quella discendente dal Regolamento Europeo 2016/679, dal D. Lgs. n. 101/2018 (di adeguamento alla normativa nazionale al GDPR), nonché di Provvedimenti, Linee Guida del Garante per la Protezione dei dati personali, opinion del WP29, etc.;
- conoscenza specialistica in attività di definizione ed implementazione di policy e procedure in termini di Data Privacy (processo di Gestione delle Istanze degli interessati, processo di gestione dei Data Breach e processo per la realizzazione della valutazione di impatto sulla protezione dei dati);
- ottima conoscenza delle prassi operative, delle tecnologie e delle misure di sicurezza in materia di protezione dei dati personali, con riferimento, in particolare nel settore della Pubblica Amministrazione;
- capacità di assolvere i compiti descritti nel paragrafo *II. Oggetto dei servizi in affidamento;*

- conoscenza delle tecnologie informatiche e misure di sicurezza dei dati, con particolare riferimento alle misure di sicurezza ICT per le Pubbliche Amministrazioni, definite dall'Agenzia per l'Italia digitale (AgId);
- capacità di promuovere la cultura della protezione dei dati personali all'interno della scrivente Agenzia;
- capacità di instaurare relazioni proficue con tutte le Divisioni / Strutture interne con cui dovrà interagire.

Sono positivamente valutate, in particolare:

- conoscenza e abilità professionali relativamente alle attività di Data Protection / Servizi di Data Privacy di competenza dei soggetti facenti parte della rete dei servizi per le politiche attive del lavoro;
- conoscenza della normativa e delle procedure applicabili alle Pubbliche Amministrazioni, con particolare riferimento al contesto dell'Agenzia;
- conoscenza della materia di protezione dei dati connessa ai temi di gestione, monitoraggio, valutazione e controllo di interventi finanziati dai fondi comunitari;
- conoscenza specialistica degli impatti privacy connessi al Decreto Legislativo n. 150/2015 di istituzione dell'Agenzia e delle funzioni conferite alla stessa.

**2) Data Protection Specialist**: n. 1 risorsa, per 20 giornate mese (media tendenziale), per complessive 480 giornate lavoro.

Tale figura dovrà essere in possesso dei seguenti requisiti:

- conoscenza specialistica approfondita della normativa vigente in materia di protezione dei dati tra cui, in particolare, del Regolamento Europeo 2016/679, del D. Lgs. n. 101/2018 di adeguamento alla normativa nazionale al GDPR, Provvedimenti, Linee Guida del Garante per la Protezione dei dati personali, opinion del WP29, etc.;
- esperienza professionale di almeno 5 anni, di cui almeno 3 anni con riferimento alla materia della protezione dei dati personali ed almeno 1 anno con riferimento ai servizi e alle attività oggetto del presente Capitolato regolamentate dal GDPR;
- conoscenza approfondita dello scoping normativo applicabile alla scrivente Agenzia incluso, in particolare - Decreto legislativo n. 150/2015, D.L. 4/2019 - nonché dei regolamenti e delle norme nazionali e internazionali di riferimento;
- conoscenza approfondita in attività di definizione ed implementazione di policy e procedure in termini di Data Privacy (processo di Gestione delle Istanze degli interessati, processo di gestione dei Data Breach e processo per la realizzazione della valutazione di impatto sulla protezione dei dati);
- conoscenza approfondita dei Servizi e delle tematiche di Data Privacy (e.g. Modelli di nomina a Responsabile Esterno, Modelli di Contitolarità) con riferimento alle attività

di competenza dei soggetti facenti parte della rete dei servizi per le politiche attive del lavoro.

**3) ICT Security Expert**: n. 1 risorsa, per 18 giornate mese (media tendenziale), per complessive 432 giornate lavoro per l'intero periodo di fornitura del servizio.

Tale figura dovrà essere in possesso dei seguenti requisiti:

- esperienza professionale di almeno 4 anni, di cui almeno 3 anni con riferimento alla materia della protezione dei dati personali ed almeno 1 anno con riferimento ai servizi e alle attività oggetto del presente Capitolato regolamentate dal GDPR;
- ottima conoscenza delle prassi operative, delle tecnologie e delle misure di sicurezza in materia di protezione dei dati personali;
- conoscenza di best practice e standard in ambito Sicurezza delle Informazioni, quali, a titolo esemplificativo, ISO 27001, ISO 31000, ISO 29134, Misure minime di sicurezza ICT per le PA definite da AgID;
- conoscenza dello scoping normativo applicabile alla Scrivente Agenzia incluso, in particolare, il Decreto legislativo n. 150/2015 ed il D.L. 4/2019, nonché dei regolamenti e delle norme nazionali e internazionali di riferimento;
- conoscenza dell'architettura logica e fisica e del contesto applicativo dell'infrastruttura dei soggetti della rete dei servizi per le politiche attive del lavoro e delle relative policy di sicurezza.

Al soggetto aggiudicatario è riconosciuta la facoltà, qualora lo necessiti, d'intesa con l'Agenzia, di accedere ad altri servizi all'interno della medesima ANPAL, così da ricevere il supporto e le informazioni necessarie all'erogazione dei servizi richiesti.

Il DPO svolge le mansioni cui è preposto in autonomia, indipendenza e in assenza di qualsivoglia "conflitto di interesse", riportando direttamente al vertice dell'Agenzia.

Costituisce requisito indispensabile che il soggetto aggiudicatario disponga di un livello adeguato di copertura assicurativa contro i rischi professionali.

Fermo questo, i contenuti specifici del servizio potranno essere ulteriormente precisati e dettagliati in sede di formulazione dell'offerta tecnica di gara.

## IV. Durata del rapporto e tempistica per lo svolgimento del servizio richiesto

La specifica tempistica di esecuzione dei servizi tutti suindicati è ovviamente strettamente dipendente dalle concrete occorrenze di supporto che andranno a manifestarsi in capo all'Agenzia.

In ogni caso, la durata complessiva del contratto è stabilita in **mesi 24 (ventiquattro)**.

La durata del contratto come sopra indicata potrà essere modificata per il tempo strettamente necessario alla conclusione delle procedure necessarie per l'individuazione del nuovo contraente ai sensi dell'art. 106, comma 11 del Codice, comunque per un periodo non superiore a mesi 4.

## V. Ammontare massimo dei corrispettivi (base d'asta)

Il corrispettivo massimo onnicomprensivo per l'espletamento dei servizi oggetto di gara è stabilito in **€ 402.720,00 (quattrocentoduemilasettecentoventi/00)** oltre IVA ed altri eventuali oneri di legge, da intendersi quindi a tutti gli effetti quale base d'asta della procedura. Il corrispettivo di effettiva competenza dell'Operatore affidatario sarà determinato dal numero delle giornate di lavoro effettivamente erogate dal Gruppo di Lavoro dedicato moltiplicato per le tariffe di impegno unitarie stabilite per ciascuna figura. Tali tariffe saranno quelle specificate nell'offerta economica dei concorrenti.

Fermo quanto sopra, non saranno ammesse offerte che prevedano tariffe giornaliere di impegno per figura superiori anche ad una soltanto delle tariffe sotto indicate:

| | |
|---|---|
| DPO: | € 590,00; |
| Data Protection Specialist: | € 370,00; |
| ICT Security Expert: | € 310,00. |

Si sottolinea che il prodotto di tali tariffe massime per i volumi complessivi di giornate lavoro per figura previsti al precedente paragrafo 3 conduce ad un importo superiore alla base d'asta. **Per l'ammissibilità dell'offerta**, una o più delle suindicate tariffe dovranno quindi necessariamente essere oggetto di riduzione, di modo che il prezzo complessivo offerto sia uguale o inferiore al prezzo complessivo a base d'asta. Tale dispositivo viene introdotto al fine di accrescere, per i potenziali concorrenti, i margini di progettazione economica dell'intervento.

## VI. Pianificazione e consuntivazione delle attività

L'affidatario del contratto dovrà formulare e sottoporre all'approvazione di ANPAL, entro 10 giorni dalla data di avvio delle attività, un Piano Generale di Lavoro di livello esecutivo, che, tenendo conto di tutto quanto richiesto dal capitolato, illustrerà nello specifico gli interventi pianificati nel tempo e distribuiti tra le risorse umane a disposizione.
Le attività svolte dovranno essere descritte, con cadenza trimestrale, da parte dell'Operatore affidatario, in apposita relazione di avanzamento lavori.

Tali relazioni dovranno svilupparsi lungo le medesime direttrici di servizio previste nel Piano di lavoro generale, così da permettere un agevole ed efficace raffronto fra l'andamento delle attività programmato e l'andamento invece concretamente registrato dalle medesime. Nelle stesse relazioni dovrà essere analiticamente indicato il volume di impegno, in termini di giornate lavoro, registrato per ciascun componente del gruppo di lavoro.
In allegato a tali relazioni dovrà essere consegnata l'eventuale documentazione integrativa utile alla illustrazione e dimostrazione dell'attività svolta (e comunque tutta la documentazione che l'Amministrazione in corso di rapporto riterrà di richiedere o acquisire).

## VII. TRATTAMENTO DEI DATI

Rispetto all'acquisizione, gestione e conservazione di eventuali dati di cui entrerà in possesso in esecuzione del servizio oggetto di gara, l'Operatore affidatario potrà essere designato quale responsabile del trattamento dei dati relativi designato dalla scrivente Agenzia, in conformità alla normativa comunitaria e nazionale applicabile in materia di tutela dei dati personali.

## VIII. OBBLIGHI E DIRITTI DELLE PARTI

Gli obblighi e i diritti delle parti, fermo quanto quivi stabilito, sono precisati nello schema di contratto allegato al presente capitolato di gara, da intendersi parte integrante del medesimo.

Al momento della stipula del contratto di affidamento a tale schema - comunque entro i limiti consentiti dall'ordinamento - potranno essere apportate quelle variazioni e/o integrazioni che risultassero in via obiettiva necessarie a seguito di modifiche al quadro regolamentare e programmatico di riferimento, nonché per obiettive sopravvenute preminenti ragioni di interesse pubblico.

FINE DOCUMENTO