SCHEDA TECNICA SERVIZI PER L'APPLICAZIONE DEL REGOLAMENTO (UE) 2016/679

L'Azienda Ospedaliera Villa Sofia Cervello intende selezionare un fornitore di servizi per l'applicazione del nuovo regolamento Europeo sulla protezione dei dati, di seguito GDPR.

Il fornitore di servizi deve avere competenze specifiche nella consulenza nei seguenti ambiti:

- D. Lgs. 196/03 Privacy e DPS;
- Regolamento (UE) 2016/679
- Qualità aziendale dei processi (ISO9001);
- Information security e Security Compliance (ISO27001:2005);
- Risk Assessment & Risk Management (ISO 31000);
- Business Continuity & Disaster Recovery;
- Vulnerability Assessment & Penetration Tests;
- Project e change management;
- Formazione;
- Audit;
- Pianificazione, progettazione, definizione dei requisiti e supporto all'implementazione delle infrastrutture ICT e specificatamente dei sistemi di sicurezza;

Elenco dei servizi richiesti per l'applicazione del GDPR:

1) Coadiuvare la stazione appaltante nella definizione dei responsabili del trattamento (come da articolo 4 del GDPR).

2) Coadiuvare la stazione appaltante nella mappatura dell'azienda, dando una rilevanza all'organigramma in modo da poter attribuire funzionalmente

ogni risorsa ad una unità operativa, includendo non solo il personale dipendente ma tutti coloro che hanno una
qualche attività con l'impresa stessa (ogni persona che può essere coinvolta in un processo di trattamento privacy)

3) Coadiuvare la stazione appaltante nel censimento dei dati personali presenti e dei relativi trattamenti. Riportare alle singole risorse l'incarico di trattare quel particolare dato. Si dovrà prevedere per ogni risorsa una lettera di incarico che evidenzi compiti e responsabilità di trattamento e un piano formativo idoneo a preparare ad una corretta gestione. La conservazione ed il trattamento del dato creano eventi di rischio (accesso indesiderato, perdita, utilizzo non permesso, trattamento non conforme, ecc.).

4) Redigere un PIA preventivo (Privacy Impact Assessment = censimento degli impatti privacy) in cui per ogni fenomeno si valuta rischiosità complessiva, azioni intraprese e rischiosità residua in modo da realizzare il primo documento che fotografa la situazione corrente. Devono essere previste le attività di seguito indicate:

• Analisi del flusso dati: in questa fase si mappano i processi di business per quanto riguarda il dato personale e si crea un diagramma di come il dato viene trattato attraverso l'organizzazione;

• Analisi della privacy: in questa fase viene richiesto al personale coinvolto con il trattamento delle informazioni di compilare i relativi questionari che vengono valutati nell'ottica rischio;

• Relazione sulla valutazione di impatto Privacy: in questo passaggio si effettua una valutazione documentata dei rischi per la privacy e le potenziali implicazioni di tali rischi e l'individuazione delle attività necessarie per mitigare o porre rimedio ai rischi.

5) A partire dalla valutazione del PIA è richiesta la redazione del piano definitivo in cui viene stabilito in quale modo verrà mitigato il singolo rischio,

coloro che sono incaricati di operare in tal senso e il costo previsto per l'attività. Il PIA dovrà essere disegnato per raggiungere i seguenti obiettivi:

- Garantire la conformità con le normative, e requisiti di politica legali applicabili per la privacy;
- Determinare i rischi e gli effetti che ne conseguono;
- Valutare le protezioni e eventuali processi alternativi per mitigare i potenziali rischi per la privacy.

6) Effettuare gli Audit periodici ufficiali del PIA.

7) Coadiuvare la stazione Appaltante nell'applicazione dello standard ISO/IEC 27001:2005 per la protezione informatica;

- Mappare le possibili situazioni di rischio dal punto di vista del tipo di violazione, delle risorse e delle unità organizzative coinvolte, della probabilità dell'evento e della gravità delle conseguenze;
- Adottare in modo preventivo misure atte ad evitare trattamenti non necessari, ridurre la possibilità di accadimento, ridurre le eventuali conseguenze negative;
- Istituire, secondo processi di qualità, un sistema di monitoraggio continuo in grado di segnalare tempestivamente eventi legati al rischio privacy;
- Predisporre misure correttive adatte in caso di incidente informando gli interessati e l'autorità competente;
- Predisporre piani di ripristino della normale operatività.

8) Coadiuvare la stazione Appaltante nella gestione dei consensi al trattamento

9) Redazione dei registri delle attività di trattamento:

- Il registro del titolare del trattamento, che contiene:
  - ✓ Anagrafica del titolare stesso, di un contitolare se presente, del rappresentante e del titolare alla protezione dati;
  - ✓ Le finalità del trattamento;
  - ✓ Le categorie degli interessati a cui fa capo il dato;

- ✓ Eventuali termini per la cancellazione automatica del dato;
- ✓ Un'eventuale descrizione generale delle misure di sicurezza tecnico-organizzative.

- Il registro del responsabile del trattamento, in cui sono presenti:
  - ✓ L'anagrafica dei responsabili del trattamento;
  - ✓ La descrizione delle categorie di trattamento effettuati;
  - ✓ Opzionalmente la descrizione delle misure di sicurezza intraprese.

10) Svolgere, per conto della stazione Appaltante, il ruolo di Data Protection Officer. Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:

• 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 presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

• sorvegliare l'osservanza del presente 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 di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

11) Coadiuvare la stazione appaltante nell'individuazione, acquisizione ed messa in esercizio di specifiche piattaforme informatiche per l'applicazione del GDPR.

12) Coadiuvare la stazione appaltante nella valutazione delle soluzioni ICT specificatamente per quanto concerne la rispondenza ai requisiti di Privacy by Design e by Default.

13) Organizzazione ed esecuzione delle attività di formazione necessarie per la compliance al GDPR.

14) Redazione di regolamenti interni utili all'applicazione del GDPR.

15) Supportare la stazione appaltante nelle attività connesse all'applicazione delle misure minime di sicurezza di cui alla circolare AGID del 18 aprile 2017, n. 2/2017.

16) Eseguire periodiche attività di verifica della sicurezza dei sistemi informatici della Stazione appaltante tra i quali a titolo esemplificativo Vulnerability Assessment e Penetration Tests.