PNG

Spett.le _____
P.IVA _____
VIA _____
CAP_____
LOCALITA _____

Oggetto: Offerta del servizio X-GDPR per gli studi Dentistici.

Facendo riferimento alla Vs. gradita richiesta, siamo con la presente a sottoporVi la nostra migliore offerta relativamente al servizio denominato X-GDPR per l'adeguamento normativo degli studi dentistici in base al nuovo regolamento europeo in materia di protezione dei dati personali GDPR[1].

Grati per l'attenzione che vorrete porre alla presente, cogliamo l'occasione per porgere distinti saluti.

PNG Srls

1 RGPD, in inglese GDPR, General Data Protection Regulation- Regolamento UE 2016/679.

PNG

Indice dei contenuti

PNG

1. Elementi di analisi e quadro di intervento

Di seguito vengono riportate in forma ridotta alcune delle analisi di contesto sulla base delle quali sono state fatte le scelte per la realizzazione della soluzione X-GDPR.

1.1. Obbligo di nomina di DPO (o RDP in Italiano)

La nomina del RPD è obbligatoria per tutte le autorità pubbliche, nonché per le attività il cui esercizio comporta la manipolazione di dati in larga scala per speciali categorie di dati, tra i quali i dati sanitari (Art. 37, Par. 1 GDPR).
Nel testo del GDPR non viene specificata la misura o la quantità di dati definita "larga scala" e al momento la stessa Commissione Europea, nonché il Garante della Privacy, interpretano la norma in modo diverso sull'obbligatorietà di nomina del RPD per gli studi medico-odontoiatrici.
Secondo il *Considerando 91*, infatti, gli studi medici, odontoiatrici e professionali con un solo titolare del trattamento dei dati personali dei pazienti non sono obbligati a nominare un RPD.
Tuttavia, se lo studio medico è convenzionato con il SSN, il Garante della Privacy raccomanda fortemente di nominare un RPD.
Maggiori chiarimenti saranno forniti prossimamente dal Garante della Privacy, per cui occorrerà attendere il lavoro del Legislatore per una definizione definitiva. **Tuttavia, essere eventualmente esentati dalla nomina di un RPD non solleva il titolare dello studio da tutte le responsabilità** e dalle attività sancite dal GDPR.
I requisiti di protezione dei dati sanciti dall'Art. 32, il controllo degli accessi ed il registro delle attività sancite dall'Art. 30 sono comunque previsti dal nuovo regolamento, quindi dovranno essere realizzati e verificabili dalle autorità di controllo.
Per soddisfare questi requisiti, lo studio medico-odontoiatrico può comunque decidere di nominare un RPD, anche qualora non ne fosse obbligato.
In ogni caso la responsabilità di nomina del RDP spetta al titolare del trattamento dati.

1.2. Valutazione Impatto sulla protezione dei dati (DPIA)

La valutazione di impatto sulla protezione dei dati si rende obbligatoria secondo le Linee Guida adottate dal Gruppo di lavoro ex art. 29: *"... quando i trattamenti riguardano (..) cartelle cliniche dei pazienti"*.
Le stesse Linee Guida indicano la necessità di seguire uno standard nella redazione della documentazione indicando a quale dei quattro standard accreditati si fa riferimento.
La suite X-GDPR include una DPIA seguendo le Linee Guida in materia e nello specifico adotta il modello tedesco di DPIA integrato, ove previsto, con lo standard ISO 27001:2013.
Gli analisti della suite X-GDPR hanno realizzato la DPIA seguendo lo standard tedesco IT-Grundschuz ed alla sua applicazione.

PNG

2. Descrizione dei prodotti

2.1. Introduzione

Per realizzare il progetto X-GDPR le società coinvolte hanno messo a fattor comune le loro competenze complementari per arrivare ad una definizione del c.d. GDPR (General Data Protection Regulation) in un'ottica fortemente orientata da un lato alla sicurezza informatica e dall'altro, all'uso di robot software per la standardizzazione e automazione dei processi di analisi e di gestione del GDPR.

Peculiarità che pongono la soluzione proposta non solo come una risposta di adeguamento normativo all'entrata in vigore di una nuova legge, ma anche come una soluzione che interpreta le crescenti necessità organizzative proprie di società complesse.

Ricordiamo a tal proposito, e solo a titolo indicativo, l'ampia bibliografia in materia il documento del European Data Protection Supervisor dal titolo esplicativo: "Artificial Intelligence, Robotics, Privacy and Data Protection"[2].

2.2. ll prodotto X-GDPR

X-GDPR è una piattaforma applicativa realizzata da BPEng Srl (www.bpeng.com) in partnership con SICURDATA Srl (http://www.sicurdata.com) che consente di gestire in modo integrato e automatizzato i principaliprocessi GDPR fra cui :

1. integrazione via API Rest con il gestionale SoftWork di SWHT;
2. configurazione struttura organizzativa tramite integrazione e interfacce dedicate dalla gestione SWHT gli utenti, le posizioni, i ruoli GDPR assegnati e i trattamenti configurati nel gestionale;
3. processo di nomina automatizzato degli incaricati GDPR;
4. processo di somministrazione automatica del questionario competenze e assegnazione automatica dei corsi di formazione necessari per adeguare le competenze rilevate a quelle minime richieste da GDPR. Archiviazione su Content Management System (CMS Alfresco) in cloud delle nomine prodotte in automatico;
5. processo di creazione del registro dei trattamenti con integrazione della struttura organizzativa rilevata, attività, processi e dati trattati dla gestionale SWHT. Archiviazione su CMS del registro dei trattamenti creato;
6. processo automatizzato per la creazione della DPIA adattata per gli studi dentistici e derivata dallo standard tedesco SDM (The Standard Data Protection Model);
7. documentazione di tutti i processi GDPR mappati, nonché possibilità di esportali in formato BPMN (Business Process Model and Notation).

NOTA: tutti i processi automatizzati sono eseguiti con il motore di Business Process Management Activiti™ che tiene traccia dei tempi e degli esecutori di ogni attività di processo svolta.

[2] https://edps.europa.eu/sites/edp/files/publication/16-10-19_marrakesh_ai_paper_en.pdf

PNG

2.3. Formazione e-learning

La formazione resta obbligatoria anche nel GDPR, da valutare all'occorrenza anche tramite fornitori terzi.

3. SERVIZIO ASP (Outsourcing) X-GDPR

Il software X-GDPR, potrà da Voi essere utilizzato attraverso il servizio di SaaS fornito da PNG Srls:
Il servizio ASP (Application Service Provisioning) o SaaS (Software as a Service), in modalità "pay per use", permette di utilizzare, tramite una connessione in Internet, i moduli applicativi, senza la necessità di dover gestire a Vs. carico i Server, il DB e tutta l'infrastruttura ICT necessaria per garantire l'uso dell'applicazione e l'integrità della base dati, fermo restante tutte le capacità di integrazione.

Numero di personale soggetto a GDPR (titolare, dipendenti, collaboratori, …)	**Canone annuale**
Da 1 a 10 (inclusa 1 ora di supporto online/telefonico)	€ 990,00
Da 11 a 20 (inclusa 1 ora di supporto online/telefonico)	€ 1.890,00
Da 21 a 30 (inclusa 1 ora di supporto online/telefonico)	€ 2.690,00
Oltre 30 (inclusa 1 ora di supporto online/telefonico)	Contattare PNG Srls

Il canone annuale si intende al netto dell'IVA, a partire dal 01.01.2019, subirà un aumento annuale pari all'indice ISTAT.
NB: nel canone è escluso il collegamento a Internet, la configurazione iniziale dei software SWHT e gli eventuali interventi presso le Vs. Sedi.

4. SERVIZIO RPD Responsabile Protezione Dati (DPO in inglese)

Per gli studi che volessero dotarsi di un RPD la figura che noi proponiamo[3] adempierà, in particolare, ai 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 regolamento GDPR 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

[3] Servizio offerto da una società specializzata e certificata organizzata in modo tale da soddisfare i requisiti previsti per l'erogazione del servizio DPO.

PNG

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.

I costi del servizio saranno concordati sulla base delle richieste

Tutto ciò che non è previsto esplicitamente nell'offerta è da considerarsi a pagamento.

Tutti i prezzi si intendono Iva 22% esclusa.

Pagamento: Da concordare.

Luogo e data

Timbro e Firma per a accettazione

Verona, _____

_____