

Ani 2021

Off. 2021_1092
Redatta: Gianni Sanna
Autorizzata: P.Deidda

ORISTANO 11.11.2021

Spettabile Comune di PALAU

Oggetto: Servizio di DPO ed Attività di accompagnamento dell'Ente ai fini dell'adeguamento alle prescrizioni al Regolamento UE 679/2016. Assessment.

A seguito della vostra richiesta, con la presente inviamo la ns. proposta relativa al Servizio di DPO ed alle attività di consulenza previste ai fini dell' adeguamento al Regolamento UE 679/2016 all'interno del Vs. Ente.

Nel caso la proposta possa essere di Vostro interesse restiamo a disposizione per un eventuale approfondimento, per chiarimenti ed integrazioni e con l'occasione porgiamo i più cordiali saluti.

Dasein s.r.l.
L'Amministratore delegato
Danilo Grimaldi



DASEIN SRL
P.I. 06367820013

Comune di Palau
Registro di Protocollo
N. 0018311 del 12/11/2021



DASEIN S.r.l.

Sede Operativa di Torino: Lungo Dora Colletta 81 - 10153 Torino - Tel.: 011 - 240.42.11 - Fax: 011 - 240.42.35
Sede Operativa di Milano: Via Boscovich Ruggero 29 - 20124 Milano
Sede Operativa di Oristano: Via Sardegna 69A - 09170 Oristano
Sede Operativa di Arenzano (GE): Via Terralba 19 - 16011 Arenzano (GE)
Sede Legale: Lungo Dora Colletta 81 - 10153 Torino
C.F., P.IVA e Reg. Imprese di Torino: 06367820013 - Cap. Soc. € 25.237,00 interamente versato
Email: info@dasein.it; Pec: dasein@legalmail.it; Sito web: www.dasein.it



PROGETTO

1. PREMESSA. IL GDPR 679/2016 E LA SUA ENTRATA IN VIGORE.

Il Regolamento europeo sulla protezione dei dati - *GDPR (General Data Protection Regulation)* - è una normativa europea, diventata operativa dal 25 maggio 2018, che sancisce dei nuovi criteri per trattare i dati personali in modo più responsabile e sicuro.

Alcuni punti chiave previsti nel GDPR sono:

- L'implementazione di un **Modello di Gestione della Privacy**
- L'implementazione di misure sicurezza **adeguate**
- L'obbligo di **formazione** verso tutte le persone autorizzate a trattare i dati personali
- La nomina del **DPO**.

La normativa ha un impatto consistente in diversi ambiti:

Ambito organizzativo:

- Istituzione di un Registro dei Trattamenti
- Implementazione del principio di Accountability
- Implementazione del criterio di Privacy by Design & Default
- Possibilità di richiedere la modifica dei dati o il diritto all'oblio
- Obbligo di notifica in caso di Data Breach entro 72 ore
- Introduzione della figura del DPO – Data Protection Officer

Misure di sicurezza:

Le misure minime ex All. B D.lgs. 196/03 vengono superate ed arricchite in relazione alla tipologia di dati trattati, giungendo al concetto di misure adeguate:

- Architettura client/server
- Sistemi per il disaster recovery e per la gestione del cyber risk
- Sistemi antintrusione hardware – firewall
- Protezione da virus
- Strategia di backup adeguata
- Minimizzazione e crittografia dei dati

I destinatari:

Il regolamento si applica, in linea generale, a liberi professionisti, aziende e pubbliche amministrazioni indipendentemente dal numero di dipendenti al suo interno.

Le sanzioni previste:

Il regolamento prevede sanzioni amministrative pecuniarie fino a 20 milioni di euro oltre che sanzioni penali secondo quanto previsto dal D.Lgs. 101/2018.



2. SERVIZIO DATA PROTECTION OFFICER – ESPERTO ESTERNO

L'applicazione del principio di *Accountability*, inteso come responsabilizzazione e dovere di rendicontazione, introduce dunque la figura del DPO, Data Protection Officer, o Responsabile della Protezione Dati.

La figura ha un ruolo fondamentale nell'assicurare che il Titolare del trattamento ottemperi con diligenza alle prescrizioni contenute nel Regolamento Europeo 2016/679.

Il DPO è un supervisore indipendente, con funzioni di supporto, consultazione, formazione e informazione e avrà il compito di cooperare con il Garante della Privacy, costituendo il punto di contatto, anche rispetto agli interessati, tra l'Amministrazione e l'Autorità.

I suoi dati dovranno essere sempre pubblicati in chiaro dalla PA e il suo nominativo comunicato al Garante.

Sono obbligati alla nomina del DPO:

- 1) Amministrazioni ed enti pubblici ad eccezione delle autorità giudiziarie
- 2) Tutti i soggetti la cui attività principale consiste in trattamenti che per natura, oggetto o finalità richiedono il controllo regolare e sistematico degli interessati
- 3) Tutti i soggetti la cui attività principale consiste nel trattamento, su larga scala, di dati sensibili relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici

I principali compiti del DPO sono:

- 1) Informare e assistere il Titolare del trattamento e i lavoratori nella corretta applicazione del Regolamento;
- 2) Vigilare sulla corretta applicazione della disciplina privacy (regolamento – policy) attraverso attività di audit e di formazione/sensibilizzazione dei lavoratori.
- 3) Fornire, se richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliare i relativi adempimenti.
- 4) Fungere da punto di contatto per gli interessati in merito a qualunque problematica connessa al trattamento dei loro dati o all'esercizio dei loro diritti.
- 5) Gestire le richieste provenienti dall'Autorità Garante per la protezione dei dati personali (es. rispondendo alle note di chiarimenti) oppure le istanze presentate dal Titolare del trattamento (es. istanze di verifica preliminare ex art. 17 C.d.P.)

La presente offerta, oltre a garantire i principali compiti del DPO, così come previsti dall'art. 39 del GDPR (punti da 1 a 5 precedenti), **garantisce inoltre:**



- a) La formulazione di pareri relativi al bilanciamento tra riservatezza e trasparenza amministrativa alla luce del decreto legislativo n.33/2013, così come riformato dal Decreto Legislativo n.97/2016 ;
- b) Il supporto nell'aggiornamento di una procedura di gestione degli affidamenti di attività che comportano un trattamento di dati personali a responsabili esterni, compresa la predisposizione delle specifiche clausole previste dall'articolo 28 del RGDP;
- c) Il supporto nell'aggiornamento degli atti di nomina dei responsabili, incaricati ed amministratori di sistema e dei correlati adempimenti;
- d) Il parere su informative specifiche relative al trattamento dei dati personali;
- e) L' audit annuale del mantenimento degli standard di protezione dei dati ;
- f) Metodologie per ottenere il consenso del cliente/ utente nella gestione dei dati;
- g) DPO on demand con servizio da remoto .
- h) Software per la gestione su Cloud di Anagrafica soggetti che trattano i dati personali;
Trattamenti, Ruoli Privacy, Informative, Analisi dei Rischi, DPIA, Data Breach, Documentazione
pertinente compresa .

L'adempimento delle attività descritte sarà in linea con gli adempimenti richiesti dal GDPR e successivi provvedimenti, pareri, linee guida emanate dall'Autorità Garante Privacy riguardo il trattamento dei dati personali effettuato dalle strutture.

Pertanto sarà altresì in grado di:

- assicurare al cittadino la riservatezza, il controllo, la chiarezza e la sicurezza necessari nel rapporto con le strutture;
- responsabilizzare i dirigenti di struttura e il personale addetto sulle responsabilità connesse con la sicurezza e protezione dei dati mediante specifica formazione;
- supportare il Referente Interno Privacy, ove previsto, con apposite verifiche sull'efficacia e l'effettiva adozione delle misure proposte e con attività di consulto per singole problematiche.

3. ATTIVITA' DI CONSULENZA PREVISTA AI FINI DELL' ADEGUAMENTO AL REG. UE 679/2016 . ASSESSMENT.
--

- 1. Attività di realizzazione del risk assessment:
 - a. Verifica della presenza delle figure coinvolte dalla normativa
 - b. Raccolta dati eseguita tramite questionari e interviste:
 - i. Censimento attività di trattamento cartacee e materiali in genere
 - ii. Censimento attività di trattamento informatizzate e ICT in genere
 - c. Analisi dei rischi fisica e ICT:
 - i. Analisi dei rischi con metodologia proattiva
 - ii. Rischi fisici legati alle sedi e/o stabilimenti produttivi



- d. Rischi legati al mondo ICT (cyber risk)
- e. Verifica compliance per eventuali impianti di videosorveglianza
- f. Analisi della Privacy Compliance del Sito web (cookie e informative)
- g. Analisi della Privacy Compliance delle eventuali attività di marketing
3. Consulenza e verifica sull'implementazione del piano di adeguamento e miglioramento scaturito dalle precedenti attività di risk assessment
4. Implementazione del modello di gestione:
 - a) Identificazione del/dei Titolari dei trattamenti e eventuale stesura del contratto di contitolarità
 - b) Stesura e aggiornamento Registro dei trattamenti
 - c) Stesura del registro dei Data Breach
 - d) Identificazione e disegno dell'organigramma ai sensi del regolamento
 - e) Identificazione e nomina dei responsabili (esterni) e stesura del contratto di servizio
 - f) Identificazione e modulazione dei livelli di delega per gli "incaricati" (persone autorizzate al trattamento)
 - g) Definizione della Data Retention Policy
5. Analisi della Privacy Compliance del Sito web
 - a) Cookie Policy
 - b) Informativa breve
 - c) Verifica dei cookie di profilazione
 - d) Privacy Policy del sito ed informativa estesa
 - e) Check Privacy Compliance per aree tematiche del sito ove presenti come ad esempio:
 - f) Opportunità di lavoro
 - g) Raccolta dati tramite form
 - h) Newsletter
6. Analisi della Privacy Compliance per eventuali APP utilizzate/gestite
7. Analisi della Privacy Compliance delle eventuali attività di promozione e/o marketing
8. Stesura della documentazione costituente un "Dossier Regolamento 679/2016 - GDPR"
9. Stesura di un documento con:
 - a) Direttive per la Compliance se necessarie
 - b) Piano di formazione per la struttura

(formazione esclusa dalla presente offerta e da quotare a parte in funzione del piano di formazione ritenuto necessario).

4. ATTIVITA' DI FORMAZIONE OBBLIGATORIA DEI SOGGETTI CHIAMATI A TRATTARE I DATI PERSONALI.

Una puntuale attività di Assessment necessita di un adeguato intervento formativo che avrà ad oggetto i profili giuridici-normativi per il corretto adeguamento alla normativa sulla Privacy.

Formazione Giuridica/Normativa

- Introduzione al Regolamento Europeo Privacy



- Le Disposizioni Generali del Regolamento Privacy Europeo
- Le Definizioni Principali del Regolamento Privacy
- Il Regolamento Europeo ed il Decreto legislativo 196/2003 come novellato dal Decreto legislativo 101/2018.
- Il Principio di Liceità e Finalità
- Il Principio di Privacy By Design e Privacy By Default
- Il Titolare del Trattamento
- Il Rappresentante del Titolare
- Il Responsabile del Trattamento
- Il Data Protection Officer
- L'Interessato
- Il Diritto di Informativa Privacy e Consenso Privacy
- Il Diritto di Accesso ai Dati Personali
- Il Diritto di Rettifica e Cancellazione
- Il Diritto all'Oblio
- Il Diritto alle Portabilità dei Dati Personali
- La Valutazione dell'Impatto sulla Protezione dei Dati Personali
- Le Misure di Sicurezza
- Il Registro delle Attività di Trattamento
- La Notifica delle Violazioni dei Dati Personali
- La Comunicazione delle Violazioni dei Dati Personali
- Le Autorità Garanti per la Protezione dei Dati Personali
- Competenza, Compiti e Poteri del Garante Privacy
- Reclami, Ricorsi e Segnalazioni al Garante Privacy
- Le Sanzioni Amministrative Pecuniarie
- Il Risarcimento Danni

Il servizio sarà svolto in staff dal dott. Giovanni Maria Sanna e dalla dott.ssa Martina Dell'Oro

Costi :

Il corrispettivo economico richiesto da Dasein S.r.l. per la fornitura dei servizi descritti il è il seguente:

RIEPILOGO ACQUISTO PER singolo MODULO



COMUNE D PALAU (ANNUO)	Costo	Mepa	Note
1. SERVIZIO DATA PROTECTION OFFICIER OFFERTA PER ANNI UNO	€ 2500,00	TRATTIVA DIRETTA <i>das_privacy_GDPR</i>	Più IVA di legge
COMUNE DI PALAU (ANNUO)	Costo	Mepa	Note
2. ATTIVITA' DI CONSULENZA PREVISTA AI FINI DI ADEGUAMENTO AL REG UE 679/2016. ASSESSMENT PER ANNI UNO	€ 1000,00	TRATTIVA DIRETTA <i>das_privacy_GDPR</i> <i>IMPORTO ANNUO</i>	Più IVA di legge
COMUNE DI PADRU (ANNUO)	Costo	Mepa	Note
3. ATTIVITA' OBBLIGATORIA DI FORMAZIONE ATTRAVERSO una mezza giornata formativa in (house)	€ 600,00	TRATTIVA DIRETTA <i>das_privacy_GDPR</i> <i>per formazione In house</i>	IVA ESCLUS A

RIEPILOGO ACQUISTO SIMUTANEO TRE MODULI

COMUNE DI PALAU	Costo	Mepa	Note
1. SERVIZIO DATA PROTECTION OFFICIER OFFERTA PER ANNI (UNO) 2. ATTIVITA' DI CONSULENZA PREVISTE AI FINI DI ADEGUAMENTO AL REG UE 679/2016. ASSESSMENT PER ANNI UNO 3. ATTIVITA' OBBLIGATORIA DI FORMAZIONE IN HOUSE PER ANNI UNO ed aggiornamenti successivi attraverso pillole formative.	€ 3900,00	TRATTIVA DIRETTA <i>das_privacy_GDPR</i>	Più IVA di legge – esclusa la parte imputabile a formazione (€ 600) in quanto IVA esente

COMUNE DI PALAU	Costo	Mepa	Note
1. SERVIZIO DATA PROTECTION OFFICIER OFFERTA PER ANNI (DUE) 2. ATTIVITA' DI CONSULENZA PREVISTE AI FINI DI ADEGUAMENTO AL REG UE 679/2016. ASSESSMENT PER ANNI UNO ed eventuali aggiornamenti per il successivo anno. 3. ATTIVITA' OBBLIGATORIA DI FORMAZIONE IN HOUSE PER ANNI UNO ed aggiornamenti	€ 5.200,00	TRATTIVA DIRETTA <i>das_privacy_GDPR</i> <i>€ 2600,00 ANNUI</i>	Più IVA di legge – esclusa la parte imputabile a formazione (€ 600) in quanto IVA



successivi attraverso pillole formative.			esente
--	--	--	--------

COMUNE PALAU	Costo	Mepa	Note
1. SERVIZIO DATA PROTECTION OFFICIER OFFERTA PER ANNI (TRE) 2. ATTIVITA' DI CONSULENZA PREVISTE AI FINI DI ADEGUAMENTO AL REG UE 679/2016. ASSESSMENT PER ANNI UNO ed eventuali aggiornamenti per i successivi due anni 3. ATTIVITA' OBBLIGATORIA DI FORMAZIONE IN HOUSE PER ANNI UNO ed aggiornamenti successivi attraverso pillole formative.	€ 6900,00	TRATTIVA DIRETTA <i>das_privacy</i> _GDPR € 2300,00 ANNUI	Più IVA di legge – esclusa la parte imputabile a formazione (€ 600) in quanto IVA esente

Modalità di fatturazione

La fatturazione per il servizio di DPO avrà cadenza : PER IL NUMERO DI MENSILITA' EROGATE entro L'ANNO DI AFFIDAMENTO; dal 2022 anno con cadenza semestrale.

Modalità di pagamento

30 giorni D.F.F.M.

Validità dell'offerta

Tale offerta è da ritenersi valida 15 giorni dalla data odierna.

Nel caso foste interessati a ricevere ulteriori informazioni la persona da contattare è:

Gianni Sanna, tel 3491275212, email sanna.dpo@dasein.it