



ORDINE
ASSISTENTI
SOCIALI
Consiglio Regionale
d'Abruzzo

Ente Pubblico non economico
L. 84/93 – D.M. 615/94

Deliberazione di Consiglio n° 75 del 16 luglio 2018

Oggetto: Regolamento europeo n. 2016/679 e nomina del responsabile per la protezione dei dati

L'anno duemiladiciotto il giorno 16 del mese di luglio alle ore 15,30, presso la sede dell'Ordine in L'Aquila, si è riunito il Consiglio presieduto dal Presidente Francesca D'Atri alla presenza dei Consiglieri:

presidente	D'Atri Francesca	P	consigliere	Ettore Massimiliano	P
vicepresidente	Di Santo Amalia	P	consigliere	Ficorilli Francesca	P
segretario	Paglia Caterina	P	consigliere	Santilli Dora	A
tesoriere	Di Iorio Marina	P	consigliere	Scarsella Pamela	P
consigliere	Cericola Alberto	P	consigliere	Trosini Cristina	P
consigliere	Di Vittorio Barbara	A			

Il Presidente, constatata la regolarità della seduta, adotta la seguente deliberazione:

Il Consiglio

- ✚ *Considerato che ai sensi del Regolamento europeo n. 2016/679 è necessario redigere un regolamento ad hoc;*
- ✚ *Vista e considerata la delibera n° 73 del 16.07.2018 con tutti i suoi allegati;*
- ✚ *Letti tutti i preventivi pervenuti;*
- ✚ *Considerata congruo il preventivo pervenuto dall'Agenzia TINN srl di Teramo (che si allega in copia) il migliore in termini di qualità e in linea con gli altri preventivi pervenuti in termini di economicità;*

con voti

favorevoli.....09.....sfavorevoli...../.....astenuti...../.....

DELIBERA

- ✚ *Di affidare alla Agenzia TINN srl di Teramo la stesura di un regolamento ad hoc e la nomina del responsabile per la protezione dei dati.;*
- ✚ *di dare immediata esecutività al presente atto deliberativo.*

IL SEGRETARIO
Caterina Paglia



IL PRESIDENTE
Francesca D'Atri

Si dispone la pubblicazione sul sito dell'Ordine regionale.



è una società del Gruppo Maggioli

Prot.: 2018/798/CO/CZ/SW

Data: 13/07/2018

Spett.Le

ORAS Abruzzo

Via Garibaldi, 3

67100 L'Aquila (AQ)

Offerta per attività di adeguamento agli obblighi normativi in tema di data protection ed attività di Responsabile della Protezione dei Dati (RPD, altrimenti denominato Data Protection Officer, DPO)

Gli obblighi normativi nazionali ed europei impongono agli enti pubblici l'adozione di **misure tecniche e organizzative adeguate** per garantire un livello di **sicurezza** proporzionato al rischio dei trattamenti di dati effettuati. In particolare, il **Regolamento UE 2016/679** (denominato **GDPR**) dovrà trovare piena attuazione **entro maggio 2018** , mentre la circolare 2/2017 di **AgID** impone già l'adozione di una serie di misure ICT per garantire la sicurezza delle informazioni.

Si propone un'attività integrata, frutto di **15 anni di esperienza a fianco delle pubbliche amministrazioni** una competenza su tre dimensioni - **legislativa, organizzativa e tecnologica** - in grado di supportare efficacemente gli enti nell'implementazione di efficaci **sistemi di gestione della compliance** alle varie normative in tema di sicurezza e protezione dei dati personali.

Le attività previste per affiancare l'ente nelle fasi di messa a norma dei propri processi con le indicazioni in tema di protezione dei dati personali sono le seguenti:

A) Mappatura dei trattamenti al fine della redazione e tenuta del registro delle attività di trattamento

L'intervento mira alla raccolta e catalogazione dei trattamenti di dati svolti all'interno dell'ente, al fine di redigere il registro dei trattamenti come richiesto dall'articolo 30 del Regolamento Europeo. Il punto di partenza sarà l'ultima versione disponibile del Documento Programmatico sulla Sicurezza, per poi effettuare una verifica con gli uffici competenti.

TINN srl

Sede Legale ed amministrativa
Via Giuseppe De Vincentiis, sn
64100 TERAMO - www.tinn.it

Tel 0861.4451
Fax 0861.210085
info@tinn.it
protocollo@pectinn.it

Iscritta al Registro
delle Imprese di Teramo
R.E.A. TE-116512
C.F. e P.IVA: 00984390674

Capitale sociale:
Euro 93.600,00
Interamente
versato

Società soggetta
all'attività di direzione
e coordinamento
di Maggioli S.p.A.



è una società del Gruppo Maggioli

B) Revisione della documentazione di nomina dei responsabili e degli incaricati del trattamento

Una volta individuati i trattamenti, si rende necessario associarli agli uffici coinvolti, al fine di costruire una matrice funzionale per definire le competenze dei singoli soggetti afferenti agli uffici. Questo consentirà di procedere alla revisione delle nomine degli incaricati del trattamento: pur non essendo più un esplicito obbligo di legge, il Garante individua questa azione come una misura idonea di sicurezza consentendo di definire i ruoli e le attività dei soggetti coinvolti nelle fasi operative del trattamento dei dati.

Inoltre, si procederà alla definizione dei responsabili del trattamento (interni ed esterni) ai sensi dell'art. 28 del Regolamento Europeo. Questa attività comporta una ricognizione tra i vari settori per individuare trattamenti di dati esternalizzati in nome e per conto dell'ente, al fine di procedere a nomine specifiche con evidenziati i perimetri operativi.

C) revisione moduli informativa ed eventuale consenso trattamento dati personali

Al fine di adeguare la documentazione redatta dall'ente in tema di informative al trattamento dei dati personali si consiglia una sessione con l'obiettivo di incontrare i vari uffici che presenteranno la modulistica attualmente utilizzata per l'aggiornamento.

D) Impostazione del processo per la redazione dell'analisi di impatto privacy in caso di nuovi trattamenti

Il nuovo Regolamento Europeo prevede, in caso di nuovi trattamenti di dati, di effettuare un'analisi preliminare dell'impatto privacy che tale nuovo trattamento comporterebbe. L'intervento prevede la redazione della necessaria documentazione per effettuare tale analisi (schede con analisi di compliance alla normativa) da produrre in caso di ispezione del Garante.

E) Formazione generica al personale in ambito privacy e sicurezza

Si propone una sessione formativa di 3 ore da svolgersi presso la sede dell'ente in cui verranno illustrati gli obblighi normativi e quelli relativi al contesto (es presenza di disciplinari risorse informatiche), al fine di rendere edotto il personale sugli obblighi e sulle responsabilità derivanti dal trattamento dei dati. Verrà fornito del materiale didattico (slides) e al termine delle sessioni si rilasceranno degli attestati di partecipazione.



è una società del Gruppo Maggioli

F) Analisi del rischio

L'attività prevede interventi per l'individuazione delle minacce e la valutazione dell'impatto che queste possono avere sulle risorse dell'ente, seguita da un piano dei trattamenti in cui sono indicate le misure da adottare per mitigare i rischi. Si tratta di una prima analisi finalizzata a definire gli ambiti principali di azione, che potrà successivamente essere approfondita con interventi più mirati e specifici a seconda delle necessità riscontrate.

G) Processo di escalation Data Breach

L'attività prevede l'impostazione del processo di rilevazione di eventuali incidenti di sicurezza, la valutazione dell'entità degli stessi e la redazione di una procedura operativa che possa concludersi con le azioni necessarie previste dal Regolamento UE per la gestione di un data breach (registrazione eventi di sicurezza, eventuale notifica all'Autorità Garante e comunicazione agli interessati in caso di necessità).

H) attività di Responsabile della Protezione dei Dati (RPD, altrimenti denominato Data Protection Officer, DPO)

Tra gli obblighi di legge, per alcune categorie di enti e tipologie di trattamenti è prevista la **nomina obbligatoria di un Responsabile della Protezione dei Dati (RPD)**. Tale figura, le cui **competenze, mansioni e responsabilità** sono previste specificamente dagli **artt. 37-39** del Regolamento Europeo 2016/679, svolge un ruolo di **supporto al titolare** e **sorveglianza** della corretta applicazione del GDPR, oltre che da **punto di contatto per l'Autorità Garante della Privacy** per qualsiasi questione connessa ai trattamenti di dati effettuati dall'ente.

Tali attività possono essere effettuate da **soggetti interni o esterni**; è prevista inoltre la possibilità di **costituire un ufficio strutturato** per lo svolgimento dei compiti stabiliti. In ogni caso, è comunque necessario che venga sempre individuata la persona fisica che riveste il ruolo di RPD mediante specifico atto di designazione. SI.net ha elaborato una proposta tecnica a supporto di tutti quegli enti che hanno deciso di ricorrere a soggetti esterni.

Attività previste nel servizio. Per lo svolgimento dei compiti definiti all'art. 39 del GDPR, sono previsti nello specifico:

- Informazione e consulenza per il titolare del trattamento e i soggetti da esso autorizzati in merito agli obblighi derivanti dalle normative in tema di protezione dei dati personali;



è una società del Gruppo Maggioli

- 2 audit annuali per la verifica del livello di adeguamento dell'ente alla normativa, con valutazione delle misure in essere e di quelle da adottare;
- Supporto al titolare per la redazione di analisi di impatto privacy (Privacy Impact Assessment, PIA)
- Webinar di aggiornamento sui temi più rilevanti della privacy e la data protection

Elementi economici

Descrizione	
Attività di affiancamento privacy (attività da A a G)	2.500,00 €
→ Attività di Responsabile della Protezione dei Dati (RPD o DPO) per 1 anno (attività H)	2.500,00 €

I prezzi indicati sono da intendersi al netto di IVA.

Fatturazione:

Attività A-G: a consuntivo delle attività effettuate

Attività I: canone annuale ad accettazione offerta

Pagamento: Bonifico bancario 30 gg. data fattura

Validità dell'offerta: 60 giorni

Nello spirito di collaborazione che contraddistingue la nostra Società siamo disponibili per ogni eventuale chiarimento ed approfondimento di quanto descritto, al fine di adattare l'offerta alle vostre specifiche esigenze, ridiscutendola in ogni sua parte in caso di necessità.

L'occasione è gradita per inviare cordiali saluti.

Servizio Commerciale
Cesare Zippilli

TINN srl

Sede Legale ed amministrativa
Via Giuseppe De Vincentiis, sn
64100 TERAMO - www.tinn.it

Tel 0861.4451
Fax 0861.210085
info@tinn.it
protocollo@pectinn.it

Iscritta al Registro
delle Imprese di Teramo
R.E.A. TE-116512
C.F. e P.IVA: 00984390674

Capitale sociale:
Euro 93.600,00
Interamente
versato

Società soggetta
all'attività di direzione
e coordinamento
di Maggioli S.p.A.