



Comune di Verdellino

(Provincia di Bergamo)

Piazza don Martinelli, 1 - 24040 Verdellino

cod.fisc./p.IVA 00321950164 - tel. 0354182811 – fax. 0354182899

E-Mail: info@comune.verdellino.bg.it – PEC: info@pec.comuneverdellino.it

sito internet: www.comune.verdellino.bg.it

SERVIZIO DI SUPPORTO PER ADEGUAMENTO DEL SISTEMA DI GESTIONE DELLA PRIVACY DEL COMUNE ALLE DISPOSIZIONI DEL NUOVO REGOLAMENTO EUROPEO SUL TRATTAMENTO DEI DATI (RE 679/2016)

Periodo: 22 MAGGIO 2018 / 31 MAGGIO 2020

- FOGLIO PATTI E CONDIZIONI -

Il servizio consiste nelle attività di supporto all'Ente nella transizione documentale legata all'adozione del GDPR in Italia, prevedendo di:

- Contenere e gestire il rischio di non conformità legislativa;
- Adottare modelli di gestione sicuri e protetti dei dati e delle informazioni;
- Integrare i sistemi organizzativi già esistenti., portando innovazione al personale coinvolto e ai vertici dell'Ente. Stesura e aggiornamento DPS (PIA)
- Fornire la formazione di base agli addetti e alle figure apicali e di responsabilità dei vari settori/aree.

Il servizio di supporto si articola nelle seguenti attività:

- A. PROPOSTA PROGETTUALE - Adeguamento del sistema di gestione della Privacy dell'ente alle indicazioni del regolamento Europeo sul trattamento dei dati attraverso lo sviluppo del SGSI: Sistema di Gestione Sistema Informativo;
- B. INCARICO DI DPO (Data Protection Officer) previsto dall'articolo 37 del regolamento europeo sul trattamento dei dati;
- C. ATTIVITA' DI FORMAZIONE.

A) - Il PROGETTO si articola nelle seguenti tre fasi:

Fase 1: verifica presso l'ente dello stato di fatto (analisi organizzativa, verifica sistema informativo, analisi delle competenze):

- Audit presso le sedi del comune in cui vengono gestiti dati ed informazioni Privacy Impact Assessment;
- Identificazione delle banche dati per definire il registro dei trattamenti
- Verifica della conformità dell'ente alle prescrizioni del REU 679/2016
- Analisi rischi e *pianificazione* degli interventi di messa in sicurezza art 35 Regolamento Europeo;
- Al termine di questa fase dovrà essere redatto un Rapporto di AUDIT con l'indicazione delle anomalie riscontrate;

Fase 2: Definizione delle procedure e della documentazione prevista dal RE 679/2016

- Identificazione dei responsabili della sicurezza e dei relativi compiti;
- Nomina degli incaricati;
- Identificazione delle aziende esterne che trattano i dati e relativa gestione del ruolo come previsto dalla normativa;
- Definizione delle procedure operative per la protezione delle aree e dei locali interessati alle misure della sicurezza;
- Definizione delle regole per assicurare la riservatezza e l'integrità dei dati;

- Procedure e regole per la gestione dell'informativa;
- Supporto per l'implementazione delle misure di sicurezza.
- Privacy by design e Privacy by default: gestione della sicurezza dei dati secondo i principi definiti previsti art 23 Regolamento Europeo

2.1 Documenti da rilasciare

- GDPR/PSSI: Piano Sicurezza Sistema Informativo
- DPIA: Data Protection Impact Assessment (Analisi dei Rischi)
- Rapporto di audit (principio di Accountability) art 24 e 32 del Regolamento Europeo
- Lettere di incarico dirigenti e funzionari art 37 del Regolamento Europeo
- Nomine delle aziende esterne come responsabili del trattamento dei dati
- Regole trattamento dei dati
- Modelli di informativa art 5 e 12 del Regolamento Europeo
- Attestati di formazione (per ottemperare al principio di accountability)
- Autorizzazione al trattamento per gli addetti;

relazioni:

- analisi dei rischi;
- misure di sicurezza adottate;
- Piani sviluppo

registri:

- Trattamenti aggiornati (incluso nel piano di sicurezza);
- Procedura gestione incidenti (incluso nel piano di sicurezza);
- Procedura qualifica Fornitori a cui sono affidati trattamenti esterni
- Regolamento gestione sistema informativo
- Uso degli strumenti di trattamento;
- Trattamento dei dati sensibili aggiornato (incluso nel piano di sicurezza);

Informative:

- Informative cittadini
- Informative dipendenti
- Informativa sito web e portali erogazione servizi

Fase 3: Definizione delle procedure e della documentazione prevista dal RE 679/2016

- Gestione dei programmi di miglioramento inerenti il trattamento dei dati (per ottemperare al principio di accountability)
- Supporto per l'implementazione delle misure di sicurezza
- Supporto nella gestione dei processi di trattamento previsti nel PSSI
- Privacy by design e Privacy by default: gestione della sicurezza dei dati secondo i principi definiti previsti art 23 Regolamento Europeo

B). L'INCARICO DI RESPONSABILE PROTEZIONE DATI, prevede le attività contemplate all'articolo 39 del Regolamento Europeo, di seguito descritte:

1. **informare e fornire consulenza al titolare e al responsabile del trattamento** in merito agli obblighi derivanti dal Regolamento 679/2016 o dalle altre disposizioni legislative interne o europee in materia di protezione dati;
2. **sorvegliare l'osservanza del Regolamento da parte del titolare e del responsabile del trattamento** in tutte le sue parti, comprese l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa al trattamento;
3. **fornire su richiesta pareri** in merito alla valutazione d'impatto e sorvegliarne lo svolgimento;
4. **cooperare con l'Autorità di controllo** fungendo, tra le altre cose, da punto di contatto per questioni connesse al trattamento effettuando consultazioni di ogni tipo, con particolare riguardo e attenzione ad un'eventuale attività di consultazione preventiva.

5. Il responsabile della protezione dei dati è **tenuto al segreto o alla riservatezza** in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri

Per lo svolgimento delle verifiche sopraindicate il RPD effettuerà **n. 8 incontri** presso la sede dell'Ente nel corso del periodo di incarico.

C). L'ATTIVITA' DI FORMAZIONE. consiste nel fornire la **formazione di base** della durata di **due ore** agli addetti e alle figure apicali e di responsabilità dei vari settori/aree **per un totale di 3 corsi nel biennio di incarico.**

PIANO DI INTERVENTO

Il DPO dovrà essere individuato in tempo utile a consentirne la nomina **entro il 25 maggio p.v.**

La 1° FASE della ATTIVITA' PROGETTUALE dovrà essere conclusa entro il 31/07/2018.

La tempistica per l'attuazione delle altre FASI dell'ATTIVITA' PROGETTUALE verrà definita tra le parti, sulla base del Rapporto di AUDIT con l'indicazione delle anomalie riscontrate da predisporre nel termine sopraindicato (entro il 31 luglio 2018).

COSTO DEL SERVIZIO E PAGAMENTI

L'importo annuale per il servizio offerto è di _____ (_____mila/00) IVA esclusa.

Il pagamento sarà effettuato in 5 rate, ciascuna pari al 20% dell'importo di aggiudicazione, da fatturare alle seguenti scadenze:

- 30 SETTEMBRE 2018;
- 31 DICEMBRE 2018;

- 30 GIUGNO 2019;
- 31 DICEMBRE 2019;

- 31 MAGGIO 2020.

Il pagamento avverrà entro 30 gg. dal ricevimento di regolare fattura elettronica previa verifica di regolarità della prestazione e di verifica di regolarità contributiva (DURC).

PRIVACY E SEGRETEZZA PROFESSIONALE

Tutti i dati raccolti nel corso dello svolgimento degli accordi commerciali e dell'attività di cui all'incarico, vengono trattati con la massima riservatezza e in conformità con quanto previsto dal Dlgs. 196/03 e "Regolamento UE 679/2016" in materia di tutela delle persone fisiche con riguardo al trattamento dei dati personali e la loro libera circolazione".

I dati e i documenti, siano essi su supporto cartaceo o informatico, sono protetti da password e sono accessibili in forma controllata dal titolare del trattamento dal nostro Studio.

Il sistema informatico è dotato di dispositivi di sicurezza (antivirus, firewall, sistemi di backup ecc.) in continuo aggiornamento.

La sede della ditta appaltatrice del servizio è soggetta a supervisione da parte di centrale di vigilanza H24, nonché di dispositivi di rilevazione fumi e protezione antincendio.

TUTELE ASSICURATIVE

La ditta appaltatrice del servizio è in possesso di assicurazioni per responsabilità professionale, civile e tutela legale. Copia delle stesse sarà fornita al cliente a seguito di conferma dell'incarico.