# Si.Re. Informatica S.r.l.

*Professionisti al servizio della P.A.*

Via Gavi, 26 - 15067 Novi Ligure (AL)
Via Bandello, 9 - 15057 Tortona (AL)
Via S. Ambrogio, 17 - 15060 Tassarolo (AL)
P.I. 01338860065 - C.F. 06481890157

Telefono: 0143.329507 - Fax: 0143.314412
Mail: info@sireinformatica.it - PEC: info@pec.sireinformatica.it - Sito: sireinformatica.it

**Divisione tecnologica**


## *Presenta il Servizio:*

# GDPR "nel Comune"

## (*in collaborazione con Avv. Massimo Ramello*)

# PROGETTO:

## Introduzione

Mancano ormai poco meno di due mesi alla scadenza del 25 maggio 2018, data che sancisce l'entrata in vigore del Regolamento Europeo n. 679/2016 (GDPR).

Pur essendo l'Italia già dotata di una normativa nazionale particolarmente stringente e simile, nei principi, all'impianto del nuovo Regolamento europeo e, pur avendo i Comuni già posto in essere quanto previsto dalla previgente disciplina nazionale, si evidenzia, tuttavia, che il percorso di attuazione delle nuove disposizioni potrebbe presentare, per le Amministrazioni locali, soprattutto quelle di minori dimensioni demografiche, difficoltà operative.

L'adozione delle disposizioni contenute nel Regolamento europeo, infatti, inciderà notevolmente sulla loro organizzazione interna, modificandone gli assetti strutturali, in quanto richiederà la ricognizione e la valutazione delle misure di sicurezza normative, organizzative e tecnologiche, già adottate dagli enti a tutela della privacy.

**Condizioni di Vendita:**

- Tutti i prezzi (salvo espressa indicazione) sono al netto di I.V.A. di Legge e da ogni eventuale spesa di Segreteria.
  Tutti i preventivi (salvo espressa indicazione) sono validi per 30 gg.
  Le offerte (salvo espressa indicazione) s'intendono con pagamento 60gg df. su
  Banco di Desio intestato a Si.Re. Informatica S.r.l. – Agenzia di Tortona
  IBAN: IT49Q 03440 48670 000002117600 – ABI 03440 – CAB 48670 – C/C 2117600

# Principali novità

Le principali novità introdotte dal Regolamento Generale sulla Protezione dei dati personali (RGPD) possono essere così sintetizzate:

- ✓ Il RGPD ridisegna il ruolo, i compiti e le responsabilità del Titolare e del Responsabile del trattamento dei dati personali in relazione ai nuovi principi e strumenti introdotti dallo stesso. E' inoltre introdotta la responsabilità diretta dei titolari del trattamento in merito al compito di assicurare, ed essere in grado di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali;

- ✓ è definita la nuova categoria di dati personali (i c.d. dati sensibili di cui al precedente Codice Privacy);

- ✓ viene istituita la figura obbligatoria del Responsabile della protezione dei dati (DPO o RDP), incaricato di assicurare una gestione corretta dei dati personali negli enti. Tale figura può essere individuata tra il personale dipendente in organico, oppure è possibile procedere a un affidamento all'esterno, in base a un contratto di servizi. Nel caso di Comuni di minori dimensioni demografiche, è possibile l'affidamento dell'incarico di RPD ad un unico soggetto, anche esterno, designato da più Comuni mediante esercizio associato della funzione nelle forme previste dal D.Lgs. 18 agosto 2000 n. 267;

- ✓ viene introdotto il Registro delle attività del trattamento ove sono descritti i trattamenti effettuati e le procedure di sicurezza adottate dall'ente;

- ✓ viene richiesto agli enti l'obbligo, prima di procedere al trattamento, di effettuare una Valutazione di Impatto sulla Protezione dei Dati (DPIA). Tale adempimento è richiesto quando un tipo di trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. (Si pensi, ad esempio, ai dati ottenuti dalla sorveglianza di zone accessibili al pubblico).


# Adempimenti

Molto importante per l'applicazione della nuova normativa è la revisione dei processi gestionali interni, finalizzata a raggiungere i più adeguati livelli di sicurezza nel trattamento dei dati personali. Ciò è ottenibile attraverso una prima opera di rilevazione dei processi di gestione e degli strumenti utilizzati dal Comune, alla quale seguirà la definizione degli interventi operativi necessari e l'adeguata implementazione delle modalità ritenute idonee a raggiungere i predetti livelli. A corollario di questi interventi si potrà riscontrare la necessità di una revisione dei processi ed eventualmente delle norme regolamentari interne laddove necessario e/o opportuno.

Le attività da svolgere possono sinteticamente essere così individuate (in successione temporale):

- ✓ mappatura dei processi per individuare quelli collegati al trattamento dei dati personali;
- ✓ individuazione, nell'ambito della suddetta mappatura, dei processi che presentano rischi con una prima valutazione degli stessi;
- ✓ definizione delle proposte di miglioramento dei processi ed eventualmente della regolamentazione interna;
- ✓ interventi formativi per il personale.

Dunque, schematicamente ed anche sulla scorta delle linee guida tracciate da ANCI, i primi adempimenti che è necessario porre in essere (prima del 25 maggio 2018) sono:

- ✓ la nomina del RPD (o DPO);
- ✓ l'adozione del Registro dei trattamenti di dati personali (obbligatorio per il Titolare) e del Registro delle categorie di attività trattate da ciascun Responsabile del trattamento, che hanno contenuti obbligatori previsti specificamente dal RGPD. I registri possono comprendere anche altre informazioni non obbligatorie, al fine di garantire il perfetto allineamento con i principali "oggetti" (mappa dei processi, organigramma dell'ente, portafoglio fornitori, mappa degli applicativi);
- ✓ la mappatura dei processi.

Tutte le informazioni raccolte per definire i contenuti dei Registri saranno utili anche successivamente, quando andranno identificati e valutati i principali gaps da colmare per essere conformi al RGPD, cioè per definire e redigere, alla luce dei divari evidenziati, un piano di adeguamento complessivo (action plan), nonché per attuare l'implementazione ed il conseguente monitoraggio degli interventi previsti.

Tale processo può essere attuato seguendo lo schema indicato di seguito:

1. struttura organizzativa: definizione, formalizzazione e implementazione della struttura organizzativa del sistema di data protection, sia a livello di macro-struttura sia a livello di micro-struttura (ruoli e responsabilità);

2. soggetti coinvolti: sensibilizzazione e formazione dei soggetti chiamati a ricoprire un ruolo attivo nell'ambito del modello di funzionamento della data protection, ma anche dei soggetti del Comune indirettamente coinvolti nella protezione dei dati personali;

3. processi: definizione, formalizzazione e implementazione di processi e regole connessi alla protezione dei dati personali, sia in modo diretto (ad esempio la gestione dei diritti degli interessati) sia in modo indiretto (ad esempio la gestione delle misure di sicurezza tecnico-organizzative);

4. documentazione: stesura ex novo della documentazione o modifica della documentazione esistente (ad esempio informative, moduli di consenso, clausole contrattuali) e avvio della relativa adozione, anche verso l'esterno;

5. controlli interni: definizione e implementazione di un sistema di controlli interni per la protezione dei dati personali (ad esempio il sistema di deleghe), ivi compresa la realizzazione di "internal audit" volti a evidenziare eventuali non conformità.

A valle dell'intero processo di adeguamento deve essere quindi effettuato un controllo periodico in merito alla corretta adozione del modello di funzionamento della data protection ed elaborazione di eventuali azioni correttive, con conseguente aggiornamento del modello stesso.


# Servizi offerti

1. attività di formazione:
   - ✓ inquadramento generale a tutti gli operatori su privacy e rapporti con trasparenza e anticorruzione
   - ✓ formazione specialistica (normativa) per titolari di P.O.
   - ✓ formazione specialistica (tecnica) per amministratori di sistema (o referenti informatici)

2. predisposizione/adeguamento e fornitura modulistica comprendente:
   - ✓ Regolamento comunale per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e bozza di delibera di approvazione;
   - ✓ modello di Informativa per il trattamento dei dati personali e richiesta di consenso;
   - ✓ modello di atto di designazione del RPD (o DPO) e relative clausole contrattuali;
   - ✓ modello di atto di designazione del Responsabile del trattamento e relative clausole contrattuali;
   - ✓ modello di atto di designazione del Sub-Responsabile del trattamento e relative clausole contrattuali;
   - ✓ modello di atto di designazione dell'Incaricato del trattamento e relative clausole contrattuali;
   - ✓ modello di atto di designazione del Co-Titolare del trattamento e relative clausole contrattuali (ad es. nel caso di esercizio associato di funzioni e servizi);
   - ✓ modello di atto di designazione del Delegato del Titolare del trattamento e relative clausole contrattuali;
   - ✓ modello di atto di designazione del Responsabile della Sicurezza dei Sistemi Informativi e relative clausole contrattuali;
   - ✓ modello di clausole contrattuali da inserire nella modulistica contrattuale dell'Ente (appalti, concessioni, incarichi professionali, ...);
   - ✓ modulistica ad uso del RPD (o DPO) per lo svolgimento dell'attività istituzionale;
   - ✓ modulistica per "attività di vigilanza" (audit) interno;

3. Implementazione/aggiornamento di apposita sezione "trattamento dati personali" sul sito web dell'Ente (e coordinamento con sezione "Amministrazione trasparente");

4. Assistenza nell'individuazione ed adozione delle misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

5. Implementazione/aggiornamento e fornitura (in formato elettronico) dei Registri delle attività di trattamento previsti dall'articolo 30 del GDPR;

6. Assistenza nelle valutazioni circa l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato;

7. Assunzione della veste di RPD (o DPO) e, in tale veste, svolge i compiti assegnatigli dal GDPR ed inoltre:
   a) procede ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;
   b) definisce un ordine di priorità nell'attività da svolgere - ovvero un piano annuale di attività - incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare ed al Responsabile del trattamento;
   c) è invitato a partecipare alle riunioni di coordinamento dei Dirigenti/Responsabili P.O. che abbiano per oggetto questioni inerenti la protezione dei dati personali (direi che partecipa ad un massimo di 1 riunione/mese, salvo rimborso spese);
   d) deve essere consultato tempestivamente qualora si verifichi una violazione dei dati od un altro incidente;

8. Assistenza nella procedura di valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 del GDPR;

9. Assistenza nella procedura esperita a seguito della "Violazione dei dati personali" (Data breach) ai sensi dell'art. 33 del GDPR, compresa l'assistenza nel procedimento di notifica al Garante;

Giornata di approfondimento con il Patrocinio del:

# *COMUNE DI CELLE LIGURE*

# Mercoledi 18 Aprile 2018

## Il nuovo Regolamento UE in materia di protezione dei dati personali: impatti, sviluppi e nuove sfide negli Enti Locali


Il nuovo GDPR, General Data Protection Regulation (Regolamento UE 2016/679), entra pienamente in vigore il 25 maggio 2018 e obbliga le Pubbliche Amministrazioni ad un effettivo controllo sul trattamento dei dati in proprio possesso e ad una reingegnerizzazione di tutti i processi gestionali, prevedendo anche la nomina di una nuova figura, il Data Protection Officer (DPO).

L'evento vuole coniugare i molteplici aspetti legati alla sicurezza delle informazioni a cui le PA devono prestare attenzione, cercando di mettere a fattor comune adempimenti normativi con strumenti e metodi organizzativi.

Il corso analizza infatti le misure e le metodologie tecniche e gestionali che il DPO e gli altri soggetti responsabili del trattamento dei dati personali devono mettere in pratica al fine di rispettare al contempo i nuovi obblighi del GDPR e le prescrizioni in materia di trasparenza e accesso civico.

Tutte le questioni saranno affrontate durante il convegno in modo da fornire agli intervenuti le informazioni generali necessarie a valutare l'incidenza della nuova normativa sul proprio ambito operativo. Stante tuttavia l'ampiezza e la complessità degli argomenti, la trattazione specifica degli ambiti applicativi viene demandata a successivi incontri a carattere tematico e settoriale.

## Relatore:

Avv. Massimo Ramello Titolare dello Studio "OfficineLegali", collaboratore storico della nostra Azienda, già analista e coordinatore del progetto **DPSonLine** (L.196/2003) con il quale abbiamo servito oltre 400 tra P.A.L. del territorio.

## Destinatari

Il Convegno è dedicato alle Pubbliche Amministrazioni locali, in particolare ai Segretari Comunali, ai Responsabili dell'informatica ed ai Dirigenti e Responsabili dei settori che trattano dati personali e dati sensibili e dovranno adattare le proprie procedure interne entro il 25 maggio 2018 al nuovo Regolamento Europeo sulla Privacy (Servizi Demografici, Tributi, Segreteria).

La gestione di dati personali, anche sensibili e giudiziari, ad opera delle forme associative di Enti locali (comunità montane, unioni di comuni, consorzi, ...) nonché quella in carico alle società partecipate dai medesimi Enti, impone che anche detti soggetti adottino cautele per il trattamento non inferiori a quelle adottate dalle amministrazioni partecipanti.

È dunque consigliata la partecipazione ai responsabili dei settori che trattino dati personali.

## Location e Data

Il Convegno è stato organizzato presso la **Comune di Celle Ligure** in Via Boagno, n. 11 nella sala consigliare.

Il corso avrà luogo in data

**Mercoledi 18 Aprile 2018**

ed avrà inizio alle **ore 9:30** e terminerà alle **ore 13:00**.

Nei giorni successivi sarà distribuita la documentazione digitale e gli attestati di partecipazione (obbligatori per l'adempimento GDPR)

Il corso è gratuito.

Il Convegno è Patrocinato dal Comune di Celle Ligure

# Programma del Seminario:

**Ore 9:00:** Registrazione – ingresso in aula

**Ore 9:30:** Messaggio di benvenuto da parte dell'Amministrazione Comunale.

- **La tutela della privacy in materia di trattamento dei dati personali**:

l'entrata in vigore del nuovo GDPR, General Data Protection Regulation (Regolamento UE 2016/679).
I principi guida della nuova normativa europea. La privacy by design e la privacy by default. La responsabilizzazione dei soggetti (accountability). I nuovi obblighi per le Pubbliche Amministrazioni, le nuove procedure e le nuove figure. Le Linee guida del Gruppo di lavoro art. 29 concernenti la valutazione di impatto sulla protezione dei dati ai sensi del GDPR.
Evoluzione della normativa in materia di privacy: dal d.lgs. 196/2003 al nuovo regolamento europeo sulla data protection.
Dalla visione amministrativa burocratica ad un concetto di responsabilizzazione.
Dati personali e pubblica Amministrazione.
Il principio di responsabilizzazione e l'interazione con l'Autorità Garante.
Come cambiano i principi e i diritti degli interessati.

- **Il rapporto tra GDPR e obblighi di trasparenza e accesso civico della PA**

I limiti generali alla trasparenza.
I limiti e le modalità di pubblicazione dei dati personali e dei dati sensibili e il divieto di pubblicazione di dati ulteriori rispetto alle finalità di trasparenza.
Le Linee guida ed i pareri del Garante per la protezione dei dati personali in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati.
Le Linee guida ANAC in materia di esclusioni e limiti all'accesso civico generalizzato Albo pretorio on line e diritto all'oblio.

- **Adempimenti operativi**

L'istituzione del registro dei trattamenti.
La progettazione dei documenti informatici nell'ottica del rispetto della privacy e l'individuazione di specifiche tecniche di tutela della sicurezza.
Gli obblighi di informativa ed i diritti dell'interessato. I limiti al riutilizzo dei dati. La durata degli obblighi di pubblicazione.
Il diritto all'oblio e la possibilità di richiedere variazioni dei propri dati personali da parte degli interessati.
"Data protection by default and by design", valutazione di impatto e consultazione preventiva

## ➢ La privacy e la security

Le misure minime di sicurezza e le sfide della PA sul data protection. I rischi interni ed esterni sulla protezione dei dati personali tra policy di sicurezza e cyber crimine.
La conservazione e cancellazione sicura dei dati personali e le responsabilità per gli amministratori di sistema. La privacy e l'utilizzo del cloud.
La valutazione dei soggetti che concorrono con la PA al trattamento dei dati personali.
Le best practices sulla sicurezza dei dati personali.
Sicurezza, minimizzazione dei rischi e data breach

## ➢ Gli attori del cambiamento

L'individuazione del Responsabile della privacy e degli incaricati al trattamento dei dati personali.
L'obbligatorietà della nuova figura del Data Protection Officer (DPO) per tutte le Pubbliche Amministrazioni. Ruolo, funzioni e requisiti soggettivi. Il coordinamento con il Responsabile della Trasparenza. Come scegliere il Responsabile della Protezione dei Dati.
Gli adempimenti operativi connessi alle figure che operano in qualità di amministratori di sistema.

## ➢ Le nuove ipotesi di responsabilità previste dal Regolamento UE 2016/679

L'inasprimento del sistema sanzionatorio.
Le responsabilità civili delle Amministrazioni e il problema dell'individuazione dei danni materiali e immateriali. Le responsabilità penali del Responsabile della privacy e degli incaricati al trattamento.

## ➢ Approfondimento tecnico operativo

Definizione dei percorsi operativi finalizzati all'ottemperamento degli adempimenti esposti e confronto sulle specifiche necessità degli Enti in base alla dimensione, capacità organizzativo - economica ed anche informatica.

## ➢ Dibattito e risposte ai quesiti