SITA srl, Milano – ANCI Liguria, Genova

Webinar Security nei Comuni

PRIVACY E PROTEZIONE DEI DATI NEI COMUNI E NEGLI ENTI LOCALI

Avv. Dino VERCELLI – Avv. Gabriele VERCELLI

Genova – 28 maggio 2025

DI CHE COSA PARLEREMO INSIEME

1. ***Introduzione alla Privacy***
   – *Panoramica generale e sua evoluzione*

2. ***Il quadro normativo per le Pubbliche Amministrazioni***
   – *Norme, evoluzioni ed adempimenti*

1

INTRODUZIONE ALLA PRIVACY

(PANORAMICA ED EVOLUZIONI)

Che cosa è la privacy?

E’ il diritto di ogni persona a **controllare le proprie informazioni personali**, decidendo **chi può accedervi, per quali scopi e in quali contesti**.

Nel mondo digitale, la privacy non è solo una questione individuale, ma ha forti **implicazioni sociali, politiche ed economiche** per la delicatezza e l’importanza dei dati raccolti.

Evoluzione della normativa

- **Prima fase (anni ‘90 – 2000):** protezione formale, legata al concetto di riservatezza (Codice Privacy italiano, Legge 675/1996).

- **Seconda fase (dal 2018):** con il **GDPR** (Regolamento UE 2016/679), la privacy diventa un diritto attivo, basato su **responsabilità, trasparenza, consapevolezza e controllo**.

Il GDPR ha superato i limiti di una normativa statica, imponendo un modello **basato sul rischio**, sull’**accountability** (responsabilizzazione) e sulla **progettazione della tutela**.

Perché la privacy è importante oggi

1. Tutela della dignità

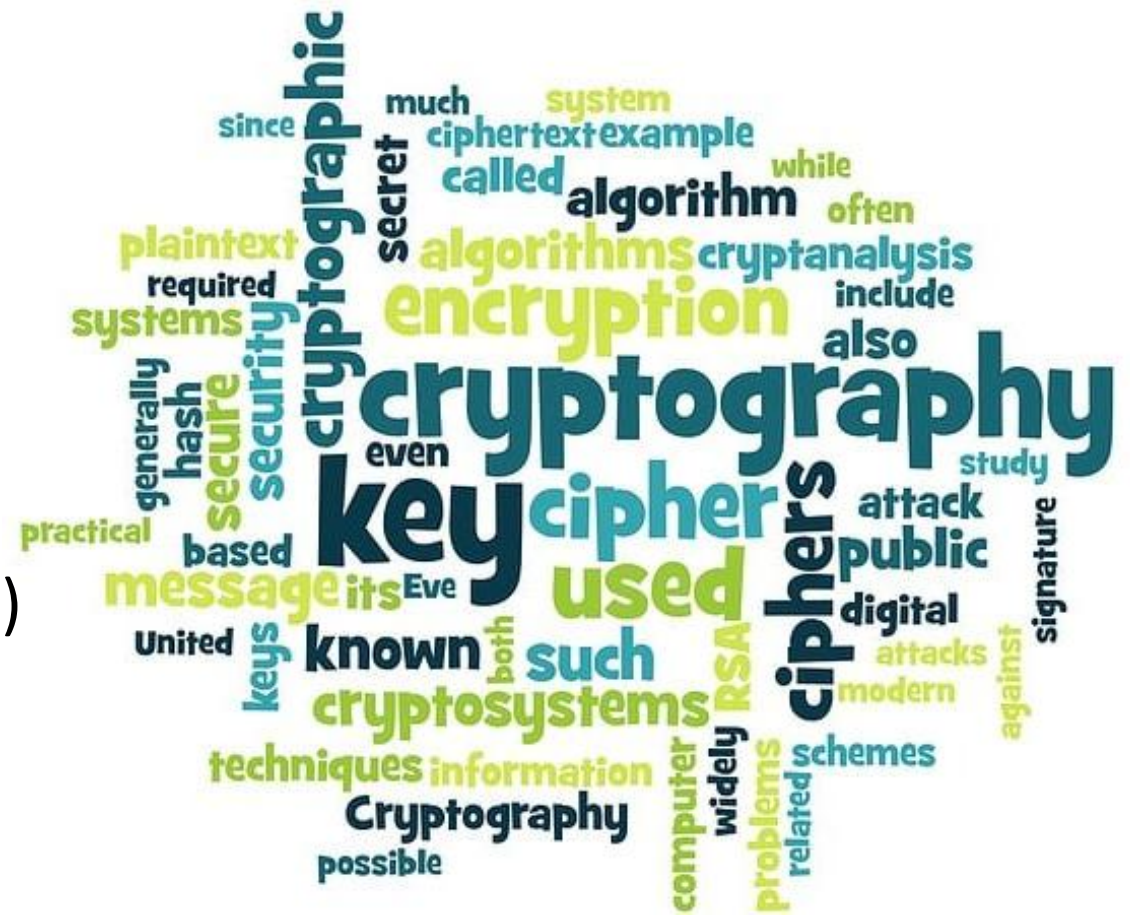
(difendere la libertà, la dignità e l'identità della persona)

2. Fiducia digitale

(fiducia tra cittadini, utenti, aziende e istituzioni)

3. Prevenzione degli abusi

(profilazioni discriminatorie, furti di identità, manipolazione delle opinioni, reati informatici



Dal Codice Privacy al GDPR: le principali novità

- **Cambia l'ambito di applicazione**

  Nazionale vs sovranazionale.

- **Gerarchia normativa**

  Il GDPR è un **regolamento**, non una direttiva

- **Il ruolo del consenso**

  Deve essere **informato, libero, specifico, inequivocabile** e **facilmente revocabile**.

  NB nuove basi giuridiche: può essere lecito per l'esecuzione di un contratto, un obbligo legale o per un interesse legittimo.

- **Accountability: il principio di responsabilizzazione**

  Dimostrare di averle applicato le norme correttamente.
  Questo implica:

  - la **documentazione delle scelte** fatte;
  - l'adozione di **misure tecniche e organizzative** adeguate;
  - protezione dei dati integrata sin dalla progettazione dei sistemi.

- **Valutazione d'impatto (DPIA)**

  Obbligo di effettuare una **DPIA** (*Data Protection Impact Assessment*) in caso di rischio elevato per i diritti degli interessati.

- **Registro dei trattamenti**

  Obbligo **registro dei trattamenti** (essenziale in caso di controlli).

- **Notifica delle violazioni (*data breach*)**
  - **Obbligo a notificare l'evento al Garante entro 72 ore;**
  - informare anche gli interessati, se il rischio è elevato.

- **Il Responsabile della protezione dei dati (DPO)**

  Obbligatorio in caso di: enti pubblici; trattamenti su larga scala di dati sensibili o giudiziari; monitoraggio sistematico e regolare degli interessati.

  NB: il DPO ha un ruolo **di garanzia e consulenza**, e funge da punto di contatto.

Approfondimenti e Principi Generali del GDPR

- **Liceità, correttezza e trasparenza**

  Liceità = il trattamento dei dati deve avere le **basi giuridiche** previste all'art. 6 del GDPR.

  Correttezza = il trattamento non deve **sorprendere né danneggiare l'interessato**.

  Trasparenza = l'interessato sia **informato in modo chiaro, semplice e accessibile** sul trattamento (sapere **chi tratta i dati, perché e come)**

- **Limitazione della finalità**

  I dati devono essere raccolti per **finalità determinate, esplicite e legittime.** L'interessato deve sapere **a cosa servono i suoi dati**.

- **Minimizzazione dei dati**

  Devono essere trattati **solo i dati adeguati, pertinenti e limitati** a quanto necessario rispetto alle finalità per cui sono raccolti (il principio del **"data economy"**)

- **Esattezza dei dati**

  I dati devono essere **corretti e aggiornati,** cancellando quelli inesatti.

  Esempio: un ente pubblico che utilizza dati anagrafici errati per notificare multe o atti amministrativi e può incorrere in gravi responsabilità.

- **Limitazione della conservazione**

  Conservati **per un tempo non superiore** a quello necessario rispetto alle finalità.

2

IL QUADRO NORMATIVO

(PER LE PUBBLICHE AMMINISTRAZIONI)

Adempimenti per i comuni rispetto al GDPR

1° ADEMPIMENTO - NOMINA DEL DPO

Chi è il DPO e perché è importante?

Il DPO è una figura **autonoma e indipendente** che svolge diverse funzioni dalla vigilanza, alla sicurezza e consulenza ed è di supporto in materia di protezione dei dati personali all'interno dell'ente.

Attenzione: il DPO **non sostituisce il dirigente** o il responsabile del servizio, ma li **affianca** con un ruolo trasversale e indipendente.

Quando è obbligatorio il DPO?

E' **obbligatoria per tutti gli enti pubblici**, senza eccezioni.

NB: il DPO va comunicato al Garante tramite un modulo disponibile sul sito del Garante e deve contenere i dati di contatto del DPO, affinché i cittadini possano raggiungerlo in caso di dubbi o reclami.

Quali sono le funzioni principali del DPO?

1. **Informare e consigliare** l'ente e i dipendenti sui loro obblighi in materia;
2. **Sorvegliare la conformità** al GDPR, al Codice Privacy e alle politiche interne;
3. **Fornire pareri su DPIA** e verificare la corretta esecuzione delle valutazioni d'impatto;
4. **Cooperare con il Garante** per la protezione dei dati;
5. **Fungere da punto di contatto** per l'autorità di controllo e per i cittadini.

Caratteristiche del DPO

- **Indipendenza**: il DPO deve agire in **piena autonomia**, senza ricevere istruzioni sulle modalità di svolgimento dei suoi compiti.
- **Assenza di conflitto di interessi**: non può ricoprire ruoli che prevedano la determinazione delle finalità e dei mezzi del trattamento (es. responsabile dei servizi informatici, del personale o dell'anagrafe).
- **Accesso alle risorse**: deve disporre del tempo, del supporto e delle informazioni necessarie per svolgere i suoi compiti.
- **Accesso diretto alla dirigenza**: deve poter riferire direttamente al vertice politico e amministrativo.

Competenze richieste al DPO

Il GDPR richiede "**conoscenze specialistiche della normativa e delle prassi in materia di protezione dei dati**, nonché la capacità di assolvere i propri compiti".

Errori da evitare nella gestione del DPO

1. **Nomina solo formale**
2. **Mancata consultazione**
3. **Isolamento organizzativo**
4. **Conflitto di interessi**

2° ADEMPIMENTO – Registro dei trattamenti

Ogni amministrazione deve tenere un **registro aggiornato dei trattamenti**. Nel registro vanno elencati tutti i trattamenti di dati personali svolti dall'ente, per ciascun ufficio, con indicazione di:

- **finalità;**
- **base giuridica;**
- **categorie di dati trattati;**
- **destinatari;**
- **tempi di conservazione;**
- **misure di sicurezza.**

3° ADEMPIMENTO – Informativa Privacy

Ogni cittadino che fornisce i propri dati ha diritto a ricevere un'**informativa chiara e comprensibile**.

NB: servono testi scritti in modo semplice, facilmente accessibili, specifici per ciascun trattamento. Informative generiche, copia-incolla da altri modelli, non aiutano né l'ente né il cittadino.

4° ADEMPIMENTO – Valutazione d'impatto (DPIA)

Quando si introducono **trattamenti nuovi** o **potenzialmente rischiosi**, come la videosorveglianza, i sistemi di controllo automatizzato, l'uso di dati sensibili in ambito sociale o sanitario, è necessario effettuare una **valutazione d'impatto**.

Questo è un altro punto cruciale del GDPR, spesso trascurato o percepito come puramente burocratico. **Ogni volta che introduciamo un'attività nuova, complessa o delicata** dobbiamo porci la domanda: *"ci sono rischi elevati per la privacy delle persone?"*

Cos'è, in sintesi, una DPIA?

La DPIA è un **processo sistematico** che serve a:

- Descrivere i trattamenti previsti;
- Valutare la **necessità e proporzionalità** del trattamento;
- Identificare i **rischi** per i diritti e le libertà degli interessati;
- Individuare **misure per mitigare quei rischi**.

In altre parole, è uno strumento **preventivo**, che permette all'ente di correggere eventuali criticità **prima** che si verifichino violazioni.

Quando è obbligatoria?

Blacklist dei trattamenti che **richiedono sempre** una DPIA da parte dei soggetti pubblici:

1. **videosorveglianza sistematica e su larga scala;**
2. **monitoraggio sistematico** degli interessati (presenze tramite badge biometrico);
3. trattamento **di categorie particolari di dati** (salute, disabilità, ass. sociale);
4. **interconnessione massiva di banche dati** (integrazione tra software gestionali diversi);
5. Trattamenti che **incidono sulla persona** (graduatorie automatizzate, sistemi di punteggio);

Esempi:

- l'installazione di nuove telecamere in aree pubbliche comporta una DPIA;
- l'uso di dati sanitari nel sistema di assistenza domiciliare potrebbe richiederla;
- l'informatizzazione completa dei servizi scolastici con raccolta di dati sensibili;

Errori comuni negli enti pubblici

- **Non fanno la DPIA pensando che serva solo per i privati**.
- **Confondono la DPIA con la semplice valutazione dei rischi**
- La fanno **solo dopo aver già avviato il trattamento**, quando dovrebbe essere **ex ante**.
- Utilizzano modelli **standardizzati e generici**, senza personalizzare l'analisi.

RUOLO DEL DPO NELLA DPIA

Il DPO deve esprimere un parere sulle misure proposte e partecipare alla redazione della valutazione. Il suo parere va messo agli atti: non è vincolante, ma l'ente deve tenerne conto.

Cosa succede se la DPIA evidenzia un rischio alto?

In casi estremi, se dopo la DPIA restano **rischi elevati non mitigabili**, il GDPR impone di **consultare il Garante prima di iniziare il trattamento**. Questo strumento si chiama "consultazione preventiva" (art. 36).

***NB**: sarebbe auspicabile che **ogni nuovo progetto digitale**, ogni nuovo trattamento significativo, **preveda una check-list di verifica DPIA**, da fare **prima dell'avvio operativo**.*

5° ADEMPIMENTO – Responsabili esterni del trattamento

Molti comuni affidano servizi a soggetti esterni: gestione del software, servizi scolastici, riscossione tributi. In tutti questi casi, se il fornitore accede a dati personali, va nominato **responsabile del trattamento**, con un **contratto scritto**, che contenga istruzioni precise.

Attenzione: non è sufficiente una clausola generica nei contratti di servizio. Serve un **atto specifico**.

6° ADEMPIMENTO – Formazione del personale

Chi lavora ogni giorno con dati personali (anagrafe, tributi, servizi sociali) deve sapere cosa può fare e cosa no. Serve una **formazione pratica**, non solo teorica.

AREE CRITICHE E PROBLEMATICHE RICORRENTI

- **Privacy e criticità nei servizi sociali e scolastici**

Si tratta di servizi che riguardano migliaia di cittadini, che spesso vivono condizioni di fragilità. richieste di assistenza economica o abitativa;

NB: In questi ambiti, il trattamento dei dati personali è inevitabile ma anche **molto delicato**, perché spesso si tratta di **categorie particolari di dati** (ex art. 9 GDPR), come **dati sanitari** (es. invalidità, certificati 104, allergie);

Rischio: trattamento non necessario o non autorizzato di dati altamente protetti.

- **Informative assenti o generiche**

  Molti moduli usati nei servizi sociali non forniscono un'adeguata informativa agli interessati:

  - chi è il titolare del trattamento;
  - quali dati vengono raccolti e per quali finalità;
  - se i dati saranno condivisi con terzi (es. ASL, cooperative).

  Rischio: violazione del principio di trasparenza e mancata base giuridica valida.

- **Condivisione informale di dati con soggetti esterni**

  In molti comuni, i servizi sociali collaborano con enti del terzo settore, cooperative, scuole o altri enti. Tuttavia, **spesso non viene formalizzata la nomina a responsabile del trattamento**, oppure si condividono dati via email senza garanzie di sicurezza.

  Rischio: accesso non autorizzato o perdita dei dati e conseguente **data breach**.

- **Eccesso di dati pubblicati in atti amministrativi**

Nei provvedimenti di concessione di contributi economici, borse di studio o agevolazioni scolastiche, si inseriscono ancora troppo spesso **dati personali non necessari**, come:

- nome e cognome del beneficiario;
- indirizzo;
- motivazioni legate alla situazione di bisogno;
- riferimenti a condizioni di disabilità o problemi familiari.

Rischio: violazione del principio di minimizzazione (art. 5.1.c GDPR) e sanzioni del Garante.

- **Conservazione dei dati per tempi eccessivi**

  Spesso non vengono stabiliti **termini precisi di conservazione** dei dati raccolti per domande o istruttorie. Questo comporta la permanenza nei sistemi di dati sensibili **anche dopo anni dalla conclusione del procedimento**.

  Rischio: violazione del principio di limitazione della conservazione (art. 5.1.e GDPR).

  NB: caso rilevato dal Garante – ambito **servizi sociali e cooperative**

  Un ente locale ha trasmesso via email ordinaria i nominativi di beneficiari di un servizio di assistenza domiciliare a una cooperativa esterna **senza nomina a responsabile del trattamento**. Il Garante ha contestato la **mancanza di adeguate garanzie contrattuali** e di misure tecniche minime (es. crittografia, protezione degli allegati).

BUONE PRASSI CONSIGLIATE

1. **Predisporre informative specifiche** per ogni servizio (sociale e scolastico), comprensibili anche ai genitori e ai minori.
2. **Formalizzare le nomine** a responsabili del trattamento con cooperative, società esterne, scuole paritarie.
3. **Usare modelli di determina privacy-by-design**, che evitino l'inserimento di dati non necessari negli atti pubblici.
4. **Limitare la diffusione online** di elenchi, graduatorie e concessioni nominative, se non richiesto da obbligo normativo.
5. **Conservare i dati solo per il tempo necessario**, stabilendo scadenze nei regolamenti o nelle informative.
6. **Formare regolarmente il personale** su questi temi, con il supporto del DPO.

CRITICITÀ

LA VIDEOSORVEGLIANZA

Molti comuni hanno installato telecamere per la sicurezza urbana, spesso con finanziamenti regionali. Ma attenzione, la **videosorveglianza è lecita solo se giustificata**, con cartelli ben visibili, tempi di conservazione precisi e, in molti casi, una valutazione d'impatto.

NB: le telecamere non devono mai essere usate per controllare il comportamento dei dipendenti o dei cittadini in modo generico.

In Italia, il Garante ha pubblicato **Linee guida sulla videosorveglianza** aggiornate al 2020, che forniscono indicazioni puntuali per enti pubblici.

Errori comuni da evitare

- Installare telecamere **senza informativa visibile** (i cartelli "area videosorvegliata" sono obbligatori e devono contenere dati chiari).
- Mantenere le registrazioni **per periodi eccessivi** (il Garante raccomanda al massimo **7 giorni**, salvo motivazioni forti).
- Utilizzare telecamere per **controllare i dipendenti**, salvo casi molto specifici e con garanzie sindacali.
- Mancare la **DPIA obbligatoria**: la videosorveglianza sistematica è uno dei casi che richiede una valutazione d'impatto.

Caso reale

Un comune ha installato telecamere vicino a una scuola e a un parco giochi, senza informativa visibile, senza DPIA e con conservazione delle immagini per 30 giorni. A seguito di un reclamo di un genitore, il Garante ha ordinato **la cessazione del trattamento** e ha imposto **una sanzione di 15.000 euro**.

Buone prassi operative

- Redigere una **DPIA preventiva**.
- Installare cartelli visibili e aggiornati.
- Definire per iscritto chi accede alle immagini e con quali credenziali.
- Conservare i filmati solo per il tempo strettamente necessario.
- Coinvolgere il DPO fin dalle fasi iniziali.

PRIVACY E TRASPARENZA – UN EQUILIBRIO NECESSARIO

Uno dei punti più delicati per la pubblica amministrazione è il bilanciamento tra **trasparenza amministrativa** e **protezione dei dati personali**.

Entrambi i principi hanno un valore costituzionale:

- la **trasparenza** tutela la legalità, l'efficienza e il controllo dei cittadini sull'attività amministrativa;
- la **privacy** protegge i diritti, la dignità e la libertà individuale.

Il punto è che **non c'è una gerarchia tra i due principi**: vanno bilanciati caso per caso, tenendo conto della **necessità**, **proporzionalità** e **adeguatezza** della diffusione dei dati.

Esempi tipici di rischio

- Pubblicazione online di **graduatorie nominative** di concorsi o bandi con dati non indispensabili (es. indirizzi, codici fiscali).
- Determine e delibere con **dettagli su situazioni personali** (es. contributi sociali, disabilità, debiti tributari).
- Atti di concessione di benefici economici con dati sanitari o familiari non pertinenti.

Il principio guida: "se un dato personale non è **strettamente necessario** per la finalità di trasparenza, **non va pubblicato**."

Caso reale: un piccolo comune ha pubblicato la graduatoria di beneficiari contributi sociali, Il Garante ha imposto **l'oscuramento dei dati**, ritenendo eccessiva la diffusione e lesiva della dignità degli interessati. E ha comminato una sanzione di EUR 10.000

CONCLUSIONE

La privacy non è un ostacolo al buon funzionamento della pubblica amministrazione. Al contrario, è una **condizione di legittimità, fiducia e qualità del servizio**. Un'amministrazione che rispetta i dati dei cittadini dimostra di rispettare la loro dignità, la loro libertà, i loro diritti.

NB: anche i piccoli comuni possono fare molto, se adottano **un approccio consapevole, responsabile e collaborativo**.

GRAZIE PER L'ATTENZIONE!

SITA – Services for Integrated Technical Assistance

Via Cellini 1 – 20129 MILANO

info@sita-international.eu