Comune di Muccia

Provincia di Macerata

Valutazione di impatto

(***D.P.I.A.*** - Data Protection Impact Assessment o ***P.I.A.*** - Privacy Impact Analysis)

Articolo 35 del Regolamento generale per la protezione dei dati (RGPD - REGOLAMENTO - UE - 2016/679)

Il documento è stato redatto, a cura del RPD, in data 27/02/2024.

Approvato con deliberazione di Giunta Comunale n. 10 in data 06/03/2024

Responsabile della Protezione dei Dati (RPD-DPO)

Gruppo Gaspari – Servizio privacy

Siamo contattabili

Via e-mail: privacy@gaspari.it

Via PEC: privacy@pec.egaspari.net

Via Posta ordinaria: Grafiche E.Gaspari Srl, Via M. Minghetti - 18, 40057, Cadriano di Granarolo Emilia (Bologna)

Via telefono: 051-763201

1. Cos'è la valutazione di impatto

(D.P.I.A. - Data Protection Impact Assessment o P.I.A. - Privacy Impact Analysis)

1.1. Premesse normative

Regolamento generale per la protezione dei dati (RGPD - REGOLAMENTO - UE - 2016/679)

Articolo 35 Valutazione d'impatto sulla protezione dei dati

1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. ***Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi***.

2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.

3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:

a) *una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;*

b) *il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o*

c) *la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.*

4. L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68[1].

---

[1] *Il Garante della Privacy italiano ha emanato un "**Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679 - 11 ottobre 2018** - (Pubblicato sulla Gazzetta Ufficiale Serie Generale n. 269 del 19 novembre 2018)" - In questo elenco sono previste le seguenti fattispecie:*

- *Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato".*
- *Trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi).*
- *Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc.*

5. L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.

6. Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.

7. La valutazione contiene almeno:

a) *una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;*

b) *una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;*

c) *una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e*

d) *le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.*

8. Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.

---

effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.

- *Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).*
- *Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).*
- *Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).*
- *Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01 .*
- *Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.*
- *Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment).*
- *Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.*
- *Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.*
- *Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.*

9. Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.

10. Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e)[2], trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, ***i paragrafi da 1 a 7 non si applicano***, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.

11. Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.

---

[2] ***Regolamento generale per la protezione dei dati (RGPD - REGOLAMENTO - UE - 2016/679)***

Articolo 6 Liceità del trattamento

1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:
[…]
*c) il trattamento **è necessario per adempiere un obbligo legale** al quale è soggetto il titolare del trattamento; […]*
*e) il trattamento **è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento**; (C45, C46)*

1.2. Premesse metodologiche

Il Garante della Privacy italiano, ha messo a punto un opuscolo che tra le altre cose [*https://www.garanteprivacy.it/documents/10160/0/Infografica+-+Valutazione+d+impatto+sulla+protezione+dei+dati++-+DPIA.pdf/13477c9e-1e81-4edc-9fa3-4ccf8e7b0e6d?version=1.3*] prevede:

> " *La DPIA è uno strumento importante in termini di responsabilizzazione (accountability) in quanto aiuta il titolare non soltanto a rispettare le prescrizioni del RGPD, ma anche ad attestare di aver adottato misure idonee a garantire il rispetto di tali prescrizioni. In altri termini, la DPIA è una procedura che permette di valutare e dimostrare la conformità con le norme in materia di protezione dei dati personali. Vista la sua utilità, il Gruppo Art. 29 suggerisce di valutarne l'impiego per tutti i trattamenti, e non solo nei casi in cui il Regolamento la prescrive come obbligatoria.*"

A tal fine ha collaborato con il Garante della Privacy Francese per mettere a punto un software open source, simili a quello che hanno messo in commercio diverse aziende private; nella pagina download [https://www.garanteprivacy.it/regolamentoue/DPIA#STRUMENTI] del software ha premesso:

> *"Il software qui presentato NON costituisce un modello al quale fare riferimento in ogni situazione di trattamento, essendo stato concepito soprattutto come ausilio metodologico per le PMI. Offre in ogni caso un focus sugli elementi principali di cui si compone la procedura di valutazione d´impatto sulla protezione dei dati. Potrebbe costituire quindi* ***un utile supporto di orientamento allo svolgimento di una DPIA****, ma non va inteso come schema predefinito per ogni valutazione d´impatto che va integrata in ragione delle tipologie di trattamento esaminate.*
>
> *E´ inoltre bene ricordare che la valutazione d´impatto sulla protezione dei dati deve tenere conto del rischio complessivo che il trattamento previsto può comportare per i diritti e le libertà degli interessati, alla luce dello specifico contesto. Pertanto, il concetto di rischio non si esaurisce nella considerazione delle possibili violazioni o minacce della sicurezza dei dati."*

1.3. Individuazione e gestione del rischio

Per valutare quali rischi corrono i dati personali dei cittadini che vengono trattati dal titolare e dal responsabile del trattamento, bisogna individuare una serie di elementi che il Garante della Privacy italiano ha messo a fuoco in alcune diapositive pubblicate sul suo sito e che riproduciamo in parte qui di seguito

[https://www.garanteprivacy.it/documents/10160/0/Individuazione+e+gestione+del+rischio+-+Tutorial+-+slide.pdf/d2eb9375-c577-4ff3-b716-38cc703ec26f?version=1.0]:

ATTENZIONE!

Regolamento UE/2016/679

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Aspetti riguardanti la sicurezza del trattamento

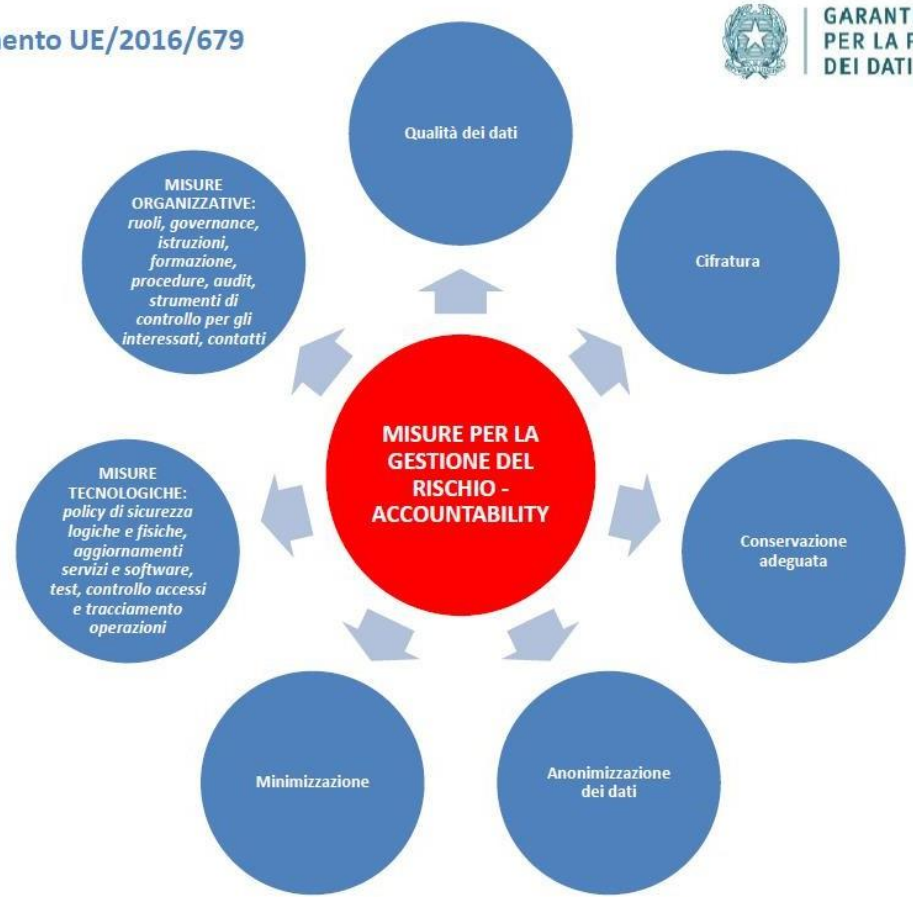
- **DISPONIBILITÀ**
  -distruzione
  -indisponibilità
  -perdita
- **INTEGRITÀ**
  -alterazione
- **RISERVATEZZA**
  -divulgazione
  -accesso

Regolamento UE/2016/679

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Regolamento UE/2016/679

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI



1.4. La valutazione di impatto per un comune, modalità

Abbiamo visto in queste premesse normative e metodologiche quattro elementi fondamentali e parzialmente contraddittori, ancora non chiariti né dal Garante né dalla dottrina, che faticosamente sta cercando di assestarsi:

1. *Quando un trattamento di dati è massivo, come quello effettuato da un comune, sembrerebbe obbligatorio fare la PIA*
2. *Quando però un trattamento di dati è previsto e disciplinato da norme imperative o è effettuato nell'ambito di un pubblico interesse, come tutti i trattamenti di dati del comune, sembrerebbe escluso che debba essere sottoposto a PIA*
3. *I prodotti informatici in commercio e il software open source del Garante non sono predisposti per i comuni, ma per le piccole e medie imprese;*
4. *Sembra opportuno in questa prima fase di applicazione del RGPD, effettuare comunque una PIA anche se non obbligati*

Ciò premesso qui di seguito effettuiamo una PIA, tenendo conto di due elementi metodologici tra quelli fin qui illustrati:

a) *Faremo, come prevede l'ultimo capoverso del comma 1 dell'art. 35: "Una singola valutazione" per esaminare tutti i trattamenti che si svolgono in comune, in quanto presentano rischi analoghi. L'ipotesi alternativa di fare una PIA per ciascun tipo di trattamento, vista la molteplicità dei trattamenti, non risulta sostenibile economicamente né utile.*

b) *Utilizzeremo gli strumenti di misurazione illustrati nelle slide e nel software opportunamente adattata ad una serie di trattamenti molto diversi, sia come metodologia che come base giuridica, rispetto a quelli delle PMI*

2. Risultati della rilevazione per la valutazione di impatto

Art. 35 del Regolamento generale per la protezione dei dati

(RGPD - REGOLAMENTO - UE - 2016/679)

Sezione 1: adempimenti di carattere generale

1. **E' stato nominato un Responsabile della protezione dei dati?**

   Sì, la nomina è stata ratificata con apposito decreto sindacale a seguito di procedura di affidamento del servizio.

Punti 6 (*Sì= 6 – No = 0*)

2. **E' stata fatta la comunicazione al Garante della Privacy della nomina del RPD?**

   Sì. In concomitanza con la nomina dell'RPD. Di seguito è stata inviata una variazione in data 09/06/2023

Punti 6 (*Sì= 6 – No = 0*)

3. **I dati di contatto del RPD sono presenti sul sito istituzionale?**

   Sì, alla pagina: https://www.comune.muccia.mc.it/privacy/

Punti 6 (*Sì= 6 – No = 0*)

4. **I dati di contatto del RPD sono presenti sulle informative?**

❒ Parzialmente, in quanto il sito e in corso di aggiornamento alle recenti linee guida AGID e verranno caricate nuove schede comprensive di riferimento ad un'informativa generale

Punti 3 (*Sì= 6 – No = 0*)

5. **E' stato adottato un Registro dei trattamenti?**

   Sì, con apposita deliberazione della giunta comunale n. 54 del 09/06/2023.

Punti 6 (*Sì= 6 – No = 0*)

Tot. punti sez.1: 27

Sezione 2: - mappatura del rischio

6. Quando è stato redatto il Registro sono state fatte valutazioni sul rischio dei seguenti trattamenti ?

COD.	Denominazione della banca dati personale	**Massimo 1,5** Per ogni riga

Il punteggio max di 1,5, da assegnare ad ogni riga si ottiene solo se il servizio è gestito direttamente dal comune, sommando questi elementi:

- *Max 0,5 se la banca dati è gestita in formato elettronico con apposito applicativo*
- *Max 0,5 se l'applicativo risponde a criteri di affidabilità*
- *Max 0,5 se gli operatori impiegati sono adeguatamente formati*

Banche dati personali degli "affari generali" e risorse umane		
A01	Anagrafe dei dipendenti e degli amministratori	1
A02	Contratti e ufficio legale	0,5
A03	Dati trattati dall' O.I.V. o dal nucleo di valutazione	1
A04	Dati trattati dal Responsabile Comunale per la prevenzione della corruzione e trasparenza	1
A05	Dati trattati dal Responsabile del Servizio Prevenzione e Protezione e dal medico del lavoro	1
A06	Dati trattati dall'organismo di disciplina	1
A07	Dati personali trattati dal "Responsabile della protezione dei dati"	1
Banche dati personali dei servizi demografici		
A08	Anagrafe comunale o anagrafe nazionale (APR – ANPR)	0,5
A09	Dinamica demografica statistica e censimenti	1
A10	Leva militare e servizio civile volontario	1
A11	Stato civile	1
A12	Elettorato attivo e passivo	1
A13	Carta d'identità (cartacea ed elettronica)	1
A14	Polizia mortuaria e servizi cimiteriali	1
Banche dati personali dei servizi alla persona		
A15	Assistiti e beneficiari di provvidenze	1
A16	Asili nido e scuole dell'infanzia	1
A17	Scuola dell'obbligo – centri giovani	1
Banche dati personali dei servizi di vigilanza e controllo		
A18	Polizia municipale/locale – polizia giudiziaria - Verbali e sistema sanzionatorio	N.R.
A19	Videosorveglianza	N.R.
Banche dati personali dei servizi alle imprese e al patrimonio edile privato		
A20	Sportello unico per le attività produttive	N.R.
A21	Sportello unico per l'edilizia	1
Banche dati personali dei servizi culturali, sportivi e turistici		
A22	Ufficio sport, manifestazioni e turismo	1
A23	Biblioteca comunale – cultura	N.R.
Banche dati personali dei servizi finanziari		
A24	Servizi finanziari – fornitori – destinatari di pagamenti vari	1
A25	Tributi	1

Segue

Banche dati personali dei servizi al terzo settore e alle attività di democrazia diretta		
A26	Protezione civile e attività di cittadinanza attiva	1
A27	Associazioni di volontariato, di promozione sociale e libero associazionismo – comitati	N.R.
A28	Organismi di democrazia diretta: petizioni, consulte, referendum e consultazioni pubbliche	N.R.
A29	Comunicazione istituzionale	N.R.
Banche dati personali dei servizi ai proprietari di animali		
A30	Gestione animali d'affezione (cani, gatti ecc.)	N.R.

N.B. *il punteggio è parametrato sulla base dei trattamenti considerati. Nell'analisi non vengono valutati trattamenti non gestiti o gestiti completamente all'esterno.*

Massimo 30 punti

Tot. punti sez. 2: 19,10

Sezione 3: misure di sicurezza fisiche

7. Sono state adottate queste misure di sicurezza (archivi cartacei) ?

ID	Denominazione scheda registro	**1** punto per ogni misura
1.	Gli accessi nelle stanze in cui sono presenti archivi cartacei sono riservati	1
2.	L'accesso agli archivi cartacei è assicurato con una serratura	1
3.	Sono presenti antifurto	1
4.	Sono presenti sistemi antincendio, climatizzazione ambientale o deumidificazione	0
5.	E' stato redatto un registro d'archivio	1

8. Sono state adottate queste misure di sicurezza (archivi informatici - HARDWARE)?

ID	Denominazione scheda registro	**5** punti per ogni misura
1.	E' stato fatto un piano per il disaster recovery (AGID)	5
2.	E' stata fatta una virtualizzazione dei server	5
3.	E' prevista una rete cablata proprietaria (no WIFI)	5
4.	Il locale server o con gli armadi è sotto protezione fisica e logica	5
5.	I client sono PC o terminali riservati all'uso d'ufficio (no rimovibili)*	2

*Per taluni trattamenti è previsto l'uso di pc portatili

Tot. punti sez. 3: 26

Sezione 4: misure di sicurezza logiche

9. Sono state adottate queste misure "logiche" di sicurezza per gli archivi informatici?

ID	Denominazione scheda registro	**3** punti per ogni misura
1.	E' stato nominato un responsabile del dispiegamento tecnologico (AGID)	3
2.	Sono state assegnati ID – PW – e Credenziali differenziate e personali	3
3.	E' presente un antivirus e/o firewall in grado di inibire la navigazione su siti e procedure pericolose	3
4.	E' presente un sistema strutturato di copie di backup	3
5.	Il software in uso è licenziato e certificato	3
6.	Il software in uso è costantemente aggiornato	3
7.	Esiste una tracciatura dei log di accesso alla intranet	3
8.	Le funzionalità su web sono riservate (non è consentito l'accesso senza profilatura)	3
9.	Il sito istituzionale e i social web in uso sono certificati ai fini privacy	3
10.	E' inibito l'uso dei social media o comunque filtrato dall'antivirus e firewall	0

Tot. punti sez. 3: 27

Sezione 5: - gestione del dato e tutela dei diritti degli interessati

10. L'assetto attuale delle misure adottate permette?

ID	Denominazione scheda registro	**2** punti ** max per ogni riga
1.	L'accesso ai propri dati da parte degli interessati	2
2.	La cifratura dei dati quando prevista dalle norme	2
3.	La pseudonimizzazione del dato nelle pubblicazioni in Amministrazione trasparente	2
4.	La pseudonimizzazione del dato nelle pubblicazioni sull'albo pretorio on line	2
5.	La tutela dei dati degli interessati nelle istanze di accesso generalizzato e documentale	2
6.	La minimizzazione dell'utilizzo dei dati e della loro richiesta	2
7.	L'informativa adeguata, specie per i trattamenti via WEB	2
8.	Evitare furti di identità	2
9.	Evitare data breach ed essere informati tempestivamente qualora avvenga una violazione	2
10.	Sistema di controllo continuo per eventuali alterazioni del dato	2
11.	La predisposizione di misure analoghe alle proprie per i trattamenti eseguiti da terzi responsabili	1
12.	L'aver individuato anche implicitamente i compiti e le funzioni di ciascun addetto	1
13	L'aver promosso iniziative di formazione e informazione per i cittadini	1
14	L'aver promosso iniziative di formazione per i dipendenti	0
15	L'aver adottato nel PTPCT idonee misure che bilancino trasparenza e riservatezza	2

** *Queste 15 misure sono degli obiettivi e, quasi sempre, richiedono un approccio graduale, pertanto il punteggio massimo è riconosciuto solo quando l'obiettivo è raggiunto al 100%; si dia un punteggio proporzionale minore, anche con l'uso dei decimali, per il raggiungimento parziale.*

Tot. punti sez. 5: 25

La rilevazione dei dati e l'assegnazione **provvisoria** dei punteggi è stata eseguita da:

Dott.ssa Antonella Michiorri

Dopodiché i dati rilevati sono stati inseriti nel gestionale, che ha assegnato i relativi punteggi **finali**, dal RPD (Responsabile per la Protezione dei Dati): Gruppo Gaspari - servizio Privacy

3. Risultati e prescrizioni della valutazione di impatto

3.1. Tabella riassuntiva (riportare i punteggi di ciascuna sezione):

Sez.	Denominazione della sezione	Punti
1	***adempimenti di carattere generale***	27
2	***mappatura del rischio***	19,10
3	***misure di sicurezza fisiche***	26
4	***misure di sicurezza logiche***	27
5	***gestione del dato e tutela dei diritti degli interessati***	25
Totale punteggio (somma da 1 a 5)		

Misure da adottare	***Valutazione di impatto*** (*rappresentazione grafica*)				
Se il punteggio della sezione è in questo spazio la situazione è sicura, ma serve vigilare per mantenere i risultati raggiunti	**Da 25 a 30**				
Se il punteggio della sezione è in questo spazio la situazione è già accettabile, ma conviene agire su qualche misura, per consolidare	**Da 19 a 24**				
Se il punteggio della sezione è in questo spazio è utile agire su qualcuna delle misure	**Da 13 a 18**				
Se il punteggio della sezione è in questo spazio è necessario agire sulla maggior parte delle misure	**Da 7 a 12**				
Se il punteggio della sezione è in questo spazio è necessario agire su tutte le misure previste	**Da 0 a 6**				
Gradazione del rischio	Rischio massimo	Rischio elevato	Rischio medio	Rischio Limitato	Rischio Trascurabile

3.2. Prescrizioni del "validatore":

Dall'analisi della rilevazione e dall'esplicazione dei punteggi ottenuti si ritiene necessario prescrivere (per ciascuna sezione):

Sez.	Denominazione della sezione
1	***Adempimenti di carattere generale***
Prescrizioni per l'abbattimento del rischio: L'Ente ha adeguato la propria struttura in modo soddisfacente, adempiendo alle prescrizioni di carattere generale dettate dal Regolamento EU 679. Si raccomanda attenzione al periodico aggiornamento del Registro delle attività di trattamento, nonché un aggiornamento puntuale in caso di variazioni importanti nell'ambito delle figure appositamente designate e dei responsabili del trattamento.	
2	***mappatura del rischio***
Prescrizioni per l'abbattimento del rischio: La maggior parte delle banche dati digitali sono al momento gestite con il supporto di software gestionali, che garantiscono in genere una maggiore protezione dei dati. L'uso di software certificati dovrebbe essere ampliato alle banche dati che attualmente non ne fanno uso. Inoltre, la trasformazione delle banche dati analogiche al formato digitale concorre all'abbattimento del rischio. L'Ente deve aumentare il grado di formazione delle figure designate al trattamento. La formazione concorre notevolmente al contenimento del rischio. Sia al personale storicamente in servizio, che a quello di nuova assunzione, è consigliata la visione dei corsi di formazione base e di aggiornamento prodotti e messi a disposizione dal RPD.	
3	***misure di sicurezza fisiche***
Prescrizioni per l'abbattimento del rischio: L'ente adotta misure di sicurezza fisiche che garantiscono un buon grado di sicurezza, che può essere ulteriormente migliorato grazie all'utilizzo di sistemi di climatizzazione ambientale o deumidificazione. La sicurezza degli archivi cartacei, nelle more di un generalizzato passaggio al digitale, può essere migliorata grazie all'estensione dell'uso di serratura e/o aumentando gli accessi riservati agli uffici da parte del personale appositamente designato al trattamento delle specifiche banche dati ivi conservate. Le misure di sicurezza delle banche dati digitali sono ottimali. Inoltre, questo RPD prende atto che l'Ente sta realizzando progetti che comporteranno il passaggio al Cloud di gran parte degli applicativi informatici. Tale processo non potrà che comportare un miglioramento del sistema di gestione del rischio relativo alla conservazione dei dati, dal momento che tali progetti sono finanziati con fondi PNRR i cui bandi prevedono, per la realizzazione degli stessi, il ricorso a fornitori certificati. Si raccomanda di limitare l'uso di PC rimovibili (portatili) perché tali dispositivi espongono maggiormente al rischio di data breach, rispetto a dispositivi fissi collegati esclusivamente al server di rete comunale.	
4	***misure di sicurezza logiche***
Prescrizioni per l'abbattimento del rischio: Le misure di sicurezza logiche applicate comportano un alto standard di sicurezza.	

Si raccomanda tuttavia la periodica modifica delle password personali da parte delle figure appositamente designate all'accesso alle banche dati, in generale l'attuazione delle prescrizioni riportate nelle recenti linee guida del Garante, pubblicate al seguente link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9962283

Inoltre, è importante aggiornare sempre i software in uso, perché le misure di protezione utilizzate dai software richiedono adeguamenti costanti e in linea con lo sviluppo di nuove minacce informatiche.

5	***gestione del dato e tutela dei diritti degli interessati***

Prescrizioni per l'abbattimento del rischio:

Il miglioramento della gestione del dato richiede un approccio graduale.

Per migliorare il grado di consapevolezza delle figure designate al trattamento dei dati, oltre alla visione dei corsi di formazione già menzionati, è opportuno consultare sempre questo RPD in caso di dubbi o incertezze.

Si prescrive un controllo accurato della formalizzazione delle nomine a Responsabile del Trattamento di cui all'articolo 28 del Regolamento EU 679/16, soprattutto in relazione a servizi continuativi affidati a terzi che prevedono il trattamento di dati personali di cui l'Ente è titolare.

Inoltre, è importante mantenere aggiornati i documenti che regolano compiti e funzioni dei dipendenti comunali, ed eventualmente comunicare l'assegnazione di specifiche responsabilità in caso di trattamenti non previsti dai piani di gestione.

Infine, si consiglia l'avvio di una semplice campagna informativa destinata a dipendenti e cittadini, affiggendo nelle bacheche pubbliche del comune e negli uffici maggiormente preposti alla trasmissione di dati personali (accoglimento istanze da parte dei cittadini) i manifesti già messi a disposizione dal Garante sui diritti e doveri legati al trattamento dati, trasmessi da questo RPD.