sistemasusio
Consulenti di direzione

Comune di Induno Olona

Servizio di DPO a supporto del sistema di protezione dei dati personali (Regolamento n. 679 del 27 aprile 2016)

Proposta tecnico-economica

Milano, 7 ottobre 2022

INDICE

1. LE ESIGENZE DEGLI ENTI ALLA LUCE DEL NUOVO REGOLAMENTO

Il R**egolamento europeo sulla protezione dei dati personali**, noto anche come **GDPR** (General Data Protection Regulation), approvato nell'aprile 2016 e pienamente operativo dal **25 maggio 2018**, sta avendo un impatto su enti e imprese, non solo dal punto di vista tecnologico, ma anche e soprattutto dal punto di vista **organizzativo**.

Sono numerose le modifiche e le novità rispetto al Codice della privacy (d.lgs. n. 196/2003), anche in relazione all'evoluzione che la tecnologia di diffusione delle informazioni ha vissuto in questi ultimi anni; nel confermare come al centro restano i diritti dei cittadini sui propri dati, è necessario che enti e imprese dimostrino di avere adottato misure di sicurezza adeguate ed efficaci, frutto di una precedente analisi dei rischi, oltre a formare e addestrare chi tratta –seppur con diversi livelli di responsabilità- dati personali.

La **protezione dei dati personali**, in alcuni casi ormai relegata a sterile adempimento tecnico e burocratico diventa così, con il nuovo regolamento, sempre più un **asse strategico**; così come le imprese private, anche la pubblica amministrazione - che più delle prime tratta quotidianamente dati personali dei cittadini- ha l'obbligo di adeguarsi alle nuove prescrizioni.

Il **Comune di Induno Olona** ha in questi anni implementato tutte le prescrizioni richiesta dal Regolamento e fruito di un servizio esterno di **responsabile della protezione dei dati (DPO);** in fase di rotazione del fornitore, essendo tale servizio un obbligo per l'Ente, è stato richiesto a Sistema Susio un preventivo in merito.

In virtù della propria conoscenza del tema della protezione dei dati personali e delle specifiche esperienze in ambito pubblico (come da profilo aziendale allegato), **SistemaSusio** propone in questo documento il **servizio di responsabile della protezione dei dati (DPO)** a supporto del **monitoraggio dell'efficacia del sistema,** così da garantire e aggiornare nel tempo quanto prescritto dal Regolamento europeo.

2. L'APPROCCIO METODOLOGICO "SICURA-PA©"

L'obiettivo dell'**approccio SICURA-PA©,** sviluppato da Sistema Susio in tema di GDPR, è garantire all'Amministrazione l'ottemperanza di tutti gli obblighi e le prescrizioni previsti dal nuovo regolamento e più in generale il presidio del processo di trattamento dei dati personali, fin dalla fase di progettazione e sviluppo dei prodotti e dei servizi.

La metodologia, sviluppata **specificatamente per la Pubblica Amministrazione**, parte dalla profonda **conoscenza dei processi** degli enti pubblici che gli esperti di SistemaSusio possono garantire grazie alla pluriennale attività in progetti di analisi di riprogettazioni organizzative, di certificazione di qualità e di individuazione e gestione dei rischi.

Sempre in questi ultimi ambiti, la Società si è creata una profonda **esperienza nelle tecniche di gestione e trattamento di rischi** secondo l'approccio della **norma UNI ISO 31000: 2010**, essenziale nella gestione dei rischi di violazione dei dati personali.

Per quanto concerne la progettazione ed attuazione di misure di sicurezza preventive e tese a evitare la violazione dei dati personali, la metodologia **SICURA-PA ©** si rifà all**'approccio dei sistemi normati**, che si fonda su

- Il **principio di documentabilità delle attività svolte**, per cui, in ogni processo, le operazioni e le azioni devono essere verificabili in termini di coerenza e congruità, in modo che sia sempre attestata la responsabilità della progettazione delle attività inerenti ogni trattamento, della validazione, dell'autorizzazione, dell'effettuazione;
- Il **principio di documentabilità dei controlli**, per cui ogni attività di supervisione o controllo deve essere documentata e firmata da chi ne ha la responsabilità.

L'obiettivo, in linea con i principi di contestualizzazione del sistema e responsabilizzazione da parte dell'organizzazione esplicitati dal regolamento, è quello di individuare e priorizzare in modo metodologicamente corretto, i rischi di violazione dei dati personali e quindi aggiornare o –nei casi più gravi- riprogettare i processi al fine di garantire il rispetto dei requisiti, attraverso ad esempio la formalizzazione di sistemi di controllo, procedure, check-list e altri strumenti gestionali e informatici.

Ricordando sempre e condividendo quanto esplicitato dal Regolamento europeo sul fatto che "*La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale*" e che il fine ultimo di tali prescrizioni, per quanto onerose possano sembrare, è quello di "*contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche*."[1]

[1] Regolamento (Ue) 679 del Parlamento Europeo e del Consiglio del 27 Aprile 2016.

3. IL SERVIZIO PROPOSTO

3.1 Monitoraggio dell'osservanza delle prescrizioni e dell'efficacia del sistema

Il servizio di **DPO** è finalizzato a garantire il monitoraggio periodico sia della osservanza di quanto previsto dal Regolamento che dell'efficacia -attraverso analisi di report e statistiche e audit in loco- del sistema della protezione dei dati personali messo in atto.

SistemaSusio, proponendosi come **Responsabile della Protezione dei dati (o DPO),** mette a disposizione dell'ente propri professionisti aventi:

- approfondite competenze nell'ambito della legislazione sul trattamento dei dati personali e "privacy" in ambito pubblico;
- conoscenza approfondita del Regolamento Europeo 679/2016;
- partecipazione a master / corsi di specializzazione in tema di tutela dei dati personali
- conoscenza e familiarità con le tecnologie informatiche e le misure di sicurezza dei dati.

Saranno garantiti, per un **12 mesi dalla data di conferimento dell'incarico, i compiti previsti dal Regolamento** (art. 39) per il responsabile della protezione dei dati:

- informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- sorvegliare l'osservanza del regolamento e delle altre disposizioni relative alla protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- cooperare con l'autorità di controllo e fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Il Responsabile della Protezione dei Dati (DPO) garantirà almeno **due incontri annui in presenza (se possibile – in alternativa in videoconferenza) presso le sedi del Comune, oltre attività di back-office e gestione dei rapporti con l'autorità**, sfruttando per la condivisione dei documenti rilasciati il proprio sistema sviluppato in cloud e a norma rispetto al GDPR stesso.

3. Formazione del personale

In coerenza con l'esperienza della Società, la formazione prevista contempla **interventi di base**, da impartire a tutti i dipendenti e **interventi specialistici** per i funzionari/Responsabili del trattamento dati che sovrintendono o svolgono le attività classificate a rischio di violazione più elevato. Sarà definito e condiviso un piano di formazione il cui calendario e modalità di articolazione saranno concordati con l'Ente. All'interno di tale attività sono previsti**:**

- un **intervento formativo d'aula specialistico** di 1/2 giornata (4 h) **rivolto ai Responsabili di Settore/ Responsabili del trattamento dati dell'ente,** su aspetti specifici dell'applicazione del GDPR, che saranno desunti da una preliminare attività di **rilevazione delle esigenze** e verteranno su temi quali ad esempio le opportunità di **definire modalità operative e procedurali già in linea con i principi della privacy ("privacy by design") o le modalità di gestione delle violazioni (data breach);**
- un **modulo formativo di base d'aula** di 2 h –da reiterare due volte nella stessa mattinata (per un totale di 4 h) al fine di non creare problemi di continuità del servizio- rivolto ai **restanti dipendenti**, sui registri delle attività di trattamento, le violazioni dei dati e la loro gestione, l'impatto sull'operatività e le misure di trattamento in atto, per dare consapevolezza delle novità e garanzia che le misure siano note e compresa da tutti coloro che devono attuarle operativamente.

Al termine degli interventi formativi saranno rilasciati ai partecipanti gli attestati di frequenza.

4. I TEMPI

Per l'esecuzione del servizio in oggetto si prevedono **12 mesi continuativi**.

5. L'ORGANIZZAZIONE DEL PROGETTO

Sul progetto sarà attivato un particolare presidio della Qualità del servizio offerto, che comprende:

- individuazione dei consulenti e formatori con esperienza specifica in ambito di Pubblica Amministrazione e conoscenza del contesto degli enti locali
- monitoraggio del livello di soddisfazione del Cliente al termine del progetto
- verifica del raggiungimento degli obiettivi definiti in fase di progettazione con il Responsabile interno del progetto.

Gli esperti facenti parte del team proposto per la realizzazione delle attività sono:

- **l'Ing. Emanuele Barbagallo** -socio di Sistema Susio e esperto di GDPR e risk management in ambito pubblico, individuato come **Responsabile del progetto**

- **la dott.ssa Valentina Vasta** –collaboratrice stabile di SistemaSusio, esperta di GDPR e aspetti giuridici inerenti la privacy in ambito pubblico -proposta come **referente del DPO**
- **l'Ing**. **Giuseppe Bottasini** –associato di Sistema Susio, esperto di GDPR e sistemi informativi e sicurezza informatica in ambito pubblico.

6. IL COSTO DEL SERVIZIO

In funzione alle attività previste si prevede un **costo di 3.800,00 euro (tremilaottocento/00 euro), oltre IVA;** rispetto alle due attività contemplate nella proposta, il costo annuo risulta così suddiviso:

- **3.000,00 euro (tremila/00 euro), oltre IVA per l'attività di DPO**
- **800,00 euro (ottocento/00 euro), esente IVA per l'attività formativa.**

Qualora, come tra l'altro auspicato dal Garante stesso nel "Documento di indirizzo su designazione, posizione e compiti del Responsabile della protezione dei dati (RPD) in ambito pubblico" dell'aprile 2021, l'Ente intendesse assegnare il servizio su un orizzonte pluriennale, le cifre suindicate sono da intendersi annuali.

I costi sono comprensivi delle attività in loco, della attività svolte in remoto e dei costi di trasferimento e vitto.

Come **modalità di fatturazione**, si propongono annualmente **tre tranches** (primo acconto al termine del primo mese, secondo acconto a metà anno e saldo al termine dell'anno solare).

Lieti di poter dimostrare la validità della nostra collaborazione, ci è gradito porgere distinti saluti.

Sistema Susio srl

Bruno Susio