COMUNE DI ORIGGIO

Regolamento (UE) 2016/679 – GDPR

Politica per la protezione dei dati personali e delle informazioni, al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche

INDICE

1. **SCOPO**
2. **DESCRIZIONE**
3. **AMBITO DI APPLICAZIONE**
4. **POLITICA PER LA RISERVATEZZA E SICUREZZA DELLE INFORMAZIONI**
5. **ISTRUZIONI PER I SOGGETTI INTERNI E/O ESTERNI CHE SI INTERFACCIANO CON LA NOSTRA AMMINISTRAZIONE**
6. **RESPONSABILITÀ DELLA POLITICA DI SICUREZZA DELLE INFORMAZIONI**

1. SCOPO

Scopo del presente documento è quello di descrivere i principi generali di sicurezza ed obblighi di riservatezza delle informazioni e dei dati personali definiti dal Titolare del trattamento, o del Responsabile che garantisce ed assicura a tutti i soggetti coinvolti nell'ambito del trattamento dei dati, al fine di sviluppare un efficiente e sicuro sistema di gestione delle procedure e dei processi per la sicurezza dei dati personali nel rispetto dei diritti e le libertà fondamentali delle persone, in ottemperanza al Regolamento Europeo 2016/679, d'ora in avanti GDPR.

2. DESCRIZIONE

Obiettivi perseguiti

Il Comune intende perseguire obiettivi di sicurezza delle informazioni, dei dati personali, della struttura tecnologica, fisica, logica ed organizzativa e della loro gestione. Questo significa raggiungere e mantenere un sistema di gestione sicura delle informazioni attraverso il rispetto dei principi previsti dagli articoli 5 e 6 del GDPR;

- Liceità, correttezza, trasparenza;
- Garanzia rispetto alla gestione e raccolta dei dati per le sole finalità contrattuali, determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità. Tali garanzie sono applicate e verificate anche a cascata nei confronti degli eventuali subfornitori;
- Adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (principio di "minimizzazione dei dati");
- Esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ("esattezza");
- Conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
- Trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione,

mediante misure tecniche ed organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali "principio di integrità e riservatezza";

- Assicurare che i dati personali siano accessibili solamente ai soggetti e/o alle categorie degli stessi debitamente autorizzati;
- Salvaguardare la consistenza dell'informazione da modifiche non autorizzate;
- Assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati in riferimento ai ruoli e mansioni ricoperti;
- Assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;
- Garantire l'affidabilità dei canali di provenienza delle informazioni;
- Garantire la protezione ed il controllo dei dati personali.

Formazione

Considerato che il GDPR all'articolo 29 prevede che tutte le persone, addetti, incaricati, sotto l'autorità del titolare o del responsabile debbano essere debitamente istruiti e quindi formati sui compiti, responsabilità e per l'effettuazione delle operazioni di trattamento dei dati, nonché si impegnino alla riservatezza, l'Amministrazione redige un piano di formazione sulla base dell'erogazione dei servizi istituzionali, dei ruoli e mansioni, degli specifici trattamenti dati ed i rischi connessi.

La formazione è pensata e realizzata per le mansioni ed i ruoli ricoperti dal personale dipendente e ed ha le seguenti caratteristiche:

a) Specifica corrispondente alla tipologia di mansione/ruolo svolto;
b) Appropriata in relazione alla tipologia dei trattamenti dati realizzati;
c) Permanente deve prevedere una programmazione temporale ed un aggiornamento periodico in particolare per eventuali nuovi assunti;
d) Documentata il suo svolgimento ed i successivi aggiornamenti devono risultare da registri, attestati o altre forme che ne diano evidenza;
e) Efficace deve essere verificata periodicamente la comprensione generale, specifica ed il recepimento delle procedure

Nei confronti dei nostri fornitori:

Tali principi e garanzie sono assicurate nella determinazione dei capitolati, e dei contratti con i fornitori il cui servizio prevede il trattamento di dati personali. A tali fornitori viene richiesta l'implementazione, nel contesto degli specifici trattamenti dati, ove necessario, delle c.d. "misure minime di sicurezza ICT" per le Pubbliche Amministrazioni emanate dall'Agid. Viene inoltre monitorato sistematicamente lo stato d'implementazione di tali garanzie.

3. AMBITO D'APPLICAZIONE

La politica per la protezione dei dati personali si applica a tutto il personale interno e si condivide e richiede alle terze parti che collaborano alla condivisione e gestione delle informazioni nonché a tutti i processi e risorse coinvolte nell'erogazione dei servizi istituzionali volti alla tutela del cittadino.

4. POLITICA PER LA RISERVATEZZA E LA SICUREZZA DELLE INFORMAZIONI

Adempimenti e procedure adottate, previsti dal Regolamento UE 2016/679, per i quali si richiede l'adesione ai nostri fornitori:

- La verifica dei dati che saranno oggetto di trattamento prevede l'identificazione delle varie tipologie di dati e delle categorie di appartenenza, la verifica della finalità di ogni trattamento e della base giuridica sul quale ciascuno di essi si fonda, anche al fine di rendere un'adeguata informativa ai soggetti interessati, come previsto dagli artt. 13 e 14 del GDPR;
- La predisposizione delle informative da fornire agli interessati nel rispetto di tutti gli elementi indicati agli artt. 13 e 14 del GDPR. In particolare gli interessati dovranno essere messi a conoscenza dei diritti che il Regolamento riconosce loro (diritto di accesso, diritto all'oblio, diritto di rettifica, diritto di limitazione e di opposizione al trattamento, diritto alla portabilità dei dati); le informative per i soggetti interessati ai trattamenti dati, ove richiesto, sono fornite dal fornitore se nei software o servizi sviluppati o configurati è prevista la raccolta di dati;

- La predisposizione del registro delle attività di trattamento dei dati personali, qualora esso risulti necessario in base al disposto dell'art. 30 del GDPR, ossia nel caso in cui l'impresa o l'organizzazione che effettua il trattamento dei dati abbia più di 250 dipendenti. Tale registro dovrà essere redatto anche nel caso in cui l'impresa od organizzazione abbia meno di 250 dipendenti, ma ponga in essere un trattamento dei dati che presenta un potenziale rischio per i diritti e libertà degli interessati il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.
- L'instaurazione di una procedura da adottare in caso di eventuali violazioni dei dati (c.d. *Data Breach* di cui agli articoli 33 e 34 del GDPR), ad esempio al verificarsi di una divulgazione (intenzionale o meno), della distruzione, della perdita, della modifica o dell'accesso non autorizzato ai dati personali oggetto di trattamento. Il GDPR prevede infatti degli specifici adempimenti nel caso in cui si verifichi una violazione di tal genere, a causa di un attacco informatico, di un accesso abusivo o di un incidente. In questi casi il GDPR impone, come previsto dall'art. 33, in capo al Titolare del trattamento l'obbligo di comunicare all'autorità di controllo l'avvenuta violazione senza ritardo, e comunque entro 72 ore. Nel caso in cui la violazione faccia presumere che vi possa essere un pericolo per i diritti e le libertà degli interessati.
- All'art. 35 del GDPR, si configura, in capo al Titolare del trattamento (e con la possibilità di consultare il Responsabile della protezione dei dati), l'obbligo di procedere ad una valutazione d'impatto sulla protezione dei dati nel caso in cui un tipo di trattamento, anche in considerazione della natura, dell'oggetto, del contesto e delle finalità del trattamento stesso, presenti un rischio elevato per i diritti e le libertà delle persone fisiche. Per i dati che codesta Pubblica Amministrazione affida ad un responsabile esterno del trattamento, nella maggior parte dei casi è richiesta la collaborazione da parte del responsabile del trattamento nel procedere all'effettuazione della valutazione d'impatto anche quando sul Titolare non incombe l'obbligo normativo in tale senso.
- Agli articoli 37, 38 e 39 viene introdotto un altro adempimento richiesto al Titolare del trattamento che consiste nella designazione del Responsabile della protezione dei dati definito altresì *Data Protection Officer*. Tale nomina, come previsto dall'art. 37 del GDPR, è obbligatoria soltanto in una serie di ipotesi, in particolare, nel caso in cui il trattamento dei dati sia effettuato da un'autorità pubblica o da un organismo pubblico (ad eccezione per le autorità giurisdizionali quando esercitano le loro funzioni); quando le attività principali svolte del titolare o del responsabile del trattamento consistono in operazioni che, per la loro natura, l'ambito di applicazione o le finalità, richiedono un monitoraggio regolare e sistematico degli interessati su larga scala; e infine nel caso in cui le attività principali effettuate consistano nel trattamento, su larga scala, di dati sensibili o di dati relativi a condanne penali e a reati consistenti nell'illecito trattamento dei dati personali. Come suggerito anche dal "Gruppo dei 29", l'organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro che ha predisposto le Linee guida dettando regolare sulla nomina del Responsabile per la protezione dei dati personali, quando il Regolamento non impone specificamente la nomina di un DPO, questa figura potrà comunque essere designata dal titolare o dal responsabile del trattamento su base volontaria. Codesta Pubblica Amministrazione verifica e richiede i dati di contatto del DPO dei fornitori, ove sia designato.

5. ISTRUZIONI PER I SOGGETTI INTERNI E/O ESTERNI CHE SI INTERFACCIANO CON IL COMUNE DI ORIGGIO

Particolare importanza viene attribuita alle istruzioni e procedure della nostra politica di sicurezza della informazioni, indicate nelle istruzioni che sono fornite al personale, e nelle istruzioni contenute nelle nomine a responsabili esterni del trattamento.

6. RESPONSABILITÀ DELLA POLITICA DI SICUREZZA DELLE INFORMAZIONI

Il "titolare del trattamento" e il "responsabile" sono responsabili del sistema di gestione sicura delle informazioni, in coerenza con l'evoluzione del contesto aziendale e di mercato, valutando eventuali azioni da intraprendere a fronte di eventi come:

- Evoluzioni significative delle tecnologie dell'informazione;
- Nuove minacce rispetto a quelle considerate nell'attività di valutazione del rischio;
- Significativi incidenti di sicurezza;

- Evoluzione del contesto normativo o legislativo in materia di trattamento sicuro delle informazioni;

Periodicamente dovrà essere svolto un riesame per la verifica dell'efficienza e dell'efficacia, nonché dell'adeguatezza delle misure tecniche/organizzative applicate, nel rispetto ed al fine ultimo della protezione dei dati, diritti e libertà fondamentali delle persone.