Comune di Ronco Briantino

Regolamento per l'adeguamento al GDPR (Reg. UE 2016/679) e per l'impostazione di un Sistema per la Gestione della Privacy e della Sicurezza delle Informazioni conforme agli standard internazionali ISO 27001 e 27002

Nome documento:	Regolamento per l'adeguamento al Regolamento UE 2016/679 (GDPR) e per l'impostazione di un Sistema per la Gestione della Privacy e della Sicurezza delle informazioni conforme agli standard internazionali ISO 27001 e 27002
Codice documento:	Ronco Briantino – Reg Adeguamento GDPR Ver 1-0.doc
Nome file:	Ronco Briantino – Reg Adeguamento GDPR Ver 1-0.doc
Stato documento:	Bozza per revisione e condivisione
Versione:	1.0
Data creazione:	2 aprile 2018
Data ultimo aggiornamento	20 aprile 2018

Indice

SEZIONE 1 – PARTE GENERALE

Art. 1 - Premessa

Il regolamento europeo Reg. 2016/679 ("GDPR" – General Data Protection Regulation), in quanto regolamento e non direttiva, è immediatamente esecutivo e pertanto non necessita di alcun recepimento o approvazione.

Il presente regolamento pertanto non concerne il recepimento del GDPR, cosa che non avrebbe alcun senso ne' da un punto di vista concettuale, ne' dal punto di vista pratico.

Tuttavia, il GDPR in alcuni punti (es. art 32 – sicurezza del trattamento) enuncia delle affermazioni di principio o degli obiettivi da raggiungere, lasciando ampio margine discrezionale sulle modalità concrete attraverso le quali gli obiettivi possono venire raggiunti.

Modalità che dipendono da molteplici fattori, tra i quali le dimensioni, l'organizzazione, la cultura, le competenze e le dotazioni dell'Ente.

Il presente documento serve pertanto a individuare con precisione le modalità, le prassi, la metodologia, le tecniche e gli strumenti mediante le quali, nell'ambito specifico del Comune di Ronco Briantino, si raggiunge e si mantiene nel tempo l'adeguamento e la conformità alle prescrizioni del GDPR e si imposta un SGSI – Sistema per la Gestione della Sicurezza delle Informazioni.

Art. 2 - Obiettivo del presente Regolamento

Il presente regolamento permette di raggiungere i seguenti obiettivi:

- implementare il principio fondamentale di responsabilizzazione ("accountability") introdotto dal GDPR, in base al quale il titolare deve non solo essere conforme alle prescrizioni del GDPR, ma deve anche essere in grado di dimostrare la conformità raggiunta;
- indicare metodologie e prassi operative specifiche per l'adeguamento alle prescrizioni del GDPR, tenendo conto del contesto specifico del Comune di Ronco Briantino
- in particolare, per quanto riguarda la sicurezza (art. 32), individuare precisamente una procedura per testare, verificare periodicamente e valutare regolarmente l'efficacia delle misure tecniche ed organizzative da mettere in atto per assicurare un adeguato livello di sicurezza e di protezione dei dati
- impostare un SGSI – Sistema di Gestione della Sicurezza delle Informazioni che permetta di dimostrare che il Comune di Ronco Briantino è conforme ai requisiti di sicurezza previsti dall'art. 32 del GDPR e conforme a riconosciuti standard di sicurezza a livello internazionale.

Art. 3 - Liceità dei trattamenti

Per ciascun trattamento effettuato, deve essere verificata e documentata per iscritto la liceità del trattamento stesso; nel caso di un soggetto pubblico come il

Comune di Ronco Briantino, la liceità del trattamento deve essere individuata nella base giuridica che giustifica/richiede il trattamento specifico.

La base giuridica deve essere può essere costituita da:

- funzioni istituzionali dell'Ente, oppure
- norme di legge di rango primario.

Si dovrà inoltre verificare che non sussistano norme di legge che vietino esplicitamente il trattamento.

Art. 4 - Informativa agli interessati

Il GDPR prevede che, oltre a quanto già previsto dall'art. 13 del D.Lgs. 196/2003, l'informativa contenga le seguenti informazioni:

- i dati di contatto del responsabile della protezione dei dati
- la base giuridica del trattamento
- il tempo di conservazione dei dati personali o, se non è possibile, i criteri utilizzati per determinare tale periodo
- gli ulteriori diritti dell'interessato introdotti dal GDPR.

Art. 5 - Consenso al trattamento dei dati

Il GDPR mantiene un principio chiave introdotto dall'art. 18 del D.Lgs. 196/2003, e cioè che i soggetti pubblici non devono richiedere il consenso dell'interessato. Pertanto, sia nei moduli cartacei che nei form web, non si dovrà

chiedere il consenso dell'interessato (mentre invece è necessario fornire l'informativa).

Art. 6 - Incaricati del trattamento dei dati

Mentre il D.Lgs. 196/2003 prevedeva esplicitamente la figura dell'incaricato del trattamento dei dati, il GDPR tratta la figura dell'incaricato in termini più generali, all'art. 29 – Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento, laddove specifica che "il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso ai dati personali, non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri. Nel caso del Comune di Ronco Briantino, per chiarezza si continuerà ad usare la dicitura "Incaricato del trattamento dei dati", intendendo con tale locuzione i soggetti di cui all'art. 29 del GDPR.

Art. 7 - Responsabili del trattamento

In seno al Comune di Ronco Briantino, viene data facoltà di designare in qualità di responsabili del trattamento dei dati il titolare di articolazione organizzativa apicale, il Segretario Comunale ed il titolare dell'Unità Organizzativa che ha in carico l'innovazione tecnologica e/o la gestione dei sistemi informativi. Ciascun responsabile del trattamento dei dati sarà responsabile delle banche dati afferenti l'unità organizzativa ed i relativi trattamenti.

Art. 8 - Responsabile della protezione dei dati (DPO – Data Protection Officer)

Coerentemente con quanto previsto dall'art. 37 comma 1 lettera a) del GDPR, il Comune di Ronco Briantino dovrà designare un Responsabile della protezione dei dati (per brevità detto anche DPO – Data Protection Officer) dotato di adeguata esperienza e competenze specialistiche.

Oltre a quanto previsto dall'art. 39 del GDPR, il DPO dovrà anche collaborare alla predisposizione e al regolare aggiornamento del dei registri delle attività di trattamento.

SEZIONE 2 – SICUREZZA

Art. 9 - Obbligo di notificazione immediata di una violazione dei dati al Responsabile della protezione dei dati

Nel caso si verifichi un qualsiasi tipo di violazione dei dati, o se ne abbia anche solamente il sospetto, ne deve essere data immediata comunicazione al Segretario Comunale e al Responsabile della protezione dei dati, il quale si attiverà immediatamente per valutare se vi sia stata effettivamente una violazione, la portata e le conseguenze, e valutare se sussistano i presupposti per effettuare la notificazione entro 72 ore all'autorità di controllo.

Art. 10 - Registro delle violazioni dei dati

Coerentemente con quanto previsto dall'art. 33 comma 5, deve essere in ogni caso tenuto un registro di tutte le violazioni di dati verificatesi, a prescindere dal fatto che siano state notificate all'autorità di controllo. Il suddetto registro deve contenere come minimo le seguenti informazioni:

- data della violazione
- descrizione delle circostanze e dell'evento
- tipologia e quantità di interessati impattati
- conseguenze della violazione.

Art. 11 - Il modello MMS – Modello per il Monitoraggio della Sicurezza

La sicurezza può continuamente essere compromessa da una serie di eventi che possono accadere. Questi eventi devono pertanto essere tracciati ed essere oggetto di analisi periodica.

La tracciatura degli eventi si effettua compilando il Modello MMS – Modello per il Monitoraggio della Sicurezza, con frequenza settimanale; il modello compilato deve essere inviato al Segretario Comunale e al RESPONSABILE DELLA PROTEZIONE DEI DATI.

Art. 12 - Il modello DMS – Documento sul Monitoraggio della Sicurezza

Gli eventi di cui all'articolo precedente devono essere analizzati con frequenza almeno trimestrale, all'interno di un documento denominato MMS – Documento per il Monitoraggio della Sicurezza, predisposto dal RESPONSABILE DELLA PROTEZIONE DEI DATI e posto all'attenzione del Comitato per la Sicurezza e la Privacy. All'interno del DMS devono inoltre trovare trattazione esaustiva ed organica tutte le problematiche relative alla sicurezza e alla protezione dei dati personali che si sono verificate nel trimestre di riferimento, come ad esempio:

- l'esternalizzazione di un nuovo trattamento di dati
- la predisposizione di una procedura operativa o di un regolamento ad-hoc
- la predisposizione di una lettera di nomina
- la predisposizione di una nuova informativa
- la predisposizione di comunicazioni ai dipendenti o agli interessati
- il recepimento di norme o linee guida emesse a livello nazionale od europeo, concernenti la sicurezza o la protezione dei dati
- l'analisi di una richiesta di accesso ai dati
- la revisione dei Registri del trattamenti dei dati
- lo svolgimento di un DPIA – Data Protection Impact Assessment
- la verifica del soddisfacimento dei principi di Privacy by Design e Privacy by default all'interno di un sistema o di un processo

Art. 13 - Requisiti per il raggiungimento di un adeguato livello di sicurezza nei trattamenti effettuati

Poiché l'art. 32 del GDPR lascia un ampio margine di discrezione sulle prassi da mettere in atto per assicurare un adeguato livello di sicurezza, in fase di prima applicazione del GDPR e per un periodo di 24 mesi a far data dal 25 maggio 2018, dovranno comunque essere messe in atto le misure minime di sicurezza previste dagli artt. 33, 34 e 35 del D.Lgs. 196/2003, nei modi previsti dal Disciplinare Tecnico (Allegato B al D.Lgs. 196/2003), nonché le misure minime di sicurezza per tutte le PA previste dalla Circolare AGID 2/2017.

Parimenti, in fase di prima applicazione del GDPR e per un periodo di 24 mesi a far data dal 25 maggio 2018, si dovranno seguire le prescrizioni dell'atto di natura regolamentare adottato dall'Ente ai sensi degli artt. 20 e 21 del D.Lgs. 196/2003.

Art. 14 - Il Comitato SP – Comitato per la Sicurezza e la Privacy

Per assicurare un adeguato livello di attenzione e di potere decisionale in merito a tutte le questioni riguardanti la sicurezza e la protezione dei dati personali, deve essere costituito un Comitato per la Sicurezza e la Privacy (per brevità denominato "Comitato SP"), costituito dai seguenti membri permanenti:

- Comandante di Polizia Locale
- Sindaco
- Data Protection Officer.

Il suddetto Comitato si deve riunire con frequenza almeno trimestrale, per analizzare tutte le problematiche inerenti la sicurezza e la privacy che si sono verificate nel periodo di riferimento e analizzare tutti i modelli MMS e DMS prodotti. Alla fine di ogni riunione del Comitato deve essere prodotto un verbale delle principale decisioni prese.

Art. 15 - Dimostrazione della conformità ai requisiti di sicurezza previsti dall'art. 32 del GDPR

In caso di verifiche da parte del Garante per la protezione dei dati o della Guardia di Finanza o delle autorità preposte, il Comune di Ronco Briantino deve essere un grado di dimostrare che ha messo in atto un sistema di gestione della sicurezza tale da soddisfare i requisiti previsti dall'art. 32 del GDPR.

A tal fine è di fondamentale importanza quanto enunciato dall'art. 32 comma 3 del GDPR, laddove si specifica che l'adesione a codici di condotta approvati o ad uno scherma di certificazione può essere addotto come elemento per comprovare la conformità ed un adeguato livello di sicurezza e di protezione dei dati.

Art. 16 - Gestione della sicurezza secondo gli standard internazionali ISO 27001 e 27002

Al fine di poter dimostrare la conformità ai requisiti dell'art. 32 del GDPR – Sicurezza del trattamento, secondo il principio di responsabilizzazione ("accountability"), entro il 31-12-2018, verrà messo in atto a cura del responsabile della protezione dei dati un SGSI – Sistema per la Gestione della Sicurezza delle Informazioni conforme ai seguenti standard internazionali di sicurezza:

- ISO / IEC 27001 (norma vera e propria)
- ISO / IEC 27002 (best practice e raccomandazioni in materia di sicurezza)
- Annex-A ("Control Objectives and Controls").

Contrassegno Elettronico

TIPO CONTRASSEGNO: QR Code

IMPRONTA (SHA-256): 42e4142b0f2d1f31385d596751d411fae22efaa28cc485fdc5ac4dd64704c7c2

Firme digitali presenti nel documento originale

EMANUELA SEGHIZZI

Dati contenuti all'interno del Contrassegno Elettronico

Delibera di Consiglio N.13/2018
Data: 15/05/2018
Oggetto: REGOLAMENTO PER L'ADEGUAMENTO AL GDPR (REG. UE 2016/679) E PER L' IMPOSTAZIONE DI UN SISTEMA PER LA GESTIONE DELLA PRIVACY E DELLA SICUREZZA DELLE INFORMAZIONI CONFORME AGLI STANDARD INTERNAZIONALI ISO 27001 E 27002

Ai sensi degli articoli 23-bis e 23-ter del d.lgs.vo n. 82/2005 e s.m.i., si attesta che il presente documento, estratto in automatico dal sistema gestione documentale del COMUNE DI RONCO BRIANTINO, è conforme al documento elettronico originale, predisposto e conservato in conformità alle regole tecniche di cui all'articolo 71.

ica del Contrassegno Elettronico

URL: http://www.timbro-digitale.it/GetDocument/GDOCController?qrc=af4f32beee89b5ab_p7m&auth=1

ID: af4f32beee89b5ab