PIANO TRIENNALE PER LA PROTEZIONE DEI DATI E LA CONFORMITÀ PRIVACY

Redatto ai sensi e per gli effetti di:
Regolamento UE 2016/679 "General Data Protection Regulation"
D.Lgs.196/2003 "Codice in materia di protezione dei dati personali"

ALLEGATO ALLA **DELIBERA**
DI GIUNTA COMUNALE ~~CONSIGLIO COMUNALE~~ N° 117 del 9/8/2018

Il Segretario Comunale
Dott.ssa Rosa Regondi

INDICE

1) PREMESSA 3

2) SCOPO DEL PIANO 3

3) LA NORMATIVA DI RIFERIMENTO 4

4) LE PRIORITA' DI INTERVENTO 6

5) I SOGGETTI COINVOLTI E LA NOMINA DEL DPO 7

6) IL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO 8

7) LA GESTIONE DEGLI INCIDENTI DI SICUREZZA (DATA BREACH) 9

8) VALIDITA' ED AGGIORNAMENTO DEL PIANO 9

ALLEGATI:

- GDPR_RegolamentoAttuativo
- GDPR_NominaDPO
- GDPR_SchedeRegistroTrattamenti
- GDPR_RegistroDataBreach
- GDPR_SegnalazioneDataBreach

1) PREMESSA

La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un **diritto fondamentale**. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che **ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano**. Sulla base di tale principio l'Unione Europea ha ritenuto di emanare uno specifico Regolamento (Regolamento UE 2016/679 o General Data Protection Regulation, di seguito **GDPR**), contenente i principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali finalizzato a garantirne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza. Il GDPR è inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche.

Il 25 maggio 2018 tale regolamento diviene definitivamente operativo e direttamente applicabile in ciascuno degli Stati membri e deve essere rispettato da tutte le organizzazioni (pubbliche e private) che effettuano trattamenti di dati personali. Il GDPR introduce il "principio di accountability" (obbligo di rendicontazione) che impone alle Pubbliche Amministrazioni, titolari del trattamento dei dati:

- di adottare misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche;
- di essere in grado di dimostrare il rispetto dei principi generali previsti dal Regolamento stesso.

2) SCOPO DEL PIANO

Il presente piano si configura, insieme ai suoi allegati ed al "Regolamento Comunale per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali", quale documento programmatico ed operativo per una progressiva piena attuazione del GDPR.

SCOPO DEL REGOLAMENTO COMUNALE: Definire linee guida e misure procedimentali per una migliore funzionalità ed efficacia dell'attuazione del GDPR.
ALLEGATO: GDPR_RegolamentoAttuativo

SCOPO DEL PIANO TRIENNALE: Definire attività, tempistiche e modalità operative per garantire un'effettiva e concreta tutela delle informazioni personali trattate e del rispetto della conformità normativa.

La corretta applicazione del piano garantirà pertanto il rispetto dei principi generali previsti dal GDPR, riassunti nella seguente tabella

PRINCIPI GENERALI	DESCRIZIONE
LICEITÀ, CORRETTEZZA E TRASPARENZA (GDPR, Art.5, c.1, l.a)	Ogni trattamento di dati è legittimato da specifici requisiti, quali un consenso espresso dell'interessato, un obbligo di legge, un contratto tra le parti, un interesse legittimo del titolare. I dati sono trattati in modo corretto e trasparente nei confronti dell'interessato
FINALITÀ (GDPR, Art.5, c.1, l.b)	I dati personali sono raccolti e trattati solo per finalità predeterminate, esplicite e legittime
NECESSITÀ, NON ECCEDENZA, ESSENZIALITÀ (GDPR, Art.5, c.1, l.c)	L'utilizzo dei dati personali è sempre ridotto al minimo necessario essenziale per il raggiungimento delle finalità dichiarate; i dati personali sono raccolti e trattati solo se funzionali al raggiungimento delle finalità dichiarate; i dati personali sono trattati con modalità e strumenti proporzionali alle finalità da raggiungere
ESATTEZZA, COMPLETEZZA, AGGIORNAMENTO (GDPR, Art.5, c.1, l.d)	I dati personali sono puntualmente verificati, in modo che sia garantita la loro esattezza, completezza ed aggiornamento
CONSERVAZIONE (GDPR, Art.5, c.1, l.e)	I dati personali sono conservati per un periodo di tempo limitato al raggiungimento delle finalità dichiarate
SICUREZZA (GDPR, Art.5, c.1, l.f)	i dati sono sempre raccolti e trattati previa adozione di idonee misure di sicurezza
RISERVATEZZA (GDPR, Art.5, c.1, l.f)	i dati sono trattati da soggetti adeguatamente identificati, autorizzati ed istruiti

3) LA NORMATIVA DI RIFERIMENTO

Il presente piano è realizzato sulla base delle prescrizioni ed adempimenti previsti dal GDPR e normative comunitarie correlate.

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (**GDPR**, General Data Protection Regulation)
WEB:http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32016R0679&from=IT

NORMATIVE CORRELATE

- Articolo 8, paragrafo 1, della **Carta dei diritti fondamentali dell'Unione europea** («Carta») e Articolo 16, paragrafo 1, del **Trattato sul Funzionamento dell'Unione Europea** («TFUE»), che stabiliscono il principio generale secondo cui ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.
- Parere del Comitato economico e sociale europeo sulla proposta della Commissione (GU C 229 del 31.7.2012, pag. 90).
- Parere del Comitato delle regioni sulla proposta della Commissione (GU C 391 del 18.12.2012, pag. 127).
- Posizione del Parlamento europeo del 12 marzo 2014; posizione del Consiglio in prima lettura dell'8 aprile 2016; posizione del Parlamento europeo del 14 aprile 2016.
- Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281 del 23.11.1995, pag. 31).
- Raccomandazione della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese (C(2003) 1422) (GU L 124 del 20.5.2003, pag. 36).
- Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati (GU L 8 del 12.1.2001, pag. 1).
- Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (Cfr. pagina 89 della presente Gazzetta ufficiale).
- Direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico») (GU L 178 del 17.7.2000, pag. 1).
- Direttiva 93/13/CEE del Consiglio, del 5 aprile 1993, concernente le clausole abusive nei contratti stipulati con i consumatori (GU L 95 del 21.4.1993, pag. 29).
- Regolamento (CE) n. 1338/2008 del Parlamento europeo e del Consiglio, del 16 dicembre 2008, relativo alle statistiche comunitarie in materia di sanità pubblica e di salute e sicurezza sul luogo di lavoro (GU L 354 del 31.12.2008, pag. 70).
- Regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione (GU L 55 del 28.2.2011, pag. 13).
- Regolamento (UE) n. 1215/2012 del Parlamento europeo e del Consiglio, del 12 dicembre 2012, concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale (GU L351 del 20.12.2012, p 1).
- Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU L 201 del 31.7.2002, pag. 37).
- Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche delle regole relative ai servizi della società dell'informazione (GU L 241 del 17.9.2015, pag. 1).
- Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) n. 339/93 (GU L 218 del 13.8.2008, pag. 30).

Sul versante comunitario si è tenuto conto infine del "Corrigendum del Consiglio UE" documento del 19/04/2018 di modifica del testo originario del GDPR.

Riferimenti alla normativa nazionale, in fase di armonizzazione:

- Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali.
- Allegato B: "Disciplinare tecnico in materia di misure minime di sicurezza".

Provvedimenti e Linee guida del Garante Privacy italiano, in fase di armonizzazione:

- "Linee Guida per il trattamento di dati dei dipendenti privati" emesse il 23/11/2006;
- "Lavoro: linee guida per posta elettronica e Internet" emesse il 1° marzo 2007;
- Provvedimento in ordine all'applicabilità alle persone giuridiche del Codice in materia di protezione dei dati personali a seguito delle modifiche apportate dal d.l. n. 201/2011 emesso il 20 settembre 2012;
- Provvedimento in materia di videosorveglianza emesso l'8 aprile 2010;
- Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema emesso il 27/11/2008;
- Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali.

Provvedimenti di armonizzazione (fase attuativa nazionale)

Legge di delegazione europea (Art.13 Legge N°163 del 21/10/2017)	Prevede una delega ai singoli Governi degli Stati membri per armonizzare le prescrizioni del GDPR rispetto agli ordinamenti nazionali, con specifici riferimenti, tra gli altri, alle modalità ispettive e sanzionatore. Più nello specifico, secondo il dettato dell'art 13 nell'esercizio della delega il Governo è tenuto a: • abrogare espressamente le disposizioni del codice in materia di trattamento dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, incompatibili con le disposizioni contenute nel regolamento (UE) 2016/679; • modificare il codice 196/2003 limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel regolamento (UE) 2016/679; • coordinare le disposizioni vigenti in materia di protezione dei dati personali con le disposizioni recate dal regolamento (UE) 2016/679; • prevedere, ove opportuno, il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante per la protezione dei dati personali nell'ambito e per le finalità previsti dal regolamento (UE) 2016/679; • adeguare, nell'ambito delle modifiche al Codice di cui al decreto legislativo 30 giugno 2003, n. 196, il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del regolamento (UE) 2016/679 con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse.
Decreto attuativo della legge delega (pending)	Il decreto doveva essere adottato entro sei mesi dalla data di entrata in vigore della legge delega avvenuta il 21 novembre 2017 acquisiti i pareri delle competenti Commissioni parlamentari e del Garante per la protezione dei dati personali. Il Consiglio dei Ministri Italiano ha approvato, in esame preliminare, una bozza di decreto legislativo (in attuazione di tale legge delega) in data 21/03/2018. Tale decreto conteneva l'espressa abrogazione definitiva del Codice Privacy. Lo schema di decreto ha subito più di una stesura, ma l'ultima versione, trasmessa all'esame delle Commissioni Parlamentari, ha rivoluzionato l'approccio originario. In sostanza si prevede il **mantenimento del Codice, tramite la sua complessiva "riscrittura"**, basata sul mantenimento degli articoli compatibili con il GDPR. Il 21 maggio è scaduto il termine per l'approvazione del Decreto Attuativo, pertanto, secondo le procedure di delegazione europea tale termine si intende prorogato di 3 mesi, al 21/08/2018.

4) LE PRIORITA' DI INTERVENTO

Le tempistiche delle attività di adeguamento sono definite in relazione a:

- priorità suggerite dall'Autorità Garante attraverso apposita scheda informativa

SCHEDA INFORMATIVA
REGOLAMENTO 2016/679/UE: LE PRIORITA' PER LE PA

La principale novità introdotta dal regolamento è il principio di "responsabilizzazione" (cd. accountability), che attribuisce direttamente ai titolari del trattamento il compito di assicurare, ed essere in grado di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali (art. 5).

In quest'ottica, la nuova disciplina impone alle amministrazioni un diverso approccio nel trattamento dei dati personali, prevede nuovi adempimenti e richiede un'intensa attività di adeguamento, preliminare alla sua definitiva applicazione a partire dal 25 maggio 2018.

Al fine di fornire un primo orientamento il Garante per la protezione dei dati personali suggerisce alle Amministrazioni pubbliche di avviare, con assoluta priorità:

1. la designazione del Responsabile della protezione dei dati – RPD (artt. 37-39)
Questa nuova figura, che il regolamento richiede sia individuata in funzione delle qualità professionali e della conoscenza specialistica della normativa e della prassi in materia di protezione dati, costituisce il fulcro del processo di attuazione del principio di "responsabilizzazione". Il diretto coinvolgimento del RPD in tutte le questioni che riguardano la protezione dei dati personali, sin dalla fase transitoria, è sicuramente garanzia di qualità del risultato del processo di adeguamento in atto. In questo ambito, sono da tenere in attenta considerazione i requisiti normativi relativamente a: posizione (riferisce direttamente al vertice), indipendenza (non riceve istruzioni per quanto riguarda l'esecuzione dei compiti) e autonomia (attribuzione di risorse umane e finanziarie adeguate).

2. l'istituzione del Registro delle attività di trattamento (art. 30 e cons. 171)
Essenziale avviare quanto prima la ricognizione dei trattamenti svolti e delle loro principali caratteristiche (finalità del trattamento, descrizione delle categorie di dati e interessati, categorie di destinatari cui è prevista la comunicazione, misure di sicurezza, tempi di conservazione, e ogni altra informazione che il titolare ritenga opportuna al fine di documentare le attività di trattamento svolte) funzionale all'istituzione del registro. La ricognizione sarà l'occasione per verificare anche il rispetto dei principi fondamentali (art. 5), la liceità del trattamento (verifica dell'idoneità della base giuridica, artt. 6, 9 e 10) nonché l'opportunità dell'introduzione di misure a protezione dei dati fin dalla progettazione e per impostazione (privacy by design e by default, art. 25), in modo da assicurare, entro il 25 maggio 2018, la piena conformità dei trattamenti in corso (cons. 171).

3. la notifica delle violazioni dei dati personali (cd. data breach, art. 33 e 34)
Fondamentale appare anche, nell'attuale contesto caratterizzato da una crescente minaccia alla sicurezza dei sistemi informativi, la pronta attuazione delle nuove misure relative alle violazioni dei dati personali, tenendo in particolare considerazione i criteri di attenuazione del rischio indicati dalla disciplina e individuando quanto prima idonee procedure organizzative per dare attuazione alle nuove disposizioni.

Fonte: sito web Autorità Garante http://www.garanteprivacy.it/regolamentoue/formazione/

- priorità connesse ai requisiti di legge introdotti ex-novo dal GDPR (es: data breach), rispetto ai requisiti già presenti nel Codice e oggetto della fase di armonizzazione

In relazione alle suddette considerazioni si definiscono 4 livelli di priorità

LIVELLO 1 *(entro fase armonizzazione legge nazionale con GDPR)*	LIVELLO 2 *(a seguire termine armonizzazione)*	LIVELLO 3 *(Entro fine 2018)*	LIVELLO 4 *(Entro fine 2020)*
- Nomina DPO - Predisposizione regolamento - Predisposizione della struttura delle schede per la compilazione dei registri del trattamento - Predisposizione modulistica per data breach - Approvazione in giunta del piano e primo set documentale	- Approvazione in consiglio del regolamento - Predisposizione istruzioni agli incaricati - Avvio attività mappatura trattamenti - Analisi infrastruttura, strumenti e processi coinvolti nei trattamenti dati - Revisione format informative - Predisposizione procedura per garantire i diritti degli interessati	- Termine attività mappatura trattamenti - Compilazione completa registri trattamento - Definizione risk-assessment e piano sicurezza - Definizione piano di formazione - Revisione completa informative	- Attività di verifica ed aggiornamento - Audit su efficacia piano sicurezza - Attività di formazione - Mantenimento carica DPO - Attuazione completa sistema privacy

5) I SOGGETTI COINVOLTI E LA NOMINA DEL DPO

Il GDPR prevede l'assegnazione di ruoli gerarchici ai soggetti coinvolti nelle attività di trattamento, da declinare in relazione alle dimensioni ed alle complessità dell'Ente.

RUOLO	RIF. GDPR	IDENTIFICAZIONE
Titolare del trattamento	Art.4, c.7	Sindaco, pro-tempore
Responsabile del trattamento	Art.28	In relazione alla struttura organizzativa ed alle dimensioni dell'Ente si ritiene di non identificare soggetti interni quali Responsabili del trattamento. Tale figura (in coerenza con le specifiche del GDPR) viene assegnata ad eventuali soggetti esterni coinvolti significativamente nel trattamento di dati personali
Responsabile della protezione dei dati	Art.37	Si è ritenuto di assegnare tale carica a consulente esterno, in modo da rispettare tutti i vincoli imposti dagli art.37-39 del GDPR
Autorizzato al trattamento dei dati	Art.29	In relazione alle definizioni di dato personale e trattamento, nonché alle prescrizioni di cui all'art.29 del GDPR, si ritiene di nominare autorizzato al trattamento tutto il personale

La designazione del Data Protection Officer

La corretta gestione dei profili connessi al ruolo di Data Protection Officer (o Responsabile della protezione dei dati, DPO o RPD) prevede le seguenti attività

ATTIVITA'	STATO / PRIORITA'	NOTE
Identificazione soggetto	**IN ESSERE**	Effettuata tramite processo di selezione interna, che ha portato alla scelta della società Galli Data Service Srl (si allega offerta economica, competenze professionali e referenze soggetto, determina affidamento incarico)
Nomina soggetto	**IN ESSERE**	**Nomina avvenuta tramite decreto sindacale N°23** del 22/05/2018
Comunicazione	**IN ESSERE**	Procedura on-line da effettuarsi sul sito dell'Autorità Garante (ai sensi dell'art.37, par.7 del GDPR) https://servizi.gpdp.it/comunicazione-rpd/compilaModulo **Comunicazione effettuata in data 23/05/2018** (Rif: GPDP.Ufficio.RegistroRPD.0002454.23/05/2018)

I referenti interni privacy

Al fine di consentire al Data Protection Officer di presidiare e gestire correttamente il sistema di conformità si ritiene indispensabile identificare dei ruoli interni, prettamente operativi, di supporto:

- coordinatore interno privacy (soggetto preposto a presidiare gli eventi interni che implicano una gestione privacy, es: incidente di sicurezza, nuova attività di trattamento, ecc. e comunicarli al DPO);
- referenti di ufficio/funzione (soggetti preposti a supportare il DPO nella predisposizione del registro dei trattamenti, tramite interviste on-site e flusso informativo).

6) IL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Nel GDPR la mappatura delle attività di trattamento si colloca alla base del processo di "Responsabilizzazione", poiché fornisce un quadro aggiornato dei trattamenti in essere all'interno dell'Ente, indispensabile per ogni successiva analisi del rischio e definizione del piano di sicurezza.

- **MAPPATURA DELLE ATTIVITÀ DI TRATTAMENTO (Registro dei trattamenti)**
- **VALUTAZIONE DEL RISCHIO (Analisi dei rischi per i diritti e le libertà degli interessati)**
- **PIANO DI TRATTAMENTO DEL RISCHIO (Adozione di adeguate contromisure di sicurezza)**

La corretta gestione dei profili connessi al registro delle attività di trattamento prevede le seguenti attività

ATTIVITA'	STATO / PRIORITA'	NOTE
Valutazione DPS	**IN ESSERE**	Effettuata analisi preliminare della classificazione contenuta nell'ultimo DPS, quale elemento essenziale per una prima valutazione delle attività di trattamento e quale prima evidenza di registro
Predisposizione format di compilazione registro	FASE 1 (vedi cap.4)	Identificazione dei parametri e degli elementi da mappare, per arrivare ad una corretta classificazione del registro dei trattamenti secondo i requisiti di legge. Operativamente si ritiene opportuno: • suddividere il registro per ufficio (al fine di una capillare analisi su tutte le attività di trattamento dati effettuate nel Comune); • integrare gli elementi di cui all'art.30 con strumenti utilizzati per le attività di trattamento, primi elementi di valutazione rischio e misure sicurezza. Vedi allegato: **GDPR_SchedeRegistroTrattamenti**
Avvio compilazione del registro	FASE 2 (vedi cap.4)	Interviste on-site ai referenti di ufficio
Completamento del registro		Attività back-office DPO
Aggiornamento del registro	FASE 4 (vedi cap.4)	Tramite flusso informativo costante ed attività di audit

7) LA GESTIONE DEGLI INCIDENTI DI SICUREZZA (DATA BREACH)

IL GDPR prevede l'obbligo, per tutti i Titolari, di notificare all'autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (GDPR, considerando 85). Il Titolare deve provvedere in ogni caso a **documentare le violazioni di dati personali** subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati.

Operativamente la corretta gestione degli obblighi prevede le seguenti fasi

FASE	SOGGETTO PREPOSTO
Rilevazione incidenti	La rilevazione degli incidenti deve essere necessariamente effettuata da tutti i soggetti preposti alle attività di trattamento. La comunicazione dell'incidente verrà effettuata dal coordinatore interno al DPO
Compilazione registro	Le fasi di compilazione registro, valutazione incidente ed eventuali segnalazioni saranno gestite dal DPO
Valutazione di rischio	
Segnalazione Garante	
Segnalazione interessati	

La corretta gestione dei profili connessi al registro delle attività di trattamento prevede le seguenti attività

ATTIVITA'	STATO / PRIORITA'	NOTE
Predisposizione fasi operative per la gestione incidenti	**IN ESSERE**	Vedi tabella precedente
Predisposizione modulo "Registro data breach" e "Comunicazione data breach"	FASE 1 (vedi cap.4)	Vedi allegati: **GDPR_RegistroDataBreach** **GDPR_SegnalazioneDataBreach**
Predisposizione istruzioni operative per un corretto flusso informativo	FASE 2 (vedi cap 4)	

8) VALIDITA' ED AGGIORNAMENTO DEL PIANO

Il presente piano è soggetto all'approvazione della Giunta Comunale per avviare le attività indicate quali prioritarie (livello 1).

Al termine di ognuna delle 4 fasi operative sarà oggetto di opportune revisioni, in modo da fornire evidenze di attuazione delle fasi terminate e progettare nel dettaglio le attività della fase successiva.

Al termine del piano triennale (fine 2020) l'Ente disporrà delle necessarie informazioni per le opportune valutazioni in ordine al mantenimento del sistema di conformità privacy.