Comune di DESANA Provincia di Vercelli	**DELIBERAZIONE N. 47** Invio ai Capigruppo Consiliari con elenco N. in data

VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE

OGGETTO: procedura per la gestione delle violazioni dei dati personali (data - breach) ai sensi degli artt. 33 e ss., GDPR (Reg. UE 2016/679). Esame ed approvazione.

L'anno **duemilaventitre** il giorno **diciassette** del mese di **aprile** alle ore **17:30** nella sala delle adunanze del Consiglio Comunale, previa l'osservanza di tutte le formalità prescritte dalla vigente legge, vennero oggi convocati a seduta i componenti la Giunta Comunale.

All'appello risultano:

			Presente	Assente
1	**Luigi Ferraris**	**Sindaco**	Si	
2	**Giovanni Varalda**	**Assessore**	Si	
3	**Roberto Ferrarotti**	**Assessore**	Si	
		TOTALI	03	00

Assiste l'adunanza l'infrascritto Segretario Comunale Dott. SCAGLIA Stefano, con le funzioni previste dall'art. 97, c. 4, lett. a) del D.Lgs. n. 267/2000 – T.U.E.L.

Essendo legale il numero degli intervenuti, il Sig. FERRARIS Luigi, *SINDACO*, assume la Presidenza e dichiara aperta la seduta per la trattazione dell'oggetto sopra indicato.

IL PRESIDENTE

VISTI E RICHIAMATI :

- il Regolamento (UE) 2016/679, recante la disciplina relativa a "Protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati", che abroga la previgente direttiva 95/46 CE;

- il D.Lgs. 196/2003, recante "Codice in materia di dati personali" ;
- il D.Lgs. 101/2018, recante le modifiche al D.Lgs. 196/2003 ;
- le Linee Guida del Gruppo "Articolo 29" ;
- la "Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali" del Garante per la Protezione dei Dati Personali ;

VISTO in particolare, l'art.4, punto 12, del Regolamento UE 2016/679, che definisce la "*violazione dei dati personali*" (c.d. **data breach**) come "… *la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati* " *;*

RICHIAMATE le sottostanti definizioni di cui all'art.4, punto 12 del Regolamento UE 2016/679 :

- **distruzione** => quando i dati non esistono più, ovvero quando non esistono in una forma che sia di una qualche utilità per il titolare del trattamento ;
- **danno** =>quando i dati sono modificati, corrotti, ovvero non siano più completi;
- **perdita** => quando il titolare ha perso il controllo o l'accesso dei dati, pur se ancora esistenti, oppure quando non ne è più in possesso ;
- **trattamento non autorizzato o illecito** => quando viene effettuata una divulgazione di dati a destinatari non autorizzati, ovvero quando viene svolta una qualsiasi forma di trattamento in violazione del regolamento (UE) 2016/679 ;

CHIARITO che :

- una "*violazione dei dati personali*" è una species del genus "incidente di sicurezza" ;
- non tutti gli incidenti di sicurezza sono delle violazioni dei dati personali, mentre tutte le violazioni dei dati personali sono, automaticamente, incidenti di sicurezza;
- la conseguenza di una violazione dei dati personali è che il titolare non è più in grado di garantire l'osservanza dei principi relativi al trattamento dei dati personali ex art. 5, Regolamento (UE) 2016/679;

CONSIDERATO che, nel parere 03/2014 sulla notifica delle violazioni, il "*Gruppo di lavoro Articolo 29*" ha chiarito che le violazioni dei dati personali possono essere classificate secondo la seguente ripartizione:

- violazione della riservatezza => quando i dati vengono divulgati ovvero quando si verifica un accesso non autorizzato o accidentale;
- violazione dell'integrità => quando si verifica una modifica non autorizzata accidentale dei dati personali;
- violazione della disponibilità => quando si verificano la perdita, l'accesso o la distruzione accidentale o non autorizzata dei dati personali ;

PRESO ATTO che per fronteggiare adeguatamente una violazione dei dati personali è necessario che l'Ente intestato :

- disponga di strumenti per individuare celermente la violazione ;
- disponga di una procedura operativa consolidata ;
- individui con precisione tutti gli attori coinvolti ;
- assegni ad ogni attore compiti ben delineati ;

PRECISATO che, dopo ogni vicenda relativa ad una violazione di dati personali, il Comune di _____ deve comunque essere in grado di tracciare e registrare ogni evento ed ogni azione adottata in maniera formale ;

RITENUTO che si debba indicare puntualmente, all'interno della struttura comunale, le modalità di gestione di una violazione dei dati personali, andando a declinare nel dettaglio gli aspetti che riguardano :

- la mappa delle responsabilità ;
- il sistema di rilevazione delle violazioni dei dati personali ;
- la procedura per la gestione della violazione dei dati personali ;

PRECISATO che la mappa delle responsabilità, il sistema di rilevazione e la procedura di rilevazione confluiscono formalmente nel documento denominato registro delle violazioni, il quale può assumere forma cartacea o dematerializzata ;

DATO ATTO che la scrivente Amministrazione Comunale, con il presente atto, intende definire :

- **La mappa delle responsabilità**, la quale individua le figura chiave della gestione delle violazioni dei dati personali nel seguente modo :
    - addetti al trattamento dei dati personali => sono tutte le persone che all'interno dell'ente gestiscono i dati personali e che devono segnalare le eventuali violazioni ;
    - amministratore di sistema = è la persona che gestisce e manutiene la sovrastruttura tecnologica dell'ente in tutte le sue componenti ;
    - segretario comunale = è la persona che sovrintende alle operazioni di gestione delle violazioni ;
    - Sindaco = è il legale rappresentante del titolare del trattamento ;
    - DPO = è il responsabile della protezione dati e ha il compito di (1) informare e fornire consulenza al titolare del trattamento (2) sorvegliare l'osservanza del Reg. UE 2016/679 (3) fornire un parere sulla DPIA se richiesto (4) cooperare con il Garante dei Dati Personali (5) fungere da punto di contatto tra l'Ente ed il Garante per la Protezione dei Dati Personali;
- **Il sistema di rilevazione delle violazioni**, il quale è strutturato su di una stretta cooperazione tra addetti al trattamento dei dati personali e amministratore di sistema ed opera nel seguente modo :
    - Nel caso di rilevazione di violazione dei dati personali, ovvero si sospetto di possibile violazione, l'addetto al trattamento, ovvero l'amministratore di

sistema, inviano una e-mail al segretario comunale, facendovi poi seguire l'invio di un sms;
    - La segnalazione deve pervenire al segretario comunale entro e non oltre le 12 ore ;
    - In alcuni casi, la segnalazione della violazione potrebbe anche pervenire da soggetti esterni, come ad esempio (1) interessato (2) responsabile esterno (3) FF.PP. (4) Autorità di controllo (5) altro soggetto ;
    - A seguito della segnalazione ricevuta, il segretario comunale attiva la procedura per la gestione della violazione ;
- **La procedura di gestione delle violazioni**, la quale si articola come di seguito specificato :
    - Acquisizione della segnalazione, che prevede (1) l'acquisizione della segnalazione, (2) la segnalazione al segretario comunale (3) la segnalazione al Sindaco ;
    - Gestione tecnica della violazione, che prevede (1) la raccolta delle informazioni necessarie (2) l'analisi tecnica della violazione (3) la definizione dei soggetti coinvolti (4) l'accertamento dell'effettiva sussistenza della violazione dei dati personali, precisando che, qualora non sussistesse concretamente la violazione, la procedura si chiuderebbe in questa fase;
    - Valutazione della violazione, che prevede (1) la valutazione della natura dei dati che sono stati violati (2) della tipologia degli eventi (3) dei soggetti coinvolti ;
    - Notifica al Garante per la Protezione dei dati Personali, che rappresenta una fase eventuale, da operarsi solo in caso di verifica positiva della violazione ;
    - Segnalazione alle FF.PP. e a Cert-PA, che rappresenta una fase eventuale, da operarsi solo in caso di verifica positiva della violazione ;;
    - Comunicazione agli interessati, che rappresenta una fase eventuale, da operarsi solo in caso di verifica positiva della violazione ;;
    - Registrazione della violazione, che rappresenta una fase eventuale, da operarsi solo in caso di verifica positiva della violazione ;

RICHIAMATI gli obblighi di comunicazione ex art. 34, Regolamento (UE) 2016/679 :

DATO ATTO che i competenti uffici comunali hanno altresì predisposto i sottostanti modelli di atto, che si allegano alla presente deliberazione per farne parte integrante e sostanziale :

- modello prima segnalazione;
- modello identificazione evento;
- modello analisi evento;
- modello segnalazione interessato;
- modello di registro delle violazioni ;
- modello di guida per analisi delle violazioni ;

ATTESO che l'assunzione del presente atto non richiede la preventiva acquisizione del parere di regolarità contabile di cui all'art. 49 TUEL, non avendo il presente atto alcune riflesso, diretto od indiretto, sulla condizione economico-finanziaria dell'Ente intestato ;

RILEVATA la necessità di provvedere in merito ;

RICONOSCIUTA la propria competenza a decidere, ai sensi e per gli effetti dell'art. 48, D.Lgs. 267/2000 e ss.mm.ii. ;

VISTI :

- lo Statuto Comunale;
- il Regolamento di organizzazione degli uffici e dei servizi;
- il Codice di comportamento interno dell'Ente;
- il D.Lgs. 267/2000;
- la Legge 241/1990;
- il D.Lgs. 196/2003;
- la Legge 190/2012;
- il D.Lgs. 33/2013;
- il Regolamento (UE) n. 679/2016;
- le Dichiarazioni del gruppo di lavoro articolo 29 sulla protezione dei dati (WP29) - 14/EN;
- le Linee-guida sui responsabili della protezione dei dati (RPD) - WP243 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- le Linee-guida sul diritto alla "portabilità dei dati" - WP242 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- le Linee-guida per l'individuazione dell'autorità di controllo capofila in rapporto a uno specifico titolare o responsabile del trattamento - WP244 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- le Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 - WP248 adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017;
- le Linee guida elaborate dal Gruppo Art. 29 in materia di applicazione e definizione delle sanzioni amministrative - WP253 adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017;
- le Linee guida elaborate dal Gruppo Art. 29 in materia di processi decisionali automatizzati e pro lazione - WP251 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- le Linee guida elaborate dal Gruppo Art. 29 in materia di notifica delle violazioni di dati personali (data breach notification) - WP250 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- il Parere del WP29 sulla limitazione della finalità - 13/EN WP 203;

RICONOSCIUTA la propria competenza a decidere, ai sensi e per gli effetti dell'art.48, D.Lgs. 267/2000 e ss.mm.ii. ;

PROPONE

1 Di approvare quanto dettagliato in narrativa che, essendo parte integrante e sostanziale presente atto, ne costituisce idoneo presupposto motivazionale, ai sensi e per gli effetti dell'art. 3, L.241/1990 e ss.mm.ii. ;

2 Di dare atto che i competenti uffici comunali hanno predisposto i sottostanti modelli di atto, modulistica e registri, che si allegano alla presente deliberazione per farne parte integrante e sostanziale :

- modello prima segnalazione;
- modello identificazione evento;
- modello analisi evento;
- modello segnalazione interessato;
- modello di registro delle violazioni ;
- modello di guida per analisi delle violazioni ;

3 Di approvare i modelli di atto, modulistica e registri di cui al punto precedente ;

4 Di approvare :

5 **La mappa delle responsabilità**, la quale individua le figura chiave della gestione delle violazioni dei dati personali nel seguente modo :

a. addetti al trattamento dei dati personali => sono tutte le persone che all'interno dell'ente gestiscono i dati personali e che devono segnalare le eventuali violazioni ;
b. amministratore di sistema = è la persona che gestisce e manutiene la sovrastruttura tecnologica dell'ente in tutte le sue componenti ;
c. segretario comunale = è la persona che sovrintende alle operazioni di gestione delle violazioni ;
d. Sindaco = è il legale rappresentante del titolare del trattamento ;
e. DPO = è il responsabile della protezione dati e ha il compito di (1) informare e fornire consulenza al titolare del trattamento (2) sorvegliare l'osservanza del Reg. UE 2016/679 (3) fornire un parere sulla DPIA se richiesto (4) cooperare con il Garante dei Dati Personali (5) fungere da punto di contatto tra l'Ente ed il Garante per la Protezione dei Dati Personali;

6 **<u>Il sistema di rilevazione delle violazioni</u>**, il quale è strutturato su di una stretta cooperazione tra addetti al trattamento dei dati personali e amministratore di sistema ed opera nel seguente modo :

a. Nel caso di rilevazione di violazione dei dati personali, ovvero si sospetto di possibile violazione, l'addetto al trattamento, ovvero l'amministratore di sistema, inviano una e-mail al segretario comunale, facendovi poi seguire l'invio di un sms;
b. La segnalazione deve pervenire al segretario comunale entro e non oltre le 12 ore ;
c. In alcuni casi, la segnalazione della violazione potrebbe anche pervenire da soggetti esterni, come ad esempio (1) interessato (2) responsabile esterno (3) FF.PP. (4) Autorità di controllo (5) altro soggetto ;
d. A seguito della segnalazione ricevuta, il segretario comunale attiva la procedura per la gestione della violazione ;

7 **<u>La procedura di gestione delle violazioni</u>**, la quale si articola come di seguito specificato :

a. Acquisizione della segnalazione, che prevede (1) l'acquisizione della segnalazione, (2) la segnalazione al segretario comunale (3) la segnalazione al Sindaco ;
b. Gestione tecnica della violazione, che prevede (1) la raccolta delle informazioni necessarie (2) l'analisi tecnica della violazione (3) la definizione dei soggetti coinvolti (4) l'accertamento dell'effettiva sussistenza della violazione dei dati personali, precisando che, qualora non sussistesse concretamente la violazione, la procedura si chiuderebbe in questa fase;
c. Valutazione della violazione, che prevede (1) la valutazione della natura dei dati che sono stati violati (2) della tipologia degli eventi (3) dei soggetti coinvolti ;
d. Notifica al Garante per la Protezione dei dati Personali, che rappresenta una fase eventuale, da operarsi solo in caso di verifica positiva della violazione ;
e. Segnalazione alle FF.PP. e a Cert-PA, che rappresenta una fase eventuale, da operarsi solo in caso di verifica positiva della violazione ;;
f. Comunicazione agli interessati, che rappresenta una fase eventuale, da operarsi solo in caso di verifica positiva della violazione ;;
g. Registrazione della violazione, che rappresenta una fase eventuale, da operarsi solo in caso di verifica positiva della violazione ;

8 Di dare idonea pubblicità al presente atto all'interno dell'ente, al fin di dare notizia a tutti i dipendenti in merito alle modalità di gestione delle violazioni dei dati personali ;

9Di trasmettere copia della presente deliberazione, per l'opportuna conoscenza :

- ai responsabili del trattamento esterno ;
- agli incaricati interni del trattamento ;

10 Di pubblicare la presente deliberazione all'Albo Pretorio dell'Ente, in ossequio ai principi di trasparenza e pubblicità di cui al D.Lgs. 33/2013 e ss.mm.ii. ;

LA GIUNTA COMUNALE

Udita la relazione del Sindaco;

Esaminata la suestesa proposta di deliberazione;

Visti i pareri favorevoli dei Responsabili del servizio finanziario e del servizio gestione del personale;

Con voti unanimi FAVOREVOLI espressi palesemente

DELIBERA

Di accogliere ed approvare integralmente la proposta di deliberazione formulata dal Sindaco.

Successivamente, su proposta dello stesso Sindaco, la Giunta delibera, a voti unanimi favorevoli resi palesemente, di dichiarare la presente deliberazione immediatamente eseguibile ai sensi dell'art. 134, comma 4, del D.Lgs. n. 267/2000.

Il presente atto viene letto e sottoscritto come segue:

IL PRESIDENTE
Sig. FERRARIS Luigi

IL SEGRETARIO COMUNALE
Dott. SCAGLIA Stefano

COMUNICAZIONE AI CAPIGRUPPO CONSILIARI

(Art.125 del T.U. delle Leggi sull'ordinamento degli Enti Locali approvato con D.Lgs. 18 agosto 2000 n.267)

Si dà atto che del presente verbale viene trasmesso in elenco, oggi giorno della sua pubblicazione, ai Capigruppo Consiliari (Prot. n._____), ai sensi dell'art. 125 del T.U. delle Leggi sull'ordinamento degli Enti Locali approvato con D.Lgs. 18 agosto 2000, n.267.

Visto: IL SINDACO
Sig. FERRARIS Luigi

IL SEGRETARIO COMUNALE
Dott. SCAGLIA Stefano

REFERTO DI PUBBLICAZIONE

(Art.12, comma 1, della Legge 18 Giugno 2009 n. 69)

N._____Reg. Pubbl.

Il sottoscritto responsabile delle pubblicazioni aventi affetto di pubblicità legale, visti gli atti d'Ufficio e lo Statuto Comunale

ATTESTA

che la presente deliberazione viene pubblicata in data odierna, per rimanervi 15 giorni consecutivi nel sito web istituzionale di questo Comune accessibile al pubblico.

Desana, lì

IL MESSO COMUNALE
Stefano BESSI

CERTIFICATO DI ESECUTIVITA'

(Art.134 del T.U. delle Leggi sull'ordinamento degli Enti Locali approvato con D.Lgs. 18 agosto 2000 n.267)

Si attesta che la suestesa Deliberazione non è stata dichiarata immediatamente esecutiva dalla Giunta e che, pertanto, la stessa é divenuta esecutiva ai sensi del 4° comma dell'art. 134 del T.U. predetto, in data _____ .

Desana, lì

IL SEGRETARIO COMUNALE
Dott. SCAGLIA Stefano