COMUNE DI BORGHETTO SANTO SPIRITO

(PROVINCIA DI SAVONA)

N° **83** registro Delibere - Seduta del **17/08/2021**

Verbale di Deliberazione della **GIUNTA COMUNALE**

Oggetto: **APPROVAZIONE PROCEDURA PER LA GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH).**

L'anno duemilaventuno addì diciassette del mese di Agosto, alle ore 13:00, in Borghetto Santo Spirito, nella sede comunale, previo esaurimento delle formalità prescritte della legge, si è riunita la Giunta Comunale.

All'appello risultano i signori:

NOMINATIVO	*PRESENTE*	*ASSENTE*
CANEPA GIANCARLO	X	
ANGELUCCI LUCA	X	
CALCATERRA MARIACARLA	X	
D'ASCENZO ALESSIO	X	
LO PRESTI CARLA CELESTE	X	

TOTALE	5	0

L'assessore Lo Presti Carla Celeste partecipa alla riunione in modalità videoconferenza.

Assiste alla seduta il Segretario Comunale Federica Morabito.

Il SindacoGiancarlo Canepa, assunta la presidenza e constatata la legalità dell'adunanza, dichiara aperta la seduta e pone in discussione la proposta segnata all'ordine del giorno, che viene presa in conformità allo schema nel testo di seguito formulato sul quale - ove previsti - sono stati rilasciati preventivamente i pareri stabiliti dall'art. 49 del D.Lgs. 18.08.2000 n° 267, che sono allegati per formarne parte integrale e sostanziale del presente atto.

Oggetto: APPROVAZIONE PROCEDURA PER LA GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH).

LA GIUNTA COMUNALE

PREMESSO che:

- la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale e che 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;
- il Comune di Borghetto Santo Spirito, in quanto Titolare del trattamento, è tenuto a mantenere sicuri i dati personali trattati nell'ambito delle proprie attività istituzionali e ad agire senza ingiustificato ritardo in caso di violazione dei dati stessi (data breach), incluse eventuali notifiche all'Autorità di controllo competente ed eventuali comunicazioni agli interessati;

VISTO:

- il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo 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 (Regolamento generale sulla protezione dei dati, di seguito "Regolamento");
- il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali, così come modificato dal decreto legislativo 10 agosto 2018, n. 101, recante «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo 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» (di seguito "Codice");
- il decreto legislativo 18 maggio 2018, n. 51, recante Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione 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, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (di seguito "d.lgs. n. 51/2018");
- le "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679" (WP250) del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati Personali del 3 ottobre 2017, come modificate e adottate in ultimo il 6 febbraio 2018 e fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018;
- la Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adottata ai sensi dell'art. 64 del Regolamento, dal Comitato europeo per la protezione dei dati in data 12 marzo 2019;
- il Provvedimento del Garante sulla notifica delle violazioni dei dati personali (data breach) - 30 luglio 2019 [doc-web n. 9126951];

CONSIDERATO che:

- in caso di violazione dei dati personali, il titolare del trattamento è tenuto a notificare tale evento al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche (artt. 33 e 55 del Regolamento, art. 2-bis del Codice);
- il titolare del trattamento è tenuto altresì a notificare la violazione dei dati personali al Garante con le modalità di cui all'art. 33 del Regolamento anche con riferimento al trattamento effettuato a fini di

prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, salvo che il trattamento medesimo sia effettuato dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali, nonché di quelle giudiziarie del pubblico ministero (artt. 26 e 37, comma 6, del d.lgs. n. 51/2018);

- per «violazione dei dati personali» (data breach) si intende 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 (art. 4, punto 12 del Regolamento; art. 2, comma 1, lett. m, del d.lgs. n. 51/2018);
- per la omessa notifica di data breach all'Autorità di controllo o per l'omessa comunicazione agli interessati o per entrambi gli adempimenti, nei casi in cui siano soddisfatti i requisiti di cui agli artt. 33 e 34 GDPR, sono previste pesanti sanzioni amministrative (art. 83 GDPR), il cui importo può arrivare a 10.000.000 di euro o al 2% del fatturato totale annuo dell'esercizio precedente, se superiore, nonché le misure correttive di cui all'art. 58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati);
- inoltre, l'art. 82 prevede che chiunque subisca un danno materiale o immateriale causato da una violazione del GDPR ha il diritto di ottenere il risarcimento del danno dal soggetto al quale l'obbligo (violato) era imposto (salvo che quest'ultimo dimostri che l'evento dannoso non gli è imputabile).
- lo stesso GDPR, all'art. 83 paragrafo 2, indica dei fattori che possono mitigare o aggravare la violazione e, tra questi, un elemento che può sicuramente mitigare il livello sanzionatorio, a fronte di una violazione, è legato al comportamento del titolare che possa dimostrare come, intervenendo con tempismo, abbia fatto il possibile per ridurre la gravità, la natura e la durata della violazione. L'atteggiamento reattivo e cooperativo comporta, inoltre, sicuramente un'attenuazione delle sanzioni applicabili;

RITENUTO pertanto:

a) di fondamentale importanza predisporre una procedura organizzativa interna per la gestione di eventuali violazioni concrete, potenziali o sospette di dati personali per adempiere agli obblighi imposti dalla normativa europea ed evitare rischi per i diritti e le libertà degli interessati, nonché danni economici per l'Ente (data breach policy). A tale riguardo si precisa che, presso il Titolare, sono già state attivate procedure a tutela della sicurezza dei dati, tra cui:
    - l'adozione di misure organizzative e tecniche per garantire un livello di sicurezza adeguato al rischio connesso al trattamento dei dati personali e alle altre informazioni trattate, comprese misure volte al tempestivo ripristino della disponibilità in caso di incidente sulla sicurezza;
    - l'organizzazione di corsi di formazione per i dipendenti sui principi cardine della normativa sul trattamento dati, sulla sicurezza dei dati personali e dei sistemi;
    - la predisposizione di un sistema di protezione, mediante apposite misure tecniche (firewall, antivirus,…) dell'accesso a internet e ai dispositivi elettronici;
b) strategico per l'ente:
    - sensibilizzare il personale in ordine alle responsabilità in materia di protezione dei dati personali ed all'importanza della collaborazione nella tempestiva segnalazione e risoluzione degli incidenti sulla sicurezza (inclusi i data breach);
    - definire processi per identificare, tracciare e reagire ad un incidente sulla sicurezza e ad un data breach, per valutarne il rischio, contenere gli effetti negativi e porvi rimedio nonché stabilire se, in caso di data breach, si renda necessario procedere alla (i) notifica al Garante e (ii) comunicazione agli Interessati;
    - definire ruoli e responsabilità per la risposta agli incidenti sulla sicurezza ed i data breach;
    - assicurare un adeguato flusso comunicativo all'interno della struttura del Titolare tra le parti interessate;
    - stabilire che le procedure contemplate nell'approvando documento siano applicabili a tutte le attività svolte dal Titolare, con particolare riferimento alla gestione di tutti gli archivi e documenti cartacei e di tutti i sistemi informatici attraverso cui vengono trattati dati personali degli interessati, anche con il supporto di fornitori esterni;

- stabilire che il rispetto dell'adottanda procedura è obbligatorio per tutti i soggetti coinvolti e la mancata conformità alle regole di comportamento previste dalla stessa potrà comportare provvedimenti disciplinari a carico dei dipendenti inadempienti, ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia. In particolare le procedure medesime sono rivolte a tutti i soggetti che, a qualsiasi titolo, trattano dati personali di competenza del Titolare, quali:
    1. i lavoratori dipendenti, nonché coloro che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto contrattuale intercorrente - abbiano accesso ai dati personali trattati nel corso del prestazioni richieste per conto del Titolare del trattamento;
    2. qualsiasi soggetto (persona fisica o persona giuridica) diverso da quelli indicati alla lettera precedente che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento (art. 28 GDPR) o di autonomo Titolare. In particolare, ogniqualvolta il Titolare si trovi ad affidare il trattamento di dati ad un soggetto terzo, in qualità di responsabile del trattamento, è tenuta a stipulare con tale soggetto uno specifico contratto che lo vincoli al rispetto delle istruzioni impartitegli dal Titolare in materia di protezione dati: è necessario che la presente procedura di segnalazione di data breach sia inclusa nel suddetto contratto. Ciò al fine di obbligare il responsabile ad informare il Titolare del trattamento senza ingiustificato ritardo, di ogni potenziale evento di data breach;

RICHIAMATA la delibera della Giunta Comunale n. 134/2020 del 23/12/2020 ad Oggetto: "DIRETTIVE PER L'INNOVAZIONE DEI SERVIZI DI INFORMATIZZAZIONE, LA GESTIONE DELLA RETE E L' ADEGUAMENTO DEI LOCALI SERVER DELL'ENTE", mediante la quale si provvedeva a impartire, al servizio AFFARI GENERALI - nel quale è ricompreso anche l'ufficio CED ed innovazione tecnologica - alcune direttive inerenti il servizio di informatico dell'Ente tra le quali quella indicata al punto f) del deliberato inerente la necessità di attivare i procedimenti amministrativi per la regolamentazione delle procedure nel caso di violazione dei dati personali (data breach) richiesta dagli articoli 33 e 34 del GDPR "Regolamento Generale sulla Protezione dei Dati" (Regolamento UE 2016/679);

VISTI:

- la determinazione n. 878 del 31.08.2018 e la determinazione n. 985 del 05.10.2018 con le quali si è affidato alla ditta Si.Re. Informatica srl con sede in Novi Ligure – via Gavi n. 26 – P.IVA 01338860065, il servizio di responsabile della protezione dei dati e adempimenti di cui al Regolamento UE 679/2016, per il periodo dall'01.09.2018 al 30.08.2021;
- la designazione dell'avv. Massimo Ramello quale Responsabile della Protezione dei Dati Personali (DPO);
- la deliberazione della Giunta Comunale n. 115 del 18.11.2020 ad oggetto: nomina Responsabile della Transizione Digitale ai sensi dell'art. 17 del CAD (Codice dell'amministrazione Digitale);
- l'atto di designazione di responsabile in outsourcing del trattamento dei dati con funzioni di amministrazione di sistemi sottoscritto con la ditta SI.NET Servizi Informatici S.r.l., P.IVA e C.F. 02743730125, con sede legale in Corso Magenta 46 - 20123 Milano, in data 13.11.2020, acclarato al prot. n. 26928 del 16.11.2020;
- la relazione effettuata dalla ditta DEMETRA s.r.l. di Genova nell'ambito dell' affidamento dell'attività di audit informatico e supporto al RUP per l'affidamento del servizio di assistenza, gestione del sistema informatico e funzioni di amministratore di sistema, giusta determinazione n. 237 del 14.05.2021, in corso di espletamento;

TENUTO CONTO che con:

- deliberazioni del Consiglio comunale n. 18 del 08.02.2006 e n. 11 del 31.01.2007 è stato approvato il regolamento comunale per il trattamento dei dati sensibili e giudiziari;
- deliberazione della Giunta comunale n. 65 del 31.03.2008 è stato approvato il documento programmatico per la sicurezza del Comune di Borghetto S.Spirito;

APPURATO che:

sono stati redatti i seguenti documenti per la procedura nel caso di violazione dei dati personali (data breach) del Comune di Borghetto Santo Spirito richiesta dagli articoli 33 e 34 del GDPR "Regolamento Generale sulla Protezione dei Dati" (Regolamento UE 2016/679), predisposti dal D.P.O. congiuntamente al servizio Affari Generali, costituiti da:

- Allegato 1: Disposizioni operative in materia di incidenti di sicurezza e di violazione di dati personali;
- Allegato A: Modulo di segnalazione di una potenziale violazione di dati personali;
- Allegato B: Modulo di inoltro di segnalazione di una potenziale violazione di dati personali;
- Allegato C: Modulo di valutazione del rischio connesso alla violazione di dati personali;
- Allegato D: Modello di notifica al garante della violazione di dati personali;
- Allegato E: Comunicazione all'interessato della violazione dei dati personali;

DATO ATTO che gli stessi sono stati altresì proposti alla consultazione della ditta che attualmente svolge il servizio di gestione della rete comunale mediante assistenza informatica, assistenza sistemistica e amministratore di sistema per la verifica della correttezza e bontà della documentazione e non sono pervenute osservazioni;

VISTA la propria competenza ai sensi dell'art. 48, comma 2 e 3 - del D.Lgs. n. 267/2000;

VISTI:

- il Decreto Legislativo 18 agosto 2000, n. 267 - "TESTO UNICO DELLE LEGGI SULL' ORDINAMENTO DEGLI ENTI LOCALI";
- lo Statuto comunale;

DATO ATTO che sulla proposta di deliberazione del presente atto il responsabile del servizio dichiara l'insussistenza d'ipotesi di conflitto d'interesse a proprio carico in relazione all'art. 6 bis della legge n° 241/1990 e al PTPC del Comune di Borghetto Santo Spirito;

ACQUISITO il parere di REGOLARITÀ TECNICA espresso dal responsabile del Servizo interessato, ai sensi dell'art. 49 del D.Lgs. n. 267/2000 e ss.mm. e ii., che si allega alla presente per formarne parte integrale e sostanziale, dando atti che non necessita quello CONTABILE;

PRESO ATTO che la presente deliberazione, oltre ai pareri ex art. 49 TUEL, è corredata di n. 6 (sei) allegati, costituiti da:

- Allegato **1**: *Disposizioni operative in materia di incidenti di sicurezza e di violazione di dati personali;*
- Allegato **A**: *Modulo di segnalazione di una potenziale violazione di dati personali;*
- Allegato **B**: *Modulo di inoltro di segnalazione di una potenziale violazione di dati personali;*
- Allegato **C**: *Modulo di valutazione del rischio connesso alla violazione di dati personali;*
- Allegato **D**: *Modello di notifica al garante della violazione di dati personali;*
- Allegato **E**: *Comunicazione all'interessato della violazione dei dati personali;*

CON VOTI unanimi, favorevoli espressi nei modi di legge,

DELIBERA

1. di dare atto che la premessa fa parte integrante e sostanziale della presente proposta deliberativa, ivi compresi gli allegati, qui richiamati integralmente, e i riferimenti citati;

2. di approvare la procedura nel caso di violazione dei dati personali (data breach) del Comune di Borghetto Santo Spirito richiesta dagli articoli 33 e 34 del GDPR "Regolamento Generale sulla Protezione dei Dati" (Regolamento UE 2016/679);

3. di inviare la procedura nel caso di violazione dei dati personali (data breach) sopra indicata al:

- responsabile della Transazione Digitale;
- responsabile del Trattamento dei Dati personali – DPO, già nominato;
- ditta incaricata della gestione del servizio informatico dell'Ente ed a eventuali successivi sostituti in caso di scadenza dell'incarico o cambio prestatore di servizio;

4. di disporre che al presente provvedimento venga assicurata:
   - la pubblicità legale con pubblicazione all'Albo Pretorio;
   - la massima diffusione presso tutto il personale operante presso l'Ente e presso tutti i soggetti esterni qualificabili in termini di responsabili del trattamento;

5. la trasmissione a tutti i T.P.O. dei servizi dell'Ente per la notifica a tutte le ditte che gestiscono banche dati del Comune.

Successivamente

LA GIUNTA COMUNALE

ATTESA l'urgenza di provvedere ai successivi adempimenti al fine di utilizzare la procedura in caso di necessità stante la mancanza di regolamentazione on merito ed evitare problematiche e sanzioni;

VISTO l'art. 134, comma 4, del D.Lgs. 18.08.2000 n° 267;

DELIBERA

di dichiarare, con separata unanime, favorevole votazione la deliberazione immediatamente eseguibile.-

---

Letto, confermato e sottoscritto

IL PRESIDENTE	IL VERBALIZZANTE
Giancarlo Canepa	Federica Morabito

Atto sottoscritto digitalmente ex artt. 20 e 21 del D.Lgs. n° 82/2005 s.m.i. e norme collegate

---

La presente deliberazione è stata pubblicata nelle forme di legge all'albo pretorio del Comune, ai sensi e per gli effetti dell'art. 124, comma 1°, del D.Lgs. 18.8.2000, n. 267, come attestato dal CERTIFICATO DI PUBBLICAZIONE e CERTIFICATO DI ESECUTIVITA'.
