CASENTINO
UNIONE DEI COMUNI MONTANI

Via Roma, 203 – 52014 – Ponte a Poppi, Poppi (Ar)
unione.casentino@postacert.toscana.it
CF/P.IVA: 02095920514

DELIBERAZIONE DI GIUNTA

COPIA CONFORME

N.	84	del	20-05-2019

Presiede: SESTINI MASSIMILIANO
Assiste: dr. GRIFAGNI PAOLO

OGGETTO: **REGOLAMENTO (UE) 2016/679 DEL 27/04/2016 IN MATERIA DI PROTEZIONE DEI DATI PERSONALI E LORO LIBERA CIRCOLAZIONE DISPOSIZIONI OPERATIVE IN MATERIA DI INCIDENTI DI SICUREZZA E DI VIOLAZIONI DEI DATI PERSONALI ED ADOZIONE DEL REGISTRO DEGLI INCIDENTI DI SICUREZZA E DELLE VIOLAZIONI DEI DATI PERSONALI (DATA BREACH PAR. N. 5 ART. 33 GDPR).**

Sono presenti e assenti:

SESTINI MASSIMILIANO	**P**
CALBI VALENTINA	**P**
DUCCI ELEONORA	**A**
PANCINI LUCIANO	**P**
TELLINI GIANPAOLO	**P**
AGOSTINI PAOLO	**A**
ABBAMONDI LORENZO	**A**
PERTICHINI ROBERTO	**P**

N.	Presenti	5	Assenti	3

Il Presidente, constatato il numero legale invita i presenti alla trattazione dell'argomento in oggetto.

Soggetta a ratifica	N
Immediatamente eseguibile	S

OGGETTO: **REGOLAMENTO (UE) 2016/679 DEL 27/04/2016 IN MATERIA DI PROTEZIONE DEI DATI PERSONALI E LORO LIBERA CIRCOLAZIONE DISPOSIZIONI OPERATIVE IN MATERIA DI INCIDENTI DI SICUREZZA E DI VIOLAZIONI DEI DATI PERSONALI ED ADOZIONE DEL REGISTRO DEGLI INCIDENTI DI SICUREZZA E DELLE VIOLAZIONI DEI DATI PERSONALI (DATA BREACH PAR. N. 5 ART. 33 GDPR).**

Vista la proposta 84 del 20-05-2019

LA GIUNTA DELL'UNIONE

Premesso che:

In data 04 maggio 2016 è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il Regolamento Europeo in materia di protezione dei dati personali nonché della libera circolazione di tali dati che abroga la direttiva 95/46/CE sulla stessa materia.

Tale regolamento europeo, di seguito identificato con GDPR, è entrato in vigore il 24/05/2016 ed è divenuto definitivamente applicabile in via diretta in tutti i paesi UE a partire dal 25/05/2018.

Il gruppo di lavoro istituito in virtù dell'art. n. 29 della direttiva 95/45/CE (gruppo di lavoro indipendente con funzioni consultive dell'UE nell'ambito dalla protezione dei dati personali e della vita privata) ed al quale si fa di seguito rifermento con la sigla WP29, ha adottato il 6 febbraio 2018 la versione definitiva delle linee guida sulla notifica delle violazioni dei dati personali (cd. "Data Breach") ai sensi del Regolamento UE n. 679/2016 (GDPR).

L'art. 33 del GDPR impone al titolare del trattamento di notificare all'autorità di controllo la violazione di dati personali entro settantadue ore dal momento in cui il titolare ne viene a conoscenza.

Il termine delle settantadue ore non è perentorio, tuttavia nel caso in cui questo termine sia superato, unitamente alla notifica occorre giustificare i motivi del ritardo (art. 33 paragrafo n. 1 del GDPR).

Secondo il sopracitato articolo 33 del GDPR la notifica al garante non è necessaria quando sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche (paragrafo n. 1).

Il mancato rispetto dell'obbligo di notifica, invece, pone l'autorità di controllo nella condizione di applicare le misure correttive a sua disposizione ovvero:

- l'esercizio dei poteri previsti dall'art. 58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati) e la imposizione di sanzioni amministrative (secondo l'art. 83 GDPR, l'importo può arrivare a 10.000.000,00 di euro o al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore).

Per "*data breach*" si intende un evento in conseguenza del quale si verifica un incidente di sicurezza a seguito del quale i dati: personali, sensibili, protetti o riservati vengono: distrutti, consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato.

Un evento di "*data breach*" non è solamente un attacco o un problema informatico poiché tale violazione può riguardare anche dati conservati su supporti analogici come archivi cartacei o audiovisivi.

Il WP29 chiarisce che la conseguenza di una violazione è la perdita della capacità di garantire che il trattamento dei dati sia effettuato in conformità con i principi indicati nell'articolo n. 5 del GDPR. Questo evidenzia la differenza tra un incidente di sicurezza e una violazione dei dati personali - in sostanza, mentre tutte le violazioni dei dati personali sono incidenti di sicurezza, non tutti gli incidenti di sicurezza sono necessariamente violazioni dei dati personali.

Secondo quanto disposto al paragrafo n. 5 del citato art. n. 33 del GDPR tutti gli incidenti di sicurezza, compresi quelli per cui non sono necessarie le notifiche o quelli non qualificabili come violazioni, devono essere documentati dal Titolare ivi incluse le circostanze, le conseguenze e i provvedimenti adottati (art. 33 par. 5 del GDPR) su un apposito registro.

A tal proposito il WP29, nelle linee guida, sottolinea che il titolare del trattamento dovrà documentare tutte le violazioni che si siano verificate, indipendentemente dall'obbligo di notifica, al fine di poter dimostrare la conformità al GDPR (principio di "*accountability*").

Infatti, è' importante tenere presente che, ai sensi dell'art. 24 paragrafo n. 1 del GDPR, il titolare deve mettere in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato in conformità del regolamento europeo.

Seppure il GDPR non fornisca ulteriori indicazioni sulla forma e sul contenuto del "registro degli incidenti di sicurezza e delle violazioni" per estensione di quanto prescritto all'art. n. 30 a riguardo dei registri delle attività e delle categorie di trattamento si desume che anche il registro delle violazioni debba essere tenuto in forma scritta ed anche in formato elettronico.

Il GDPR non specifica un periodo di conservazione per tale documentazione. Qualora tali registrazioni contengano dati personali, spetta al titolare del trattamento determinare il periodo appropriato di conservazione conformemente ai principi relativi al trattamento dei dati personali e indicare la base legale per il trattamento.

La documentazione dovrà essere conservata, in conformità all'articolo 33, comma 5 del GDPR, nella misura in cui tale documentazione consenta all'Autorità di controllo di verificare il rispetto di tale articolo o, più in generale, del principio di responsabilizzazione.

La normativa nazionale dovrà essere adeguata alla normativa europea e, a tal fine, è stata approvata la Legge n. 163/2017 (entrata in vigore il 21 novembre 2017) "Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea – Legge di delegazione europea 2016-2017", in cui viene contemplato il GDPR tra i provvedimenti che lo Stato Italiano è tenuto a recepire.

L'art. 13 della Legge di delegazione europea demanda al Governo il compito di adottare i decreti legislativi per adeguare entro 6 mesi il quadro normativo nazionale al Regolamento UE 2016/679 (GDPR).

Nelle more dell'adeguamento della normativa nazionale si è comunque tenuti a dare applicazione al GDPR entro il 25.05.2018.

Ritenuto pertanto necessario provvedere a fornire agli uffici delle indicazioni operative sulle modalità di attuazione del GDPR assegnando un'alta priorità alle attività di definizione di procedure, metodologie e modelli di costituzione del registro degli incidenti e relative comunicazioni.

Con provvedimento sindacale n. 5/2018 si è provveduto a nominare il Responsabile per la Protezione dei Dati dell'ente. I dati di riferimento dell'RPD sono stati comunicati al garante in data 29.08.2018.

Considerato che i modelli che si adottano con il presente provvedimento potranno eventualmente essere sostituiti qualora:

- sulla base dell'evolversi della normativa e del pensiero in materia di protezione dei dati personali le autorità o gli organismi pubblici mettano a disposizione modelli di comunicazioni o metodologie di comunicazione che sostituiscano i modelli approvati con il presente provvedimento.
- il software gestionale di cui l'ente potrebbe dotarsi, fosse configurato in modo da produrre notifiche, segnalazioni, comunicazioni e registri utilizzando dei modelli diversi da quelli qui approvati.

Considerato altresì che:

- non è ancora chiaro il quadro giuridico di riferimento per il mancato adeguamento della normativa nazionale al GDPR e che, di conseguenza, tutti gli allegati che si approvano con la presente deliberazione potrebbero subire delle successive modificazioni;
- il Responsabile per la Protezione dei Dati personali del comune (designato con provvedimento sindacale n. 5/2018) ha provveduto ad inoltrare a questo Ente gli allegati che si approvano con il presente provvedimento, con ciò ritenendo gli stessi in linea con la normativa comunitaria.

Ritenuto comunque necessario dover fornire agli uffici precise istruzioni circa la gestione di eventuali incidenti di sicurezza per poter ottemperare alle disposizioni del GDPR nei tempi stabiliti.

Visti:

- il Regolamento Europeo 2016/679 del 27/04/2016 in materia di protezione dei dati personali nonché della libera circolazione di tali dati che abroga la direttiva 95/46/CE sulla stessa materia pubblicato in data 04/05/2016 è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea;
- l'art. 48 del D. Lgs. 18/8/2000 n. 267 e ss.mm.ii.;

Dato atto, ai sensi dell'art. 49 sopra citato, che il presente provvedimento non comporta riflessi diretti o indiretti sulla situazione economico-finanziaria o sul patrimonio dell'ente e che, pertanto, non viene acquisito il parere in ordine alla regolarità contabile;

Accertato che in fase istruttoria, sulla proposta in argomento, è stato espresso il parere favorevole di regolarità tecnica ai sensi e per gli effetti di cui all'art. 49 del Decreto Legislativo n. 267/2000, parere espresso in calce all'originale e per estratto nelle copie:

Visto il parere favorevole di regolarità tecnica e contabile, espresso ai sensi dell'art. 49, comma1, del D.Lgs 267/2000 del 18.08.2000;

Atteso che la votazione, espressa scrutinio palese, ha dato il seguente risultato:

- Presenti 05
- Votanti 05
- Voti Favorevoli 05
- Voti Contrari 00
- Astenuti 00

DELIBERA

1. di approvare ed adottare le disposizioni operative per la gestione degli incidenti di sicurezza riportate nell'allegato n. 1 al presente provvedimento: "DISPOSIZIONI OPERATIVE IN MATERIA DI INCIDENTI DI SICUREZZA E DI VIOLAZIONE DEI DATI PERSONALI (DATA BREACH) che forma parte integrante e sostanziale della presente deliberazione;
2. di approvare ed adottare il "REGISTRO DEGLI INCIDENTI DI SICUREZZA E DELLE VIOLAZIONI DI DATI PERSONALI" il cui modello è contenuto nell'allegato n. 4 al presente provvedimento e che ne forma parte integrante e sostanziale;
3. di approvare ed adottare i modelli di notifica e comunicazione nonché di informativa da rendere ai soggetti segnalatori di un incidente di sicurezza che formano parte integrante e sostanziale del presente documento e ne costituiscono gli allegati;
4. di dare atto che il registro, le disposizioni ed i modelli potranno subire modifiche nella forma e nei contenuti in seguito all'acquisizione del software gestionale di cui in premessa o in seguito dell'evoluzione della normativa e della riflessione a livello nazionale ed europeo;
5. di stabilire che il presente documento ed i suoi allegati dovranno essere comunicati a tutti i dipendenti per mezzo di posta elettronica ordinaria e resi disponibili sulle risorse di rete alle quali è consentito l'accesso in sola lettura di tutti gli utenti del sistema informatico comunale;
6. di dichiarare, il presente atto immediatamente eseguibile con il voto unanime dei presenti .

F.TO IL PRESIDENTE
SESTINI MASSIMILIANO

F.TO IL SEGRETARIO
dr. GRIFAGNI PAOLO

PUBBLICAZIONE E COMUNICAZIONE AI CAPIGRUPPO

Reg. Pubb.

La presente deliberazione:

- è stata pubblicata in data odierna nel sito istituzionale dell'Ente http://www.uc.casentino.toscana.it/albo/, ai sensi dell'art. 32, comma 1, della legge 18 giugno 2009 n. 69, per rimanervi per 15 giorni consecutivi accessibile al pubblico così come disposto dal comma 2 dell'art. 124 del D.Lgs. 18 agosto 2000 n. 267.
- è stata trasmessa in elenco ai Capigruppo consiliari con lettera prot. n. in data odierna ai sensi dell'art. 125 del D.Lgs. 18 agosto 2000 n. 267.

Poppi, lì

L'INCARICATO DELLA PUBBLICAZIONE

La presente copia cartacea composta da n. __ facciate scritte e sin qui della presente è perfettamente conforme nei contenuti all'originale informatico. L'originale è conservato presso gli archivi informatici dell'Unione dei Comuni Montani del Casentino.
Poppi, lì _____

La segreteria
Il responsabile