MONTEPULCIANO SERVIZI s.r.l.

Società a Responsabilità Limitata con unico socio

COMUNE DI MONTEPULCIANO

Verbale Amministratore Unico n. 19/2024 AF del 19/07/2024

OGGETTO: Approvazione procedura per la gestione del Data Breach

L'Amministratore Unico di Montepulciano Servizi s.r.l., Alessandro Fracassi nato a Montepulciano (SI) il 28 ottobre 1966 ed ivi residente in via di Ciliano, 1 con cod. fisc. FRCLSN66R28F592X;

VISTO:

- l'atto costitutivo a rogito Dott. Alfonso Amorosa del 18 marzo 2009 Rep. n. 9117, le successive modifiche ed integrazioni;
- che la società ha unico socio il Comune di Montepulciano;
- la deliberazione del Consiglio Comunale di Montepulciano n. 5 riunione del 18 febbraio 2019 per oggetto: SOCIETA' MONTEPULCIANO SERVIZI s.r.l. – ATTO DI INDIRIZZO;
- la delibera dell'Assemblea Ordinaria dei Soci del 24 marzo 2022 nella quale è stato nominato Amministratore Unico il Alessandro Fracassi;
- la deliberazione di Consiglio Comunale n. 87 e 90 del 29 dicembre 2022;
- il contratto di servizio stipulato tra Comune di Montepulciano e Montepulciano Servizi srl Rep. n. 4926 del 20 luglio 2023;
- il contratto di servizio stipulato tra Comune di Montepulciano e Montepulciano Servizi srl Rep. n. 4927 del 20 luglio 2023;
- l'iscrizione, dal 25 Ottobre 2019, nell'elenco delle amministrazioni aggiudicatrici e degli enti aggiudicatori che operano mediante affidamenti diretti nei confronti di proprie "società" in house, all'ID domanda n. 389 prot. 014092;
- il Decreto Legislativo n. 36/2023 "Codice dei contratti pubblici in attuazione dell'articolo 1 della legge 21 giugno 2022, n. 78, recante delega al Governo in materia di contratti pubblici";

PRESO ATTO:

- del verbale dell'Amministratore Unico n. 3/2023 "ATTO DI RICOGNIZIONE DEL RUOLO DI "TITOLARE" DEL TRATTAMENTO DEI DATI AI SENSI E PER GLI EFFETTI DEGLI ARTT. 4 E 24 DEL REGOLAMENTO UE 2016/679 (GDPR)";

- che con verbale dell'Amministratore Unico n. 18/2023 AF del 18/12/2023 "Atto ricognitivo di designazione del Responsabile della Protezione dei Dati personali (RDP) ai sensi dell'art. 37 del Regolamento UE 2016/679" è stato designato l'Avv. Flavio Corsinovi Responsabile della Protezione dei Dati / Data Protecion Officer (RPD / DPO) per la società Montepulciano Servizi s.r.l. in attuazione della deliberazione dell'Amministratore Unico n. 1 del 19/05/2018 (Atto di adesione al percorso di area vasta);

- che allo scopo di contenere i danni derivanti dalla violazione della sicurezza che comporti la perdita accidentale o l'accesso non autorizzato a dati personali si rende necessario redigere una procedura per la gestione del cosiddetto Data Breach;

- Che la redazione di tale procedura è prevista espressamente dal Regolamento Europeo 679/2016 (GDPR);

- Che la necessità di predisporre la procedura è stata rimarcata anche in sede di audit con RPD/DPO della società;

- Che pertanto è stata redatta apposita “Procedura per la gestione del Data Breach” parte integrante del presente verbale.

DETERMINA:

- di adottare la “Procedura per la gestione del Data Breach” allegata al presente verbale;

- la trasmissione del presente verbale Responsabile della Protezione dei Dati / Data Protecion Officer (RPD / DPO) della società;

- la pubblicazione nella sezione “Atti” del sito internet www.montepulcianoservizi.it del presente verbale.

L’Amministratore Unico
Alessandro Fracassi

Fracassi Alessandro
2024.07.19 09:13:06
CN=Fracassi Alessandro
C=IT
2.5.4.5=TINIT-FRCLSN66R28F592X
2.5.4.42=Alessandro
RSA/2048 bits

MONTEPULCIANO SERVIZI s.r.l.

Società a Responsabilità Limitata con unico socio

COMUNE DI MONTEPULCIANO

PROCEDURA PER LA GESTIONE DEL DATA BREACH

PREMESSA
La presente procedura definisce le attività da svolgere in caso di Data Breach, ovvero una violazione della sicurezza che comporti la perdita accidentale o l'accesso non autorizzato a dati personali. Lo scopo è quello di contenere i danni derivanti dalla violazione, tutelare i diritti degli interessati e adempiere agli obblighi previsti dal Regolamento Europeo 679/2016 (GDPR).

CAMPO DI APPLICAZIONE
La procedura si applica a tutti i trattamenti di dati personali effettuati dall'organizzazione.

DEFINIZIONI
- **Data Breach:** Violazione della sicurezza che comporti la perdita accidentale o l'accesso non autorizzato a dati personali.
- **Titolare del trattamento:** Soggetto che determina le finalità e le modalità del trattamento dei dati personali.
- **Responsabile del trattamento:** Soggetto nominato dal Titolare per trattare i dati personali per suo conto.
- **Data Protection Officer (DPO):** Figura professionale con la responsabilità di assicurare la conformità al GDPR all'interno dell'organizzazione.
- **Interessato:** Persona fisica cui si riferiscono i dati personali.

RILASCIO E REVISIONE DELLA PROCEDURA
La procedura è stata redatta in data 19 Luglio 2024 e sarà soggetta a revisione periodica o a seguito di modifiche legislative o normative.

RESPONSABILITÀ
Il Titolare del trattamento è responsabile dell'attuazione della presente procedura. Il DPO è responsabile dell'adozione delle misure necessarie per garantire la conformità al GDPR.

FASI DELLA PROCEDURA

1. Rilevamento e segnalazione del Data Breach
- Qualsiasi persona che abbia ragionevole motivo di ritenere che si sia verificato un Data Breach deve segnalarlo immediatamente al DPO o al Referente per la Privacy.
- La segnalazione deve contenere le seguenti informazioni:
  - Data e ora presunta del Data Breach;
  - Natura del Data Breach (es.: perdita di un dispositivo portatile, accesso non autorizzato a un sistema informatico);
  - Tipi di dati personali coinvolti;

- Numero stimato di interessati;
- Eventuali informazioni utili per contenere il Data Breach e per valutarne l'impatto.

2. Valutazione del rischio

- Il DPO o il Referente per la Privacy, ricevuta la segnalazione, deve immediatamente valutare il rischio per i diritti e le libertà degli interessati.
- La valutazione del rischio deve prendere in considerazione i seguenti fattori:
  - La natura dei dati personali coinvolti;
  - La sensibilità dei dati personali;
  - Le potenziali conseguenze per gli interessati (es.: furto d'identità, frodi finanziarie);
  - La probabilità che il Data Breach si verifichi nuovamente.

3. Contenimento del Data Breach

- Se il Data Breach presenta un rischio elevato per gli interessati, il DPO o il Referente per la Privacy deve adottare immediatamente le misure necessarie per contenerlo, come ad esempio:
  - Resettare le password;
  - Disattivare gli account compromessi;
  - Sospendere l'accesso ai dati personali;
  - Informare le forze dell'ordine.

4. Notifica al Garante per la protezione dei dati personali

- Il Titolare del trattamento deve notificare il Data Breach al Garante per la protezione dei dati personali entro 72 ore dalla sua scoperta, se il Data Breach presenta un rischio elevato per i diritti e le libertà degli interessati.
- La notifica deve contenere le seguenti informazioni:
  - Descrizione del Data Breach;
  - Misure adottate o che si intendono adottare per contenere il Data Breach;
  - Eventuali categorie di dati personali coinvolti;
  - Eventuali categorie di interessati coinvolti;
  - Misure di sicurezza previste per prevenire futuri Data Breach.

5. Comunicazione agli interessati

- Se il Data Breach presenta un rischio elevato per i diritti e le libertà degli interessati, il Titolare del trattamento deve comunicare il Data Breach agli interessati senza ingiustificato ritardo.
- La comunicazione deve contenere le seguenti informazioni:
  - Natura del Data Breach;
  - Misure adottate o che si intendono adottare per contenere il Data Breach;
  - Consigli pratici per gli interessati per mitigare i potenziali rischi;
  - Dati di contatto del DPO o di un altro referente per informazioni.

6. Documentazione

Tutte le attività svolte nell'ambito della gestione del Data Breach devono essere documentate.

7. Formazione

Il Titolare del trattamento deve fornire al proprio personale una formazione adeguata in materia di Data Breach, in modo che sia in grado di riconoscerli e segnalarli tempestivamente.