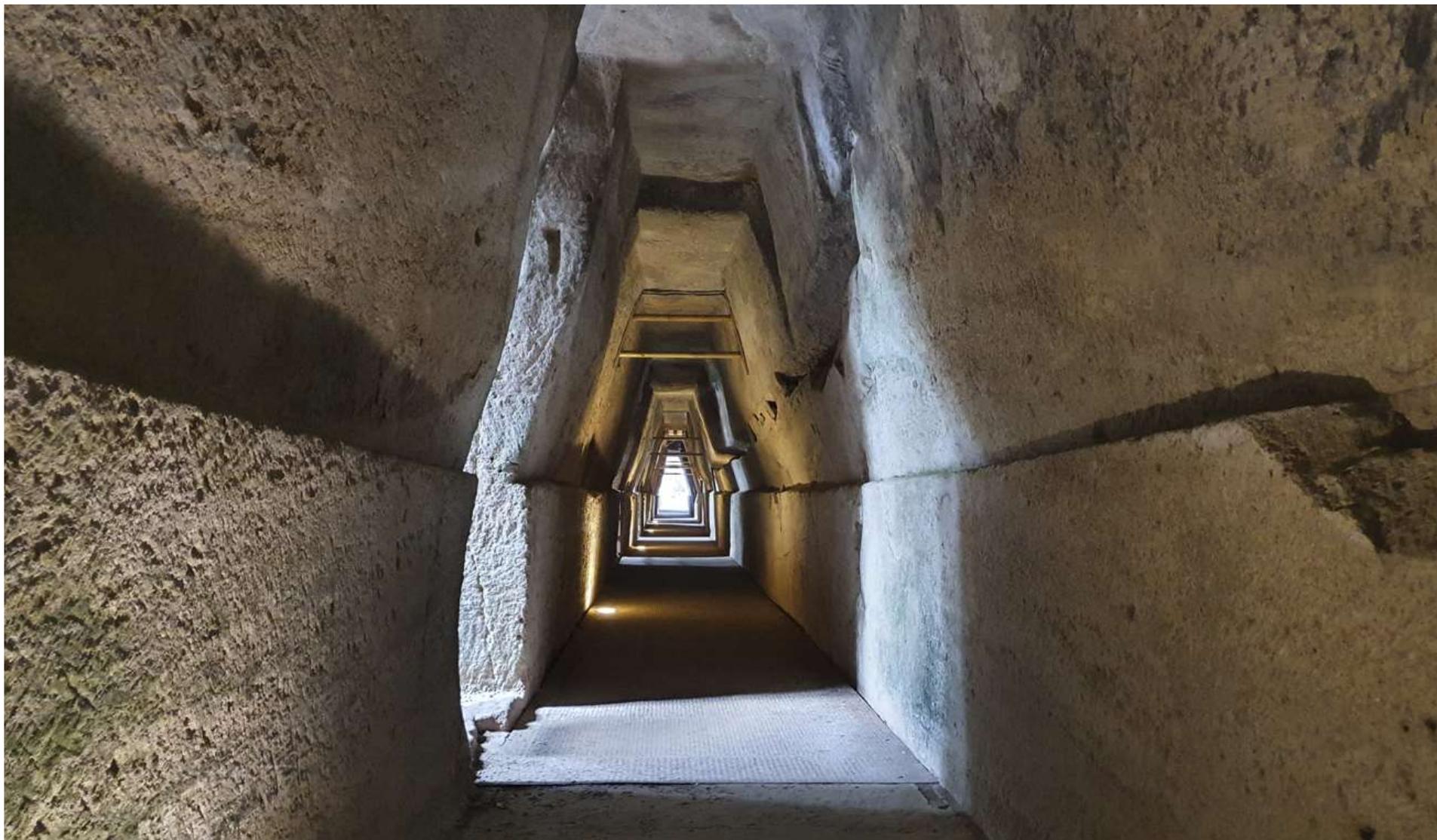


Whistleblowing (una soluzione da discutere)



Cesare Gallotti (con suggerimenti di altri Idraulici)

Milano, 27 gennaio 2024 (aggiornata dopo aver ricevuto i suggerimenti)

Nota

- Fonte primaria usata è il «Nuova disciplina “whistleblowing”: Guida operativa per gli enti privati» di Confindustria.
- Ulteriori spunti sono stati forniti da:
 - > «Modello di procedura di gestione delle segnalazioni» di www.transparency.it;
 - > «Data Privacy Impact Assessment (DPIA): Whistleblowing - Consorzio IT”.

Piattaforma

- Scelta la piattaforma Trusty: <https://trusty.report/it/>.
 - > L'email potrebbe essere un mezzo utile, se il gestore è esterno e usa un'email non controllata dall'organizzazione. Un'email interna potrebbe essere intercettata dagli amministratori di sistema.
 - > L'email, con canale non sempre cifrato, potrebbe essere vulnerabile a intercettazioni (anche se con bassa verosimiglianza). Quindi è per questo che spesso sono promosse le piattaforme.
 - > L'email è solitamente usato come canale alternativo. Se fosse il canale primario, ne andrebbe identificato un altro come alternativo (p.e. telefono).
- Dal sito Trusty è stato scaricato il «Data Processing Agreement» (Contratto di Elaborazione Dati), dove ci sono molte informazioni utili.

Nota: la questione sull'uso dell'email mi è stata posta via email da Andrea Maria Marconi.

Procedura di gestione delle segnalazioni “whistleblowing”

1. Scopo e campo di applicazione
2. Chi può segnalare violazioni (Tutele e Limite delle tutele)
3. Quali illeciti possono essere segnalati
4. Chi gestisce le segnalazioni (Gestore)
5. Procedura di gestione delle segnalazioni interne
 - > Modalità di segnalazione (canali di segnalazione)
 - > Ricezione della segnalazione
 - > Esame preliminare e valutazione di procedibilità
 - > Valutazione di ammissibilità
 - > Istruttoria e accertamento della segnalazione
 - > Esiti della segnalazione
 - > Procedimenti disciplinari
 - > Riscontro al segnalante
6. Se altri ricevono segnalazioni (oltre al gestore)
7. Segnalazioni anonime o inammissibili
8. Modalità e termini di conservazione dei dati
9. Informativa sul trattamento dei dati personali
10. Segnalazione esterna

Registro dei trattamenti

- Aggiunto il trattamento, come da informativa sulla procedura:
 - > Finalità del trattamento è la gestione delle segnalazioni di tipo whistleblowing, descritte in questo stesso documento.
 - > I dati trattati saranno di tipo personali e riguarderanno dati identificativi e di contatto.
 - Potrebbero essere trattati dati appartenenti a “categorie speciali” (es.: idonei a rivelare lo stato di salute, le opinioni politiche o l’adesione ad un sindacato) e giudiziari, se presenti nelle segnalazioni.
 - > Base legale del trattamento è il rispetto della normativa vigente e in particolare del D. Lgs. 24 del 2023.
 - Può essere richiesto il consenso per azioni successive che richiedono di fornire l’identità del segnalante (p.e. se necessaria al diritto di difesa di altri, in caso di trasmissione all’autorità).

DPIA (1/2)

1. Introduzione e ambito
2. Panoramica del trattamento
 - > Responsabilità connesse al trattamento
 - > Dati, processi e risorse di supporto
 - > Principi fondamentali
 - > Misure a tutela dei diritti degli interessati
 - > Misure tecnologiche
3. Analisi dei rischi
 - > Analisi delle misure adottate
 - > Valutazione del rischio

Ho letto tutta
l'informativa sulla
Privacy.
Alla fine lui muore!

DPIA (2/2)

- Rischi analizzati:
 - > Accesso non autorizzato
 - > Modifiche non autorizzate
 - > Perdita dei dati
 - > Trattamento non autorizzato
 - > Perdita di controllo da parte degli interessati.
- Non è stato fatto alcun calcolo. In un paragrafo finale si attesta l'efficacia delle misure adottate.
- E' stata comunque aggiornata la valutazione del rischio relativo alla protezione dei dati personali, ossia una valutazione del rischio privacy "generale" dell'organizzazione (ovviamente usando VERA!).

Comunicazioni

- Comunicazione a RSA.
- «Incarico gestore procedura whistleblowing», simile alla «nomina a incaricato», con riferimento alla procedura per l'applicazione delle misure da adottare.
- Verbale del CDA di adozione del «pacchetto».
- Distribuzione della procedura «Whistleblowing» con il Codice Etico (in discussione se accorparla, con pro e contro di fruibilità e mantenibilità).

