FNOVI – Whistleblowing e GDPR

30 novembre 2023

Ing. Giorgio Bontempi

Whistleblowing: cos’è?

Con il termine whistleblowing s’intende la rivelazione spontanea da parte di un individuo, detto “segnalante” (in inglese “whistleblower”) di un illecito o di un’irregolarità commessa all’interno dell’ente o dell’azienda, del quale lo stesso sia stato testimone nell’esercizio delle proprie funzioni.

Il segnalante spesso è un dipendente ma può anche essere una terza parte, per esempio un fornitore o un cliente.

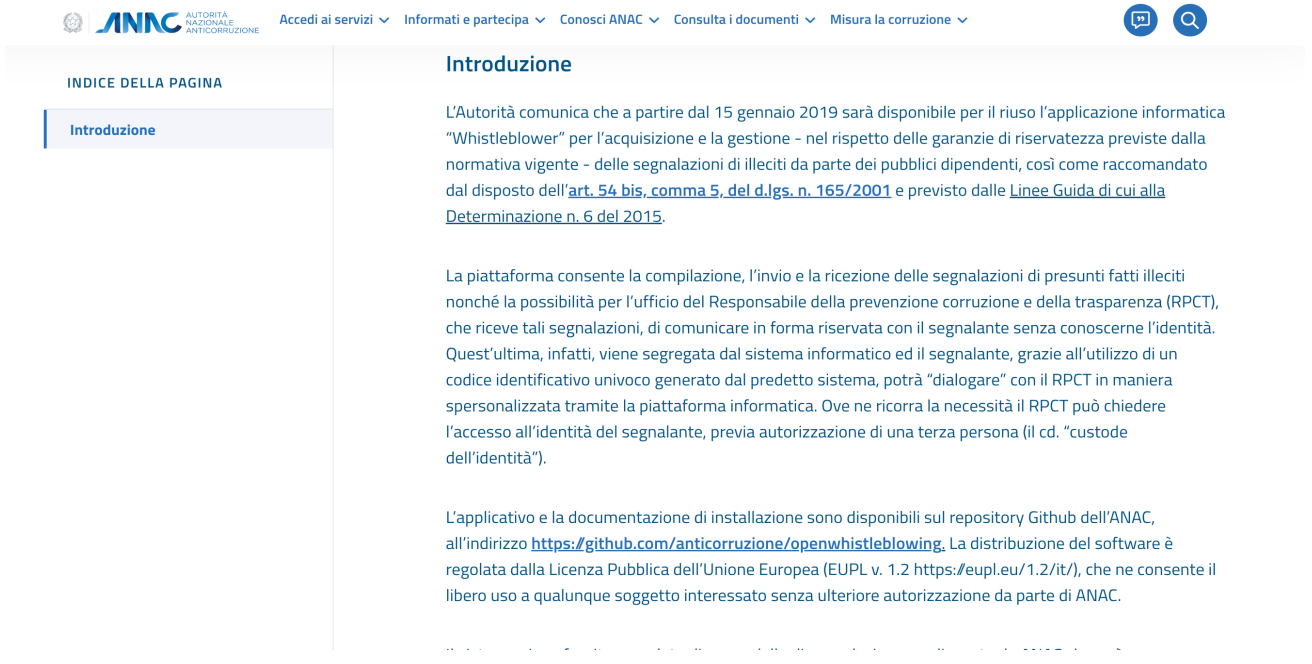
Cosa bisogna fare

Tutti i datori di lavoro devono implementare un canale interno con cui dipendenti, collaboratori o professionisti possano segnalare eventuali illeciti di cui siano venuti a conoscenza in virtù del rapporto di lavoro o collaborazione.

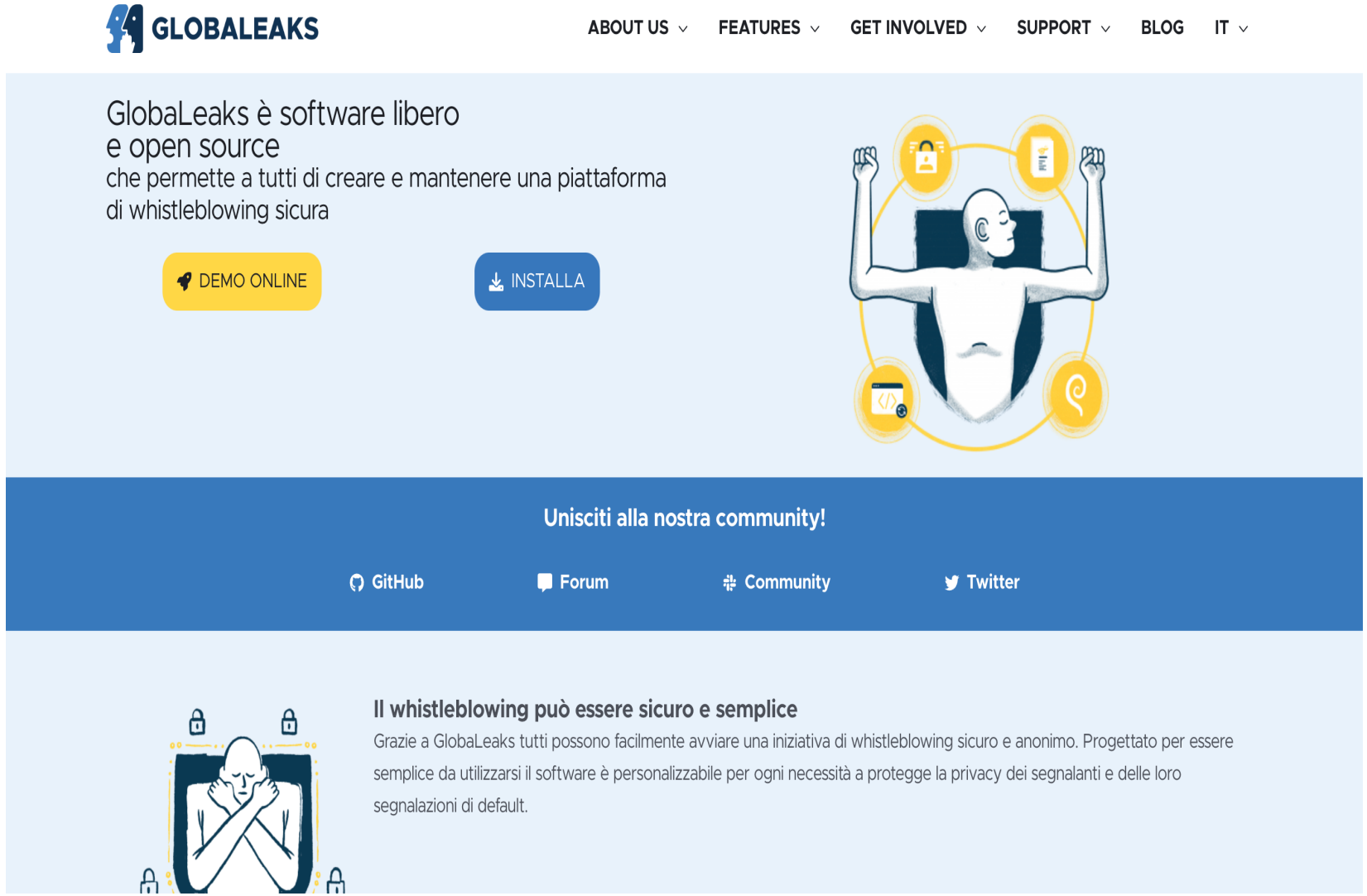
Questo canale dovrà essere gestito da un soggetto che garantisca l'anonimato e la riservatezza del segnalante.

Bisognerà adottare procedure e formare i soggetti coinvolti.

Che canale? Piattaforma web



Che canale? Piattaforma web



Che canale? Piattaforma web

https://www.whistleblowing.it/

Ma non basta

- L’informativa da conferire agli interessati;
- l’autorizzazione da rendere ai preposti al trattamento con le relative istruzioni;
- l’introduzione di una procedura organizzativa;
- l’implementazione di specifiche misure di sicurezza (specie a tutela dell’anonimato del segnalante);
- l’inquadramento del fornitore della piattaforma di segnalazione, la data retention,
- l’aggiornamento del registro dei trattamenti;
- ……..

DPIA – valutazione d'impatto privacy

L'art. 17 della Direttiva Whistleblowing – che concerne il trattamento dei dati personali – si limita ad affermare che "*Ogni trattamento dei dati personali effettuato ai sensi della presente direttiva, compresi lo scambio e la trasmissione di dati personali da parte delle autorità competenti, deve essere effettuato a norma del regolamento (UE) 2016/679 (…)*".

Il Considerando 83 precisa che, sempre in riferimento alla disciplina GDPR da applicarsi in materia, "*particolare attenzione dovrebbe essere riservata ai principi relativi al trattamento dei dati personali definiti all'articolo 5 (…) e al principio della protezione dei dati fin dalla fase di concezione e d'ufficio stabilito all'articolo 25 (…)*".

DPIA – valutazione d'impatto privacy

Negli ultimi anni il Garante ha emanato, verso specifici titolari del trattamento (e, talora, anche verso i loro responsabili), alcuni provvedimenti nei quali:

- ha invocato la necessaria esecuzione di DPIA (v. parere ad ANAC del 2019);
- o ha censurato, a seguito di istruttoria, la sua mancata esecuzione. L'omissione è stata contestata ad un soggetto pubblico (v. ordinanza avversa l'Azienda Ospedaliera di Perugia del 2022) e ad una compartecipata che, peraltro, aveva vanamente addotto rispetto al proprio trattamento l'assenza del criterio "larga scala" di cui all'art. 35, par. 1, lett. c), del GDPR (v. ordinanza avversa all'Aeroporto di Bologna del 2021).

DPIA – valutazione d'impatto privacy

Negli ultimi anni il Garante ha emanato, verso specifici titolari del trattamento (e, talora, anche verso i loro responsabili), alcuni provvedimenti nei quali:

- ha invocato la necessaria esecuzione di DPIA (v. parere ad ANAC del 2019);
- o ha censurato, a seguito di istruttoria, la sua mancata esecuzione. L'omissione è stata contestata ad un soggetto pubblico (v. ordinanza avversa l'Azienda Ospedaliera di Perugia del 2022) e ad una compartecipata che, peraltro, aveva vanamente addotto rispetto al proprio trattamento l'assenza del criterio "larga scala" di cui all'art. 35, par. 1, lett. c), del GDPR (v. ordinanza avversa all'Aeroporto di Bologna del 2021).

Precauzioni per il segnalante

Il whistleblowing è un atto coraggioso che implica il segnalare comportamenti illegali, scorretti o poco etici. Tuttavia, coloro che si impegnano in questa pratica possono essere soggetti a rischi significativi.

É importante mettere in evidenza questi rischi per garantire che i whistleblower siano consapevoli delle possibili conseguenze che potrebbero affrontare durante il processo di segnalazione.

Uno dei rischi principali è la perdita dell'anonimato.

Precauzioni per il segnalante

Proteggere la propria identità è, quindi, di fondamentale importanza.

Durante il processo di segnalazione, è necessario **prendere precauzioni** per evitare la divulgazione dell'identità.

Ciò può includere l'utilizzo di strumenti tecnologici per nascondere l'indirizzo IP o utilizzare reti VPN per creare un tunnel sicuro e garantire l'anonimato della connessione.

Precauzioni per il segnalante

Altro rischio che deve essere sottolineato è la possibile esposizione delle informazioni personali. Mentre il whistleblower cerca di raccogliere prove o documentazione per sostenere la segnalazione, potrebbe incappare in documenti sensibili o informazioni confidenziali che potrebbero danneggiare l'organizzazione coinvolta.

È fondamentale che il whistleblower protegga queste informazioni e le gestisca in modo responsabile.

Cifrare i file, evitare di condividerli con terze parti non autorizzate o memorizzarli in modo sicuro sono azioni che possono minimizzare il rischio di divulgazione accidentale o illegittima di informazioni personali o riservate.

Precauzioni per il segnalante VPN

Le prime precauzioni sono:

- Non usare dispositivi aziendali
- Compilare la segnalazione in un luogo riservato e discreto
- Utilizzare software per rendere anonima la navigazione
- Se si hanno dati personali sensibili conservarli crittografati

Precauzioni per il segnalante VPN

Una VPN, (Virtual Private Network), può offrire numerosi vantaggi in termini di anonimato e privacy durante la connessione.

1. **Anonimato:** Una VPN nasconde il tuo indirizzo IP reale e sostituisce con un indirizzo IP del server VPN. Ciò significa che la tua attività online sarà associata all'indirizzo IP del server VPN, garantendo il tuo anonimato e proteggendo la tua identità online.

2. **Protezione dati**: Utilizzando una VPN, tutti i dati che invii e ricevi dalla rete saranno crittografati. Questo rende estremamente difficile per gli hacker o le agenzie di sorveglianza intercettare i tuoi dati sensibili come password, informazioni personali o dati finanziari.

3. **Wi-Fi pubblici sicuri**: Le reti Wi-Fi pubbliche, come quelle presenti in caffetterie e aeroporti, sono spesso vulnerabili agli attacchi informatici. Utilizzando una VPN, puoi criptare la tua connessione e proteggere la tua privacy anche quando utilizzi reti Wi-Fi pubbliche non sicure.

Precauzioni per il segnalante VPN

1. Scegliere un provider di VPN affidabile e di fiducia.
2. Scaricare e installare l'app VPN.
3. Configurare l'app VPN.
4. Connettersi al server VPN: l'app stabilirà quindi il tunnel crittografato con il server VPN selezionato.
5. Utilizzare la connessione VPN: tutte le attività online saranno crittografate e rimarranno private.

Precauzioni per il segnalante VPN

Ci sono diversi siti che offrono servizi di navigazione anonima, tra cui:

Tor Browser:

(https://www.torproject.org/projects/torbrowser.html)

quando si parla di navigazione anonima non fare il nome di Tor Browser è un vero e proprio sacrilegio.

Si tratta infatti di un browser gratuito, fruibile su Windows e Mac (oltre che su Linux), che si basa su una versione modificata di Mozilla Firefox e sul sistema di navigazione libera Tor, che rende impossibile l'identificazione del PC connesso ad Internet in quanto "rimbalza" la connessione su vari computer sparsi in tutto il mondo

Precauzioni per il segnalante VPN

Hotspot Shiled

(https://www.hotspotshield.com/vpn/vpn-for-windows/)

è un programma che funge da VPN, vale a dire un sistema che fa da tramite tra il computer dell'utente e i siti (o i servizi) utilizzati, nascondendo la sua identità e proteggendo il traffico in entrata e in uscita fruibile, a costo zero (nella versione base) e disponibile per Windows e Mac

Precauzioni per il segnalante VPN

Hotspot Shiled

(https://www.hotspotshield.com/vpn/vpn-for-windows/)

è un programma che funge da VPN, vale a dire un sistema che fa da tramite tra il computer dell'utente e i siti (o i servizi) utilizzati, nascondendo la sua identità e proteggendo il traffico in entrata e in uscita fruibile, a costo zero (nella versione base) e disponibile per Windows e Mac

Precauzioni per il segnalante VPN

DotVPN

(https://chrome.google.com/webstore/detail/dotvpn-%E2%80%94-a-better-way-to/kpiecbcckbofpmkkkdibbllpinceiihk/)

Navigare anonimi in rete è cosa fattibile anche ricorrendo all'uso di apposite estensioni, disponibili per i più comuni browser Web ed in grado di fungere da VPN, come nel caso del software di cui sopra.

Tra le varie in circolazione vi segnalo DotVPN. È fruibile su Chrome, Firefox ed Opera.

Precauzioni per il segnalante VPN

- NordVPN: Offre un'ampia rete di server in tutto il mondo e una crittografia sicura per garantire la tua privacy online.
- ExpressVPN: Un altro provider VPN affidabile che garantisce una connessione sicura e anonimizzata.
- CyberGhost: Questo servizio VPN offre anche una funzione di anonimizzazione della navigazione e una vasta selezione di server.
- Surfshark: Si distingue per il suo piano di abbonamento economico e per le caratteristiche di sicurezza avanzate.

.

Precauzioni per il RPCT

- Consultare le segnalazioni in un luogo riservato
- Non copiare o tenere informazioni al di fuori della piattaforma telematica
- Non tenere appunti o alto in luoghi accessibili e non controllabili
- In caso di colloquio il verbale dello stesso o la sua registrazione deve essere crittografata e conservata in un posto il più sicuro possibile

Precauzioni per il RPCT Crittografia

Che programmi per crittografare i file:

- VeraCrypt (https://www.veracrypt.fr/en/Home.html)
  - Ottimo per la crittografia nascosta.
- BitLocker (https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/
- 7Zip (https://www.7-zip.org/): comprime e crittografa i dati

Grazie per l’attenzione