Comune di Cembra Lisignago

PIAZZA MARCONI, 7 - 38034 CEMBRA LISIGNAGO (TN)
C.F./P.IVA 02401950221
☎ 0461/683018 - 0461/683583
Sito www.comune.cembralisignago.tn.it
Email protocollo@comune.cembralisignago.tn.it
Pec comune@pec.comune.cembralisignago.tn.it

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI ART. 35 REG UE 16/679

LA PRESENTE VALUTAZIONE DI IMPATTO CONCERNE IL SEGUENTE TRATTAMENTO:

Trattamenti effettuati nell'ambito della gestione delle segnalazioni di condotte illecite (c.d. whistleblowing).

La presente valutazione di impatto tiene in considerazione il seguente modello organizzativo:

PREMESSA

La Valutazione d'Impatto sulla Protezione dei Dati (di seguito "DPIA) è un processo che il Titolare del trattamento deve effettuare, in via preventiva, ogni qual volta un trattamento di dati personali, in particolare connesso all'impiego di nuove tecnologie, in considerazione della natura, dell'oggetto, del contesto e delle finalità del trattamento, possa presentare un rischio elevato peri diritti e le libertà delle persone.

Il processo di DPIA è ritenuto uno degli aspetti di maggiore rilevanza nel nuovo quadro normativo definito dal Regolamento Generale sulla Protezione dei Dati (Regolamento UE 2016/679), in quanto esprime chiaramente la responsabilizzazione (c.d. accountability) del titolare nei confronti dei trattamenti dallo stesso effettuati.

Il Titolare del trattamento, infatti, è tenuto non solo a garantire l'osservanza delle disposizioni regolamentari, quanto anche a dimostrare adeguatamente in che modo egli garantisca tale osservanza.

VALUTAZIONE DELLE POTENZIALI CONSEGUENZE DERIVANTI DALLA MANCATA ADOZIONE DI ADEGUATE MISURE DI SICUREZZA

Il trattamento oggetto di questa valutazione di impatto potrebbe essere soggetto ai seguenti rischi per i diritti e le libertà degli interessati sopra individuati:

ELENCAZIONE DEI RISCHI POTENZIALMENTE INCOMBENTI SUL TRATTAMENTO SOPRA DESCRITTO	SI	TENORE DEL RISCHIO: 1 MOLTO BASSO 2 BASSO 3 MEDIO 4 ALTO 5 MOLTO ALTO	NO
lesione della dignità dell'interessato (ad es. pregiudizio alla reputazione)	x	4	
rischio discriminazione dell'interessato	x	2	
rischio furto o usurpazione dell'identità dell'interessato	x	3	
danno economico per l'interessato	x	4	
VALUTAZIONE DEL COMPLESSIVO LIVELLO DI RISCHIO CONNESSO AL TRATTAMENTO SVOLTO		13	

DESCRIZIONE DELLA PIATTAFORMA WHISTLEBLOWING

Whistleblowing Solutions, in qualità di responsabile del trattamento per conto della scrivente amministrazione, titolare del trattamento, è affidataria della gestione del sistema di whistleblowing per l'esecuzione di operazioni informatizzate di trattamento.

L'architettura del sistema in uso è composta da:

- Un cluster di due firewall perimetrali;
- Un cluster di due server fisici dedicati;
- Una Storage Area Network pienamente ridondata.

La piattaforma informatica di segnalazione è basata sul software libero ed open-source **GlobaLeafis** di cui Whistleblowing Solutions è co-autore e coordinatore di progetto.
In aggiunta a GlobaLeaks, utilizzato in via principale per l'implementazione del servizio, per finalità di pubblicazione, documentazione e supporto del progetto vengono utilizzate altre tecnologie a codice aperto e di pubblico dominio la cui qualità è indipendentemente verificabile. Vengono anche in modo limitato utilizzate alcune note tecnologie proprietarie e licenziate necessarie per finalità di gestione infrastrutturale e backup professionale.

Vengono primariamente utilizzati le tecnologie open source:

- Debian/Linux (principale sistema operativo utilizzato);
- Postfix (mail server);
- Bind9 (dns server);
- OPNSense (firewall);
- OpenVPN (vpn).

Le componenti software di natura proprietaria impiegate sono le seguenti:

- VMware, software di virtualizzazione;
- Veeam, software di backup;
- Plesk, software per realizzazione siti web di facciata del progetto.

Predisposizione dei sistemi virtualizzati:

- i server eseguono software VMware e vCenter abilitando funzionalità di High Availability;
- su VMware vengono istanziate macchine virtuali Debian/Linux nelle sole version Long Term Support (LTS);
- ogni macchina virtuale Debian implementa configurazione securizzata con: Full Disk Encryption (lvm/crypto), SecureBoot, Apparmor, Iptables;
- entrambi i server fisici eseguono una macchina virtuale di Key Management System (KMS) per consentire continuità di servizio con immediato automatico riavvio dei sistemi senza intervento amministrativo anche in caso di totale fallimento di uno dei due server fisici componenti il cluster.

ARCHITETTURA DI RETE

- l'architettura di rete prevede un firewall perimetrale e segregazione della rete in molteplici VLAN al fine di isolare le differenti componenti secondo loro differente natura al fine di limitare ogni esposizione in caso di vulnerabilità su una singola componente;
- una VPN consente l'accesso alla gestione dell'infrastruttura a un limitato e definito insieme di amministratori di sistema;
- ogni connessione di rete implementa TLS 1.2;
- ogni macchina virtuale istanziata vede esposizione di rete limitata all'effettiva necessità;

- tutti i dispositivi utilizzati quali l'applicativo GlobaLeaks, Log di sistema e Firewall sono configurati per non registrare alcun tipo di log e/o informazioni lesive della privacy e dell'anonimato del segnalante quali per esempio indirizzi IP e User Agents;
- l'applicativo GlobaLeaks abilita la possibilità di navigazione tramite Tor Browser per finalità accesso anonimo con garanzie al passo con lo stato dell'arte della ricerca tecnologica in materia.
-

DESCRIZIONE E ANALISI DEL CONTESTO DEL TRATTAMENTO

Responsabilità connesse al trattamento:	**APSP** > Titolare del trattamento **Whistleblowing Solutions** > Responsabile del trattamento per la fornitura e la gestione del sistema di whistleblowing **Seeweb** > Sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per la gestione dell'infrastruttura (IaaS) **Transaparency International Italia** > Sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per la collaborazione nella gestione del sistema di whistleblowing
Standard applicabili:	ISO27001"Erogazione di Servizi SaaS diWhistleblowing Digitale su base GlobaLeaks" ISO27017 controlli di sicurezza sulle informazioni basati sulla per i servizi Cloud ISO27018 per la protezione dei dati personali neiservizi Public Cloud Qualifica AGID Certificazione CSA Star
Dati e operazioni di trattamento:	Operazioni informatizzate di trattamento di dati personali relative alla raccolta e conservazione dei dati necessari per l'erogazione dei servizi in modalità SaaS. **Dati di registrazione** Dati identificativi e di contatto dei referenti del Titolare che attivano il servizio di digital whistleblowing (es. ResponsabileAnticorruzione). **Categorie particolari di dati** Dati eventualmente contenuti nelle segnalazioni e in atti e documenti ad essa allegati. **Dati relativi a condanne penali e reati** Dati eventualmente contenuti nella segnalazione e in atti e documenti ad essa allegati.

Ciclo di vita del trattamento e dei dati	Attivazione della piattaforma Configurazione della piattaforma Fase d'uso della piattaforma con caricamento delle segnalazioni da parte dei segnalanti e accesso alle stesseda parte dei riceventi preposti Fase di dismissione della piattaforma al termine del contratto e alla scadenza degli obblighi di legge per finalità amministrative e contabili con conseguente cancellazione sicura dei dati da parte del fornitore
Risorse a supporto delle attività di trattamento	Software di whistleblowing professionale GlobaLeaks Infrastruttura IaaS e SaaS privata basata su tecnologie: Risorse a supporto Delle attività di trattamento: - Dettaglio Hardware - VMWARE (virtualizzazione) - Debian Linux LTS (sistema operativo) - VEEAM (backup) - OPNSENSE (firewall) - OPENVPN (vpn)

VALUTAZIONI IN MERITO AL TRATTAMENTO

Adeguatezza, pertinenza e limitazione a quanto è necessario in relazione alle finalità per le quali i dati sono trattati (minimizzazione)	Per la registrazione e attivazione del servizio sono richiesti unicamente i seguenti dati: nome, cognome, telefono, e-mail, ruolo dell'utente che effettua la registrazione e i dati relativi all'ente (nome, indirizzo, CF e PI). Il software di whistleblowing raccoglie segnalazioni secondo i migliori questionari predisposti in ambito di whistleblowing in collaborazione con importanti enti di ricerca in materia di whistleblowing e anticorruzione e messi a punto da Transparency International Italia in relazione alla normativa vigente in materia. Nel rispetto del principio di privacy by design tutti i dispositivi utilizzati quali applicativo GlobaLeaks, log di sistema e firewall sono configurati per non registrare alcun tipo di log di informazioni lesive della privacy e dell'anonimato del segnalante, quali per esempio indirizzi IP, User Agents e altri Metadata. L'applicativo GlobaLeaks vede abilitata la possibilità di navigazione tramite Tor Browser per finalità accesso anonimo con garanzie al passo con lo stato dell'arte della ricerca tecnologica in materia.
Esattezza e aggiornamento dei dati	L'aggiornamento dei dati è a cura degli utenti stessi che si sono registrati attraverso l'accesso alla propria area riservata. Non appena vengono modificati i dati di contatto all'interno della piattaforma, questi diventano i dati di contatto ufficiali a cui sono inviate le comunicazioni relative a ogni tipo di aggiornamento.
Periodo di conservazione dei dati	Policy di data retention di default delle segnalazioni di 18 mesi, prorogabili al doppio sulle singole segnalazioni per

	scelta precisa del soggetto ricevente, con cancellazione automatica sicura delle segnalazioni scadute. Cancellazione della piattaforma 15 giorni dopo la disattivazione del servizio.
Protezione in caso di trasferimento di dati al di fuori dell'Unione europea:	I Dati Personali sono trattati principalmente in Italia ed esclusivamente nei Paesi dell'Unione Europea. Non esiste alcun trasferimento di Dati Personali in paesi extra UE.

MISURE DI SICUREZZA

CRITTOGRAFIA
L'applicativo GlobaLeaks implementa uno specifico protocollo crittografico realizzato per applicazioni di whistleblowing in collaborazione con l'Open Technology Fund di Washington.
Ogni informazione scambiata viene protetta in transito da protocollo TLS 1.2 con SSLLabs rating A. Ogni informazione circa le segnalazioni e i relativi metadati registrata dal sistema viene protetta con chiave asimmetrica personale e protocollo a curve ellittiche per ciascun utente avente accesso al sistema e ai dati delle segnalazioni. Nessun dato viene salvato in chiaro su supporto fisico in nessuna delle fasi di caricamento. Il sistema è installato su sistema operativo Linux su cui è attiva Full Disk Encryption FDE a garanzia di maggiore tutela dei sistemi integralmente cifrati in condizione di fermo e in condizione di backup remoto. Protocollo crittografico: https://docs.globaleaks.org/en/main/security/EncryptionProtocol.html

CONTROLLO DEGLI ACCESSI LOGICI
L'accesso applicativo è consentito ad ogni utilizzatore autorizzato tramite credenziali di autenticazione personali. Il sistema implementa policy password sicura e vieta il riutilizzo di precedenti password. Il sistema implementa protocollo di autenticazione a due fattori con protocollo TOTP secondo standard RFC 6238. Gli accessi privilegiati alle risorse amministrative sono protetti tramite accesso mediato via VPN.

TRACCIABILITÀ
L'applicativo GlobaLeaks implementa un sistema di audit log sicuro e privacy preserving atto a registrare le attività effettuate dagli utenti e dal sistema in compatibilittà con la massima confidenzialità richiesta dal processo di whistleblowing. I log delle attività del segnalante sono privi delle informazioni identificative dei segnalanti quali indirizzi IP e User Agent. I log degli accessi degli amministratori di sistema vengono registrati tramite moduli syslog e registri remoti centralizzati.

ARCHIVIAZIONE
L'applicativo GlobaLeaks implementa un database SQLite integrato acceduto tramite ORM. Le configurazioni effettuate sono tali da garantire elevate garanzie di sicurezza grazie al completo controllo da parte dell'applicativo delle funzionalittà sicurezza del database e delle policy di data retention e cancellazione sicura.

GESTIONE DELLE VULNERABILITÀ TECNICHE
L'applicativo GlobaLeaks e la relativa metodologia di fornitura SaaS sono periodicamente soggetti ad audit di sicurezza indipendenti di ampio respiro su base almeno annuale e tutti i report vengono pubblicati per finalità di peer review. A questi si aggiunge la peer review indipendente realizzata dalla crescente comunità di stakeholder composta da un crescente numero di società quotate, fornitori e utilizzatori istituzionali che su base regolare commissionano audit indipendenti che vengono forniti al progetto privatamente. Audit di sicurezza: https://docs.globaleaks.org/en/main/security/PenetrationTests.html

BACKUP

I sistemi sono soggetti a backup remoto giornaliero con policy di data retention di 7 giorni necessari per finalittà di disaster recovery.

MANUTENZIONE
È prevista manutenzione periodica correttiva, evolutiva e con finalità di miglioria continua in materia di sicurezza. Per i server applicativi virtuali che realizzano il servizio di whistleblowing è prevista una modalità di manutenzione accessibile al solo personale Whistleblowing Solutions attraverso cui svolgere le modifiche al sistema installare gli aggiornamenti previsti. Per i sistemi che compongono l'infrastruttura fisica, di backup e firewall è prevista una modalità di manutenzione accessibile al solo personale Whistleblowing Solutions e del relativo fornitore SaaS attraverso cui svolgere le modifiche al sistema installare gli aggiornamenti previsti.

SICUREZZA DEI CANALI INFORMATICI
Tutte le connessioni sono protette tramite protocollo TLS 1.2. Le connessioni amministrative privilegiate sono mediate tramite accesso VPN e connessioni con protocollo SSH.

SICUREZZA DELL'HARDWARE
I datacenter del fornitore IaaS dispongono di un'infrastruttura dotata di controllo degli accessi, procedure di monitoraggio 724 e videosorveglianza tramite telecamere a circuito chiuso, in aggiunta al sistema di allarme e barriere fisiche presidiate 724. I datacenter del fornitore IaaS sono certificati ISO27001.

GESTIRE GLI INCIDENTI DI SICUREZZA E LE VIOLAZIONI DEI DATI PERSONALI
Whistleblowing Solutions ha definito una procedura per la gestione delle violazioni dei dati personali.

LOTTA CONTRO IL MALWARE
Tutti i computer del personale di Whistleblowing e dei sub-responsabili nominati eseguono firewall e antivirus come da policy aziendale ed il personale riceve continua e aggiornata formazione al passo con lo stato dell'arte in materia di lotta contro il malware. Parimenti le utenze del servizio di whistleblowing vengono sensibilizzate sulla tematica tramite formazione diretta o documentazione online.