

FONDAZIONE FILM COMMISSION REGIONE CAMPANIA

**VALUTAZIONE DI IMPATTO SULLA PROTEZIONE
DEI DATI NELLA PROCEDURA DI SEGNALAZIONE
DI CONDOTTE ILLECITE (WHISTLEBLOWING)**

1. Premessa

L'art. 35 del Regolamento UE n. 2016/679 (cd. 'GDPR') prevede che venga effettuata una preventiva valutazione d'impatto dei trattamenti previsti (cd. DPIA) qualora tale trattamento di dati personali possa presentare un rischio elevato per i diritti e le libertà delle persone interessate al trattamento, tenuto conto della natura, del contesto e delle finalità del trattamento stesso.

Il GDPR, quindi, introduce una valutazione preliminare che consente al Titolare del trattamento di valutare il rischio prima ancora di procedere al trattamento e di eventualmente attivarsi affinché tale rischio possa essere ridotto al minimo.

I principi fondamentali alla base della DPIA risultano essere:

- i diritti e le libertà fondamentali dell'interessato, punto cardine dell'intero impianto del GDPR, non negoziabili, stabiliti dalla legge, che vanno rispettati in todo, indipendentemente dalla natura, gravità e probabilità dei rischi;
- la gestione dei rischi per la protezione dei dati personali, tramite l'adozione di adeguate misure tecniche ed organizzative di volta in volta adeguate al rischio.

2. Contesto

2.1. Panoramica del trattamento

Il trattamento ha ad oggetto i dati personali dei soggetti che effettuano segnalazioni ai sensi del D.lgs. n. 24/2023. La gestione delle segnalazioni viene effettuata attraverso canale esterno (piattaforma adottata dall'Ente), di cui vengono riportate le principali caratteristiche.

ARCHITETTURA DI SISTEMA	• Un cluster di due firewall perimetrali; • Un cluster di due server fisici dedicati; • Una Storage Area Network pienamente ridondata.
SOFTWARE IMPIEGATO	• software libero ed open-source GlobaLeaks Tecnologie open source: • Debian/Linux (principale sistema operativo utilizzato); • Postfix (mail server); • Bind9 (dns server); • OPNSense (firewall); • OpenVPN (vpn). Software: • 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.

2.2 Responsabilità connesse al trattamento

Ruolo	Nominativo
Titolare del trattamento	Fondazione Film Commission Regione Campania
Responsabile del trattamento	Whistleblowing Solutions
Sub Responsabile	Seeweb

Sub Responsabile	Transparency International Italia
Incaricati al trattamento	RPCT e ODV

2.3 Normative applicabili al trattamento

Al trattamento in materia di segnalazioni e normativa whistleblowing si applicano le seguenti normative e standard:

D.lgs. n. 24/2023;

Regolamento UE n. 2016/679 (c.d. GDPR);

D.lgs. n. 196/2003 (c.d. Codice Privacy) così come modificato dal D.lgs. n. 101/2018;

Direttiva UE 1937/2019.

2.4 Dati ed 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 come da disciplinare.

Categoria di dato personale	Categoria di interessato
Dati personali comuni	- Dati identificativi e di contatto dei referenti del Titolare che attivano il servizio di digital whistleblowing (es. Responsabile Anticorruzione). - Dipendenti e collaboratori che effettuano una segnalazione o che ne sono oggetto - Fornitori che effettuano una segnalazione o che ne sono oggetto
Dati particolari	- Dipendenti e collaboratori che effettuano una segnalazione o che ne sono oggetto - Fornitori che effettuano una segnalazione o vengono segnalati
Dati giudiziari (es. condanne penali)	- Dipendenti e collaboratori che effettuano una segnalazione o che ne sono oggetto - Fornitori che effettuano una segnalazione o vengono segnalati

2.4.1 Ciclo di vita del trattamento dei dati (descrizione funzionale)

1. Attivazione della piattaforma;
2. Configurazione della piattaforma;

3. Fase d'uso della piattaforma con caricamento delle segnalazioni da parte dei segnalanti e accesso alle stesse da parte dei soggetti preposti;
4. 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.



2.5. Risorse a supporto dei dati

Software di whistleblowing professionale GlobaLeaks.

Infrastruttura IaaS e SaaS privata basata su tecnologie:

- VMWARE (virtualizzazione)
- Debian Linux LTS (sistema operativo)
- VEEAM (backup)
- OPNSENSE (firewall)
- OPENVPN (vpn)

3. Valutazioni in merito ai trattamenti

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, Ruolo, Telefono, Email di ruolo dell'utente che effettua la registrazione e i dati relativi all'ente (denominazione, indirizzo, Codice Fiscale, Partita IVA). Il software di whistleblowing raccoglie segnalazioni secondo questionari in ambito di whistleblowing predisposti 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. Al fine di consentire la possibilità di segnalazioni orali e al contempo tutelare l'anonimato e la confidenzialità, il sistema applica avanzate tecniche di "vocoding" (atte a evitare di raccogliere il timbro vocale) e "pitch shifting" (atte a variare il tono della voce in modo casuale) capaci di offrire elevate caratteristiche di anonimizzazione al passo con la ricerca nello specifico contesto d'uso. Tali tecniche permettono ai riceventi di ascoltare la registrazione senza essere in condizione di identificare la voce direttamente e rendendo altamente inefficaci tecniche moderne di de-anonimizzazione. Nonostante la registrazione venga protetta sotto questo profilo e venga mantenuta in forma alla pari di ogni allegato della segnalazione, per l'ascolto è indicato l'uso di cuffie per limitare l'esposizione del contenuto del messaggio.
--	---

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 12 mesi, con cancellazione automatica sicura delle segnalazioni che raggiungono la data di scadenza. Il gestore può anticipare la scadenza delle segnalazioni fino a 3 mesi dalla data dell'operazione e può prorogare la scadenza delle segnalazioni per il tempo ritenuto congruo al trattamento dei dati. Anticipazioni e proroghe delle scadenze possono essere fatte dal gestore più volte. Cancellazione della piattaforma 15 giorni dopo la disattivazione del servizio, a condizione che non esistano segnalazioni aperte sulla piattaforma.
Definizione degli obblighi dei responsabili del trattamento e formalizzazione dei contratti	Gli accordi contrattuali sono definiti con le seguenti società: • Whistleblowing Solutions in qualità di Responsabile del trattamento • Seeweb in qualità di Sub-Responsabile del trattamento nominato da Whistleblowing Solutions • Transparency International Italia in qualità di Sub-Responsabile del trattamento nominata da Whistleblowing Solutions
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 verso l'estero in paesi extra UE.

3.1. Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?	Gli interessati sono informati attraverso una specifica informativa resa ai sensi degli artt. 13-14 GDPR. L'informativa viene resa disponibile secondo le seguenti modalità: - Processo comunicazione aziendale sull'esistenza del canale di segnalazione interno (canale informatico); - Pubblicazione sito internet – sezione dedicata al Whistleblowing
Ove applicabile: come si ottiene il consenso degli interessati?	Il trattamento dei dati personali relativi la segnalazione da parte dei soggetti espressamente autorizzati al trattamento non necessita di consenso da parte dell'interessato, in quanto la base giuridica del trattamento è l'adempimento di un obbligo di legge (Art. 6.1. lett. c) del GDPR). Nel caso invece ricorra l'ipotesi di comunicazione dei dati personali a soggetti diversi da quelli espressamente autorizzati dal Titolare, il segnalante dovrà prestare il suo consenso specifico alla segnalazione ai sensi degli, tramite piattaforma artt. 6.1. lett. a) e 7 del GDPR.
Come fanno gli interessati a esercitare i loro diritti previsti dagli artt. 15 ss. GDPR?	Gli interessati possono esercitare i diritti previsti dagli artt. 15 ss. del GDPR attraverso l'indirizzo di posta elettronica del RPD gdpr@hsh.it, nei limiti di cui all'articolo 2-undecies del Codice Privacy
Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?	Le terze parti che trattano dati personali per conto del Titolare hanno stipulato accordo per la nomina di Responsabili del trattamento ai sensi dell'art. 28 GDPR.

5. 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 1.22 con SSL Labs rating A2. 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 FDE2 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 compatibilità con la massima confidenzialità richiesta dal processo di whistleblowing. Ogni log di audit viene mantenuto per un periodo massimo di 5 anni, fatto salvo il caso specifico dei log pertinenti le segnalazioni che vengono mantenuti per tutto il tempo di conservazione delle stesse. 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 funzionalità 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.
Backup	I sistemi sono soggetti a backup remoto con frequenza di 8 ore e policy di data retention di 7 giorni necessari per finalità di disaster recovery garantendo dunque una RPO di 8 ore.

Manutenzione	E' 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 1.23 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 7324 e videosorveglianza tramite telecamere a circuito chiuso, in aggiunta al sistema di allarme e barriere fisiche presidiate 7324. I datacenter del fornitore IaaS sono certificati ISO27001.
Gestione incidenti di sicurezza e 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 sono protetti tramite 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.

6. Rischi

6.1 Metodologia

Per stabilire l'entità dell'eventuale rischio elevato per il trattamento specifico si è seguito un sistema di calcolo del rischio basato su parametri oggettivi: la valutazione pertanto passa attraverso un

modello di 'Probabilità e Gravità' in grado di rispecchiare il contesto in cui l'Ente opera. Sono state identificate griglie oggettive di calcolo delle Probabilità e Gravità con riguardo ai diritti e libertà dell'interessato.

12

Matrice Ri = P x G					
	Probabilità	1 - Trascurabile	2 – Limitata	3 – Importante	4 – Massima
G r a v i t à	1 - Trascurabile	1	2	3	4
	2 – Limitata	2	4	6	8
	3 – Importante	3	6	9	12
	4 – Massima	4	8	12	16

Gravità	Significato	Descrizione generica degli impatti (diretti e indiretti)
4	Massima	I soggetti interessati possono incontrare conseguenze irreversibili.
3	Importante	I soggetti interessati possono incontrare conseguenze significative, e difficoltà nella loro risoluzione, ma comunque superabili.
2	Limitata	I soggetti interessati possono incontrare inconvenienti superabili.
1	Trascurabile	Gli interessati non saranno coinvolti o potrebbero incontrare alcuni lievi inconvenienti senz'altro superabili.

Probabilità	Significato	Criterio di scelta
4	Massima	Il verificarsi del danno dipende da condizioni direttamente connesse alla situazione; Il verificarsi del danno non provocherebbe alcuna reazione di stupore; Eventi simili sono già accaduti in azienda o in aziende dello stesso tipo
3	Importante	Il verificarsi del danno dipende da condizioni non direttamente connesse alla situazione ma possibili; Il verificarsi del danno provocherebbe reazioni di moderato stupore; Eventi simili sono stati già riscontrati
2	Limitata	Il verificarsi del danno dipende da condizioni impreviste Il verificarsi del danno provocherebbe reazioni di grande stupore tra gli addetti; Eventi simili si sono verificati molto raramente

1	Trascurabile	Il verificarsi del danno è subordinato a un concatenamento di eventi indipendenti tra loro; Il Verificarsi del danno è creduto impossibile dagli addetti; Non è mai accaduto nulla di simile
---	--------------	---

Valutazione delle Misure esistenti

Rating	Valutazione conseguente
1-25 %	Misure non adeguate
26-50%	Misure minime
51-75%	Misure adeguate

Valutazione del rischio residuo (Rr)

Rischio Alto	6,1-16
Rischio Medio	3,1-6
Rischio Basso	1-3

Elementi per la valutazione:

- Ri** è il Rischio Inerente valore di riferimento su cui effettuare le valutazioni e le operazioni di mitigazione
- Rr** è il Rischio Residuo calcolato al netto delle misure di mitigazione del rischio (determinate in via percentuale - % abbattimento)
- L'Ente valuta come Rischio Accettabile (**Ra**) = 3
- Se il rischio inerente **Ri** a seguito delle valutazioni oggettive, dovesse risultare superiore ad **Ra**, l'azienda interverrà con mitigazioni opportune tali che ad **Rr < Ra**

6.2 Analisi dei rischi

6.2.1. Accesso illegittimo – Perdita della riservatezza

GRAVITÀ (G)	I soggetti interessati possono incontrare conseguenze significative e difficoltà nella loro risoluzione, ma comunque superabili come: disagio, Diffusione indesiderata dei propri dati, Consultazione dei propri da parte di personale non autorizzato, Ricatto economico, Problematiche di natura giuslavoristica e contrattuale, Mobbing, Discriminazioni lavorative, Ritorsioni.					
PROBABILITÀ (P)	Il verificarsi del danno dipende da condizioni impreviste. Il verificarsi del danno provocherebbe reazioni di grande stupore tra gli addetti; Eventi simili si sono verificati molto raramente					
FONTI DI RISCHIO	Fonti umane interne (es. dipendenti, collaboratori, la cui condotta può essere accidentale o intenzionale) Fonti umane esterne (es. fornitori la cui condotta può essere accidentale o intenzionale, attaccanti e hacker) Fonti non umane (es. allagamenti, materiali pericolosi o virus informatici generici)					
MISURE	Le misure che contribuiscono a mitigare il rischio sono quelle descritte al paragrafo 5 del presente documento					
CALCOLO DEL RISCHIO RESIDUO						
		G	P	Ri	Mitigazione % abbattimento rischio	Rr
		3	2	6	70%	1,8

6.2.2. Modifiche indesiderate – Perdita dell'integrità

GRAVITÀ (G)	I soggetti interessati possono incontrare conseguenze significative e difficoltà nella loro risoluzione, ma comunque superabili come: Disagio, Diffusione indesiderata dei propri dati, Consultazione dei propri da parte di personale non autorizzato, Ricatto economico, Problematiche di natura
--------------------	--

	giuslavoristica e contrattuale, Mobbing, Discriminazioni lavorative.					
PROBABILITÀ (P)	Il verificarsi del danno dipende da condizioni impreviste. Il verificarsi del danno provocherebbe reazioni di grande stupore tra gli addetti. Eventi simili si sono verificati molto raramente.					
FONTI DI RISCHIO	Fonti umane interne (es. dipendenti, collaboratori, la cui condotta può essere accidentale o intenzionale) Fonti umane esterne (es. fornitori la cui condotta può essere accidentale o intenzionale, attaccanti e hacker) Fonti non umane (es. allagamenti, materiali pericolosi o virus informatici generici).					
MISURE	Le misure che contribuiscono a mitigare il rischio sono quelle descritte al paragrafo 5 del presente documento.					
CALCOLO DEL RISCHIO RESIDUO						
		G	P	Ri	Mitigazione % abbattimento rischio	Rr
		3	2	6	70%	1,8

6.2.3. Perdita del dato – Perdita della disponibilità

GRAVITÀ (G)	I soggetti interessati possono incontrare conseguenze significative e difficoltà nella loro risoluzione, ma comunque superabili come: Disagio, Diffusione indesiderata dei propri dati, Consultazione dei propri da parte di personale non autorizzato, Ricatto economico, Problematiche di natura giuslavoristica e contrattuale, Mobbing, Discriminazioni lavorative.
PROBABILITÀ (P)	Il verificarsi del danno dipende da condizioni impreviste Il verificarsi del danno provocherebbe reazioni di grande stupore tra gli addetti. Eventi simili si sono verificati molto raramente.
FONTI DI RISCHIO	Fonti umane interne (es. dipendenti, collaboratori, la cui condotta può essere accidentale o intenzionale) Fonti umane esterne (es. fornitori la cui condotta può essere accidentale o intenzionale, attaccanti e hacker) Fonti non umane (es. allagamenti, materiali pericolosi o virus informatici generici).

MISURE	Le misure che contribuiscono a mitigare il rischio sono quelle descritte al paragrafo 5 del presente documento.					
CALCOLO DEL RISCHIO RESIDUO		G	P	Ri	Mitigazione % abbattimento rischio	Rr
		3	2	6	70%	1,8

7. Parere delle parti interessate

Non è stato richiesto un parere alle parti interessate in quanto la finalità del trattamento rappresentano l'adempimento di obblighi di legge. Ai fini dell'attivazione del canale di segnalazione interna, si precisa che l'Ente non dispone di rappresentanze sindacali.

8. Parere del Responsabile della Protezione Dati

Il Responsabile della Protezione Dati esprime il proprio parere favorevole alla DPIA effettuata con riferimento alla valutazione di impatto dei dati personali relativi agli adempimenti in materia di whistleblowing, in quanto conformi al dettato normativo.

8. Conclusioni

Dall'analisi sull'impatto dei rischi valutati in particolare nell'ambito dei trattamenti individuati aventi l'obbligo di DPIA, emergono "rischi inerenti (Ri)" con impatto sui diritti e libertà degli interessati con stima a valore Medio. Nell'ottica di mitigazione di tali rischi, si evince che, con l'implementazione delle misure tecnico/organizzative pianificate ad integrazione di quelle già messe in atto, il valore di rischio residuo rientra nei parametri accettabili uguali o minori rispetto al Rischio accettato (Ra) dall'organizzazione aventi stima a *valore Basso*, valore ritenuto accettabile in relazione dai parametri oggettivi considerati.

Si ritiene pertanto che il trattamento in oggetto presenta un grado di rischio sui diritti e libertà dell'interessato rientrante nei parametri accettabili e di conseguenza *non è richiesta una consultazione preventiva all'Autorità Garante*.

Napoli, data riportata nella firma digitale

per il Legale Rappresentante
Dott.ssa Concetta Fiore (detta Titta)
Il Direttore
Maurizio Gemma

Il Responsabile della Protezione dati
Ing. Gianfranco Bruno

GIANFRANCO
STEFANO
BRUNO
27.01.2025
20:36:38
GMT+02:00

MAURIZIO
GEMMA
27.01.2025
16:14:21
GMT+01:00
frc@pec.it