Per Noli Srl

Sede Legale : Via Crescenzago 55 – 20134 Milano (MI)
Sede Amministrativa : Via Crescenzago 55 – 20134 Milano *PEC:* pernoli@lamiapec.it
Tel. 02-36743200 – Fax 02-36680845
C.F. – P.IVA 07699330960 – Codice Univoco W7YVJK9 *Sito Internet: www.pernolisrl.it*

Analisi rischi privacy e valutazione d'impatto in attuazione del Regolamento Generale sulla Protezione dei Dati

GDPR RE 679/2016 D.Lgs. 196/2003 D.Lgs. 101/2018

Aggiornamento in data 30 Giugno 2023

Il Titolare del Trattamento

PER NOLI srl
via Crescenzago 55 20134 Milano MI
C.F. e P.IVA: 07699330960
Presidente e Legale Rappresentante: Gianluca Premoselli
Tel. 02.36743200
email privacy@hcmitalia.it info@hcmitalia.it pec pernoli@lamiapec.it
sito internet www.pernolisrl.it

unità operative:
RESIDENZA PROTETTA VILLA ROSA REGIONE POZZALI, 5 NOLI SAVONA

Legale Rappresentante e Titolare del Trattamento dei Dati

- Presidente Gianluca Premoselli

Soggetti designati al Trattamento dei Dati:

- ROSATI MONICA
- DIEGO MARCHINI

Responsabile IT

- MARTINANGELI SERGIO
  data nomina: 30-06-2023 scadenza nomina: al termine del mandato e/o del rapporto di collaborazione

Responsabili esterni del Trattamento dei Dati

- Consorzio HCM : contabilità e paghe, gestione personale, progettazione, qualità, compliance normativa
  data nomina: 30-06-2023 scadenza nomina: al termine del mandato e/o del rapporto di collaborazione
- Davide Locastro : OdV 231
  data nomina: 30-06-2023 scadenza nomina: al termine del mandato e/o del rapporto di collaborazione
- LDL Lawyers - Avv. Elisabetta Portoghese : Affari Legali
  data nomina: 30-06-2023 scadenza nomina: al termine del mandato e/o del rapporto di collaborazione
- PREMOSELLI GIANLUCA RSPP
  data nomina: 30-06-2023 scadenza nomina: al termine del mandato e/o del rapporto di collaborazione
- PENATI DR. PIETRO : Medico Competente
  data nomina: 30-06-2023 scadenza nomina: al termine del mandato e/o del rapporto di collaborazione

Incaricati al Trattamento dei Dati

Tutti gli Operatori della Società che compiono operazioni sui dati presenti nelle diverse sedi e servizi vengono nominati, all'atto dell'assunzione, Incaricati al Trattamento dei Dati; allo stesso modo tutti i collaboratori e i consulenti che operano nelle diverse sedi e servizi vengono nominati, con il contratto di collaborazione o la lettera di incarico, Incaricati al Trattamento dei Dati.

Titolarità e Responsabilità nel Trattamento dei Dati in progetti e servizi in gestione

Per alcuni progetti/servizi Per Noli srl può essere chiamato come Contitolare del trattamento o come Responsabile esterno del trattamento da parte dell'Ente Committente e Titolare; allo stesso modo può essere nominata Corresponsabile o Subresponsabile del trattamento in occasione di RTI o altre forme di partnership per la gestione di progetti e servizi. Le specifiche delle diverse nomine e responsabilità sono inserite e aggiornate regolarmente nel Registro del Trattamento dei Dati.

Le Linee Guida Attuative sono state emesse da questa Società ai sensi del RE 679/2016 allo scopo di definire il sistema di gestione e protezione dei dati personali. Il presente documento è integrato dal **Registro dei Trattamenti** dei dati detenuto in formato informatico e dalla seguente documentazione allegata:

Documento	Presente	Formato C Cartaceo E Elettronico
Registro Trattamento dei Dati	SI	E

Registro data Breach	SI	E
Informativa/e sul trattamento dei dati	SI	C E
Consenso al trattamento dei dati	SI	C E
Liberatoria video audio foto	SI	C E
Valutazione dei rischi e di impatto	SI	E
Nomina Responsabile IT	SI	C E
Nomina Soggetti designati	SI	C E
Nomina Responsabili Esterni	SI	C E
Regolamento utilizzo strumenti informatici e tecnologici	SI	C E

Elenco dei trattamenti

Nome / sigla	**N° / RIF**		**N° / RIF**
Gestione Personale	001	Gestione Servizi Residenziali	005
Gestione Professionisti esterni	002	Gestione Istruzione Formazione professionale	006
Gestione Fornitori	003		
Preventivazione Fatturazione	004		

All'interno del Registro Trattamenti sono specificati e aggiornati i singoli progetti/servizi e le specifiche tipologie di trattamento, con le relative nomine e responsabilità.

Dati sensibili trattati

Origini razziali e/o etniche	S	
Convinzioni religiose, filosofiche o di altro genere	S	
Opinioni politiche		N
Adesione a partiti/sindacati/associazioni/organizzazioni a carattere religioso/filosofico/politico/sindacale	S	
Stato di salute	S	
Dati biometrici		N
Vita sessuale	S	

Dati relativi ai provvedimenti di cui all'art. 686 Codice di Procedura Penale, commi 1, lettere a) d), 2, 3: dati giudiziari trattati

Dati evincibili dalle iscrizioni nel casellario giudiziario:	S	
condanna penale, dichiarazione di abitualità del reato, pene accessorie...		
Dati evincibili dalle relazioni del tribunale e/o dei Servizi Sociali	S	
decreti allontanamento, decreti limitazione patria potestà...		

Modalità di elaborazione dei dati

Elaboratori accessibili per il tramite di una rete di telecomunicazioni (Internet) e VPN	S	
Fogli di calcolo e programmi di scrittura (file elettronici e stampati)	S	

Modalità di archiviazione dei dati

archiviazione elettronica su server fisico e in cloud	S	
archiviazione fisica /archivi cartacei	S	

Soggetti che trattano i dati

Legale Rappresentante e Titolare	S	
Soggetti designati al trattamento dei dati	S	
Responsabili esterni del trattamento dei dati	S	
Incaricati del trattamento dei dati	S	
Terzi (persone fisiche e/o giuridiche) (*previo incarico scritto*)	S	

In ottemperanza al dispositivo del D.P.R. 28 Luglio 1999, n. 318 e al Codice sulla privacy, si è già provveduto a introdurre adeguate misure per gli accessi e l'archiviazione, da comunicare a tutti i soggetti che trattano i dati personali specificamente interessati

Ambito di divulgazione dei dati

Comunicazione all'interno	S	
Comunicazione nell'ambito di strutture (comprese Comuni/Servizi Sociali, ATS, ecc.) (*ove del caso*)	S	
Comunicazione ad altre strutture in Italia (*ove del caso e richiesto dalle Leggi vigenti*)	S	
Comunicazione ad altre strutture all'estero		N
Diffusione generalizzata verso l'esterno		N

Modalità e strumenti di comunicazione dei dati

Posta elettronica	S	
Invio comunicazioni, relazioni, valutazioni, progetti relativi all'utenza Invio preventivi fatture Invio comunicazioni al personale e ai collaboratori		
Posta ordinaria	S	
Contratti e documentazione burocratico amministrativa Comunicazioni formali in originale		

Supporti e strumenti per il trattamento dei dati

Personal computer (desktop/portatili)	S	
Smartphone/Tablet	S	
Server	S	
USB	S	
Nastri magnetici video audio video-audio	S	
Archivi cartacei	S	
Archivi di fotografie	S	

ANALISI dei RISCHI

Questo documento intende ridefinire formalmente, sulla base di un'adeguata "analisi dei rischi" e della distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati medesimi, quanto segue:

- i criteri tecnici ed organizzativi adottati per proteggere aree e locali interessati dalle misure di sicurezza e le procedure adottate per controllare l'accesso delle persone autorizzate alle aree/ai locali medesime/i
- i criteri e le procedure adottati/e per assicurare l'integrità dei dati
- i criteri e le procedure adottati/e per garantire la sicurezza della trasmissione dei dati (ivi comprese quelle adottate per *restringere* gli accessi per via telematica)
- i piani di formazione di tutti gli incaricati del trattamento, al fine di renderli adeguatamente edotti dei criteri e delle procedure adottati/e per prevenire danni associati ai rischi individuati
- L'obiettivo finale è di garantire *non solo la conservazione, oltre al possibile miglioramento*, delle misure minime di sicurezza dei dati di cui al RE, *ma di misure "idonee" ad offrire garanzie "certe" in merito alla sicurezza medesima*, rispettando le indicazioni fornite dall'Ufficio del Garante a far data dalla precedente emissione del presente documento.

Questo documento verrà costantemente aggiornato, a seguito di:

- una puntuale verifica dell'efficacia delle misure adottate
- l'eventuale decisione in merito all'attivazione di processi correttivi e/o preventivi e/o di miglioramento continuo

L'analisi dei rischi ha comportato:

- la rilevazione dei rischi che gli strumenti utilizzati, i supporti cartacei e magnetici, i contenitori e gli archivi, le risorse umane, ... coinvolti/e nelle operazioni di trattamento dei dati personali possono correre
- l'individuazione delle minacce che possono causare tali rischi
- la valutazione delle conseguenze potenziali e la valutazione della loro gravità in tutti i casi in cui uno o più rischi si verifichino

La definizione del piano di miglioramento si basa sull'analisi dei seguenti rischi, minacce e conseguenze e sulla compilazione/revisione delle tabelle di cui alle pagine seguenti, anch'esse potenzialmente variabili nel tempo.

Rischi:

- ☐ distruzione o perdita, anche accidentale, di dati
- ☐ accessi non autorizzati
- ☐ trattamenti non consentiti o non conformi alle finalità della raccolta dei dati

Minacce:

- ☐ alterazione di dati
- ☐ disastri naturali, quali incendi e/o allagamenti
- ☐ divulgazione/comunicazione non consentita/autorizzata
- ☐ duplicazione e diffusione di dati a scopo di lucro e/o di nocumento
- ☐ sottrazione/furto di dati
- ☐ guasti delle apparecchiature informatiche
- ☐ errori umani causati da imperizia

Conseguenze:

- ☐ sanzioni di natura penale
- ☐ risarcimenti in sede civile
- ☐ sanzioni amministrative da parte del Garante
- ☐ perdite economico/finanziarie
- ☐ blocco dell'attività
- ☐ perdita di immagine
- ☐ costi gestionali
- ☐ responsabilità contrattuali

Tipologia e natura dei dati trattati

Per Noli srl raccoglie, gestisce, comunica e archivia una serie di dati personali e sensibili (sanitari e giudiziari) relativi ai propri dipendenti e collaboratori, ai clienti pubblici e privati, ai committenti e ai fornitori, agli utenti dei servizi e alle loro famiglie.
Relativamente ai dipendenti, ai soci, ai collaboratori, ai tirocinanti e ai volontari i dati sono dati personali e sensibili (nome e cognome, dati anagrafici, titolo di studio, esperienza lavorativa, coordinate bancarie, dati familiari, particolari condizioni di salute, particolari condizioni di reddito, certificato casellario giudiziale e dei carichi pendenti...) necessari alla gestione e alla tutela del contratto di lavoro o di collaborazione e dei rapporti sociali.
Relativamente a clienti, committenti e fornitori i dati sono dati personali (anagrafica, coordinate bancarie...) necessari alla gestione dei contratti.
Relativamente agli utenti dei servizi e alle loro famiglie i dati sono dati personali e sensibili (nome e cognome, dati anagrafici, dati familiari, condizione di salute, eventuali atti di natura giudiziaria come tutele, curatele, amministrazioni di sostegno, relazioni specialistiche e di altri servizi...); tali dati, peraltro richiesti in maniera vincolante dalle DGR che stabiliscono requisiti e criteri per le diverse unità di offerta e da convenzioni, contratti e accreditamenti, sono necessari ai fini dell'erogazione del servizio.

Categorie di interessati

Per Noli srl ha determinato tre macro-categorie di soggetti interessati:

- dipendenti, collaboratori, tirocinanti e volontari
- committenti e fornitori
- clienti/utenti e loro famiglie

Liceità e congruità del trattamento

Per quanto riguarda dipendenti, collaboratori e volontari i dati vengono acquisiti e trattati sulla base di specifici vincoli contrattuali (leggi sul Terzo Settore, contratto di lavoro, lettere di incarico e contratti di consulenza, legislazione nazionale sul lavoro, DGR sulle diverse unità di offerta, convenzioni e accreditamenti) con l'esclusiva finalità di gestione dei contratti di lavoro o di collaborazione e di gestione dei rapporti sociali all'interno del Consorzio. Anche l'eventuale comunicazione a terzi di tali dati è strettamente legata a disposizioni di legge o a necessarie procedure di tipo contabile e amministrativo.
Per quanto riguarda clienti pubblici e privati, committenti e fornitori i dati vengono acquisiti e trattati sulla base di specifici vincoli contrattuali (ordini e offerte, contratti, convenzioni, accreditamenti...) con l'esclusiva finalità di gestione dei contratti. Anche l'eventuale comunicazione a terzi di tali dati è strettamente legata a disposizioni di legge o a necessarie procedure di tipo contabile e amministrativo.
Per quanto riguarda gli utenti dei servizi e le loro famiglie i dati vengono acquisiti e trattati sulla base di specifici vincoli legislativi (convenzioni e accreditamenti, DGR sulle diverse unità di offerta, contratti, leggi di settore...) con l'esclusiva finalità di gestire ed erogare in maniera efficace e corretta il servizio. Anche l'eventuale comunicazione a terzi di tali dati è strettamente legata a disposizioni di legge, vincoli derivanti da convenzioni e accreditamenti o a necessarie procedure di tipo contabile e amministrativo.

Descrizione del trattamento

Per il personale, i collaboratori e volontari i dati vengono raccolti e archiviati in formato cartaceo e/o elettronico ed eventualmente organizzati in database ordinati, in modo da poter espletare in maniera completa e corretta tutte le operazioni relative ai contratti e alle collaborazioni (operazioni sul contratto di lavoro, operazioni contabili e amministrative, adempimenti fiscali e assicurativi...). I dati raccolti possono essere consultati solo dal personale incaricato e preposto a tali operazioni e comunicate ai soggetti autorizzati o previsti per legge.

Per i clienti, i committenti e i fornitori, i dati vengono raccolti e archiviati in formato cartaceo e/o elettronico ed eventualmente organizzati in database ordinati, in modo da poter espletare in maniera completa e corretta tutte le operazioni relative ai contratti, alle convenzioni e agli accreditamenti (operazioni sui contratti, operazioni contabili e

amministrative, adempimenti fiscali e assicurativi...). I dati raccolti possono essere consultati solo dal personale incaricato e preposto a tali operazioni e comunicate ai soggetti autorizzati o previsti per legge.

Per gli utenti e le loro famiglie i dati vengono raccolti e archiviati in formato cartaceo e/o elettronico ed eventualmente organizzati in cartelle e database ordinati, in modo da poter espletare in maniera completa e corretta tutte le operazioni relative all'erogazione del servizio (inserimento, osservazione, valutazione, presa in carico socio-educativa e socio-sanitaria, progettazione e verifica personalizzata, rapporti di rete, attività). I dati raccolti possono essere consultati solo dal personale incaricato e preposto a tali operazioni e comunicate ai soggetti autorizzati o previsti per legge.

Soggetti che eseguono il trattamento

Per Noli srl ha provveduto a nominare formalmente i Soggetti designati, gli Incaricati e i Responsabili esterni del trattamento, specificando per ogni categoria di soggetti interessati, per tipologia di dati e per Area/Servizio le funzioni preposte al trattamento. Ai Soggetti designati, agli incaricati e ai Responsabili sono state fornite le necessarie istruzioni operative ed è stata loro consegnata la documentazione di pertinenza. Per Noli srl ha provveduto inoltre a nominare il Responsabile IT.

Strumenti utilizzati per il trattamento

I dati vengono gestiti e archiviati sia in formato cartaceo che in formato elettronico.
Gli archivi cartacei sono costituiti da copie fotostatiche di documenti, dichiarazioni, attestazioni etc... e da stampe di file elaborati elettronicamente da programmi di scrittura o elaborazione del pacchetto Office (Word, Excel).
Alcuni dati contabili e amministrativi sono gestiti in formato elettronico da software gestionali dedicati
- PRESSO LA SEDE DI MILANO
- A NOLI COMPIUTER PROTETTO DA FAREWALL MODELLO
VIENE EFFETTUATO BACK UP – MENSILE
VIENE EFFETTUATO BACK UP MENSILE SU UNITA ESTERNA CONTENUTA IN ARMADIO CUSTODITO

Cartelle e archivi cartacei sono riposti in armadi e classificatori in uffici chiusi con chiave.

Per quanto riguarda gli strumenti informatici la Società dispone di:

- Unità Desktop PC
- Unità PC Portatili
- Unità Server

L'elenco completo degli strumenti elettronici, delle loro caratteristiche e della loro assegnazione è riportato in apposito elenco, documento archiviato e aggiornato dal Referente Privacy.

Il Sistema Operativo è Microsoft Windows in diverse versioni gli applicativi sono Microsoft Office.

La manutenzione hardware è in assistenza con: MARTINANGELI SERGIO

IL router è configurato per non accettare alcuna connessione in entrata, fatta eccezione per quelle necessarie al server VPN, al server ssh.

Firewall perimetrale a protezione dei server Cloud viene periodicamente aggiornato

Antivirus si aggiorna automaticamente.

Per aggiornare i server è necessario concordare specifiche finestre di manutenzione che non consentiranno gli accessi utente.

Le password degli utenti sono personali e possono essere cambiate in ogni momento.

Collocazione dei dati

Archivi cartacei in armadi situati nei luoghi di lavoro; computer situati all'interno dei luoghi di lavoro (Sede legale e sedi operative). Un elenco con l'attribuzione dei diversi PC (e degli eventuali archivi cartacei) è inserito nell'Elenco PC, documento archiviato e aggiornato dal Responsabile del trattamento.

Strutture che concorrono al trattamento

Per la gestione organizzativa e l'erogazione dei servizi
- Servizio di elaborazione paghe e gestione contabilità
- Consulenti fiscali, del lavoro, legali
- RSPP
- Medico Competente
- Responsabile IT

Per la verifica della compliance normativa
- OdV 231
- RGQ

Strutture alle quali vengono comunicati i dati

Per il personale, i soci, i collaboratori e i volontari:
- INPS, INAIL e altri enti statali di riferimento
- Agenzia delle Entrate
- Assicurazioni
- Enti accreditanti e committenti
- Forze dell'ordine, di pubblica sicurezza e di pronto soccorso

Per clienti, committenti e fornitori
- Agenzia delle entrate

Per gli utenti e le loro famiglie
- Enti invianti Servizi Sociali e rete dei Servizi
- ASST e relativi servizi e presidi
- Medici di base e specialisti
- Tutori, Curatori e Amministratori di Sostegno
- Servizi territoriali di riferimento
- Tribunali
- Forze dell'ordine e di pubblica sicurezza e di pronto soccorso

Protezione fisica del server

Il sistema centrale è situato in locale chiuso	S	
L'accesso al locale è:		
controllato	S	
consentito soltanto alle persone autorizzate	S	
Sono in funzione sistemi di allarme	S	
Sono operativi i dispositivi antincendio di cui al D.Lgs. 81/08 e s.m.i. (estintori)	S	
E' garantita la continuità elettrica		N
Sono operativi dispositivi di antintrusione fisica		N
E' operativo un servizio di vigilanza		N
E' in funzione un sistema di climatizzazione del locale		N

Protezione logica del server

Il sistema operativo è:		
aggiornato/i con le ultime patch	S	
protetto/i con sistemi antivirus aggiornati	S	
protetto con sistemi antintrusione logica e hardware aggiornati (Firewall)	S	
Le password di accesso sono assegnate:		
secondo criteri approvati	S	
E' prevista l'autenticazione delle password all'atto della connessione alla rete	S	
E' previsto il log/la memorizzazione di:		
connessioni effettuate	S	
tentativi di penetrazione (lo strumento adottato è il Firewall hardware)	S	
E' formalmente definita l'ubicazione di detto log/memorizzazione	S	

Protezioni dei personal computer (portatili e non portatili)

E' previsto l'uso di Antivirus e di un Firewall aggiornato	S	
E' previsto l'aggiornamento automatico e/o manuale dell'antivirus	S	
E' prevista una password per l'accesso secondo quanto richiesto dall'Uff. del Garante	S	

Protezioni reti/lan

I cavi di connessione sono:		
protetti	N	
sotto controllo	S	
certificati	S	
Gli armadi e/o i contenitori delle apparecchiature di collegamento sono chiusi a chiave	N	

Protezioni globali: backup e disaster/recovery

Il salvataggio dei dati personali sensibili viene effettuato su:		
Server	S	
Chiave USB o Hard Disk esterni		N
Il salvataggio dei dati personali comuni (tutti gli altri dati personali) viene effettuato su:		
Server	S	
Chiave USB o Hard Disk esterni		N
I supporti di salvataggio dei dati personali sensibili sono:		
custoditi in altro luogo	S	
protetti in cassaforte		N
E' previsto un test periodico di recovery		N
Se no: è prevista la definizione di un Piano di disaster/recovery		N
Se sì: è previsto l'aggiornamento a frequenza fissa del Piano di disaster/recovery		N

Protezione delle aree/dei locali in cui sono custoditi dati personali

E' prevista una divisione "certa" degli archivi dei dati sensibili da quelli dei dati comuni		N
I locali in cui sono conservati i dati personali sono sempre chiusi	S	
L'accesso ai vari archivi prevede:		
una pre-selezione (con predisposizione, *ove del caso*, di lista degli incaricati del trattamento)		N

l'identificazione e la registrazione dei soggetti che vi accedono fuori orario		N
Nei locali sono attivi sistemi di allarme		N
Nei locali sono attivi sistemi ai sensi del D.Lgs. 81/08 e s.m.i. (estintori con contratto di manutenzione)	S	
Nei locali sono attivi sistemi di climatizzazione	S	N
Nei locali sono attivi sistemi di antintrusione fisica (parziale)	S	
I dati sono conservati in armadi/ambienti:		
muniti di chiusura	S	
ignifughi		N
È attivo un sistema di vigilanza		N
È stata formalizzata la nomina del custode delle chiavi di accesso ad aree/archivi contenenti i dati:		
personali (sensibili, comuni)		N

Regole di accesso ai dati personali

L'accesso è consentito soltanto alle persone formalmente autorizzate	S	
Al termine della loro consultazione è fatto obbligo agli incaricati del trattamento di restituire/ ricollocare nella posizione originaria atti e documenti	S	
Durante la consultazione e fino alla restituzione è fatto obbligo agli incaricati del trattamento di conservare atti e documenti contenenti dati personali in contenitori chiusi	S	
Per ciò che attiene ai terzi (persone fisiche e/o giuridiche che possono avere accesso ai dati personali):		
sottoscrivono clausole di riservatezza sugli accordi contrattuali (*in alternativa, vedi nel seguito*)	S	
vengono nominati responsabili del trattamento	S	
vengono nominati incaricati del trattamento (*in alternativa, vedi sopra*)	S	

Misure di sicurezza adottate

L'accesso fisico alle stanze contenti documenti trattanti dati personali è permesso solo agli incaricati del trattamento. Gli armadi in cui sono detenuti documenti cartacei inerenti dati personali devono essere dotati di serratura a chiave. Il Responsabile del trattamento si occupa della gestione delle chiavi in oggetto Sono state fornite istruzioni organizzative e tecniche ad hoc per la custodia e l'uso di supporti rimovibili contenenti dati sensibili e giudiziari (chiavette, hard disk, cd riscrivibili, ecc.).

Per Noli srl ha attivato un sistema d'autenticazione per ognuno degli incaricati che trattano dati personali. È stato attribuito un codice identificativo (username, user ID) strettamente personale per l'utilizzazione degli strumenti elettronici (di solito personal computer) del sistema informatico della Società.

I codici identificativi sono frequentemente aggiornati, inserendo quelli dei nuovi incaricati e cancellando quelli degli incaricati non più autorizzati. Il sistema di autenticazione prevede l'utilizzo di parole chiave (password) sia a livello di sistema operativo sia a livello di singola applicazione. Il Responsabile IT è incaricato della gestione delle password.
Viene segnalato agli incaricati che la lunghezza della password da utilizzare non deve essere inferiore ad otto caratteri, salvo limitazioni tecniche nei software in uso. Si sollecita l'Incaricato che riceve una password a modificarla al primo utilizzo. Viene segnalato ad ogni Incaricato la necessità di cambiare la password almeno ogni 6 mesi. È prevista una scadenza nella validità di ogni password utilizzata in Per Noli srl. Sono vietate in azienda credenziali di autenticazione (username e password) condivise fra più persone. Le credenziali di autenticazione non utilizzate da almeno sei mesi vengono disattivate. Le credenziali di autenticazione vengono immediatamente revocate in caso di provvedimenti disciplinari o quando si presentano situazioni che possono compromettere la sicurezza. Sono state consegnate istruzioni scritte agli incaricati in merito alle modalità di gestione e di custodia delle password. In caso di prolungata assenza dell'Incaricato, il Soggetto designato al trattamento è autorizzato ad rivelare la password in uso per assicurare la disponibilità dei dati e degli strumenti elettronici. La visualizzazione della password sullo schermo dei personal computer è impedita da tutti i software in uso. Il sistema di identificazione ed autenticazione è operativo anche sui computer portatili.
Gli strumenti informatici sono dotati delle opportune misure difensive in termini di firewall e antivirus.
L'archiviazione delle cartelle e dei file informatici avviene su server. È regolarmente predisposto il backup dei dati.

Analisi dei rischi *Classi di rischio da 1 a 5 (dal meno grave al più grave)*

Rischi	SI/NO	Descrizione dell'impatto sulla sicurezza *(gravità: alta, media, bassa)*
Comportamento degli operatori		
Sottrazione di credenziali di autenticazione	**SI**	Furto dati. Frequenza: **Irrilevante** Gravità **Media** **Classe di rischio 1**
Carenza di consapevolezza, disattenzione o incuria	**SI**	Perdita dei dati. Frequenza: **Bassa** Gravità **Media** **Classe di rischio 2**
Comportamenti sleali o fraudolenti	**SI**	Furto dati. Frequenza **Irrilevante** Gravità **Media** **Classe di rischio 1**
Errore materiale	**SI**	Perdita dati. Frequenza: **Bassa** Gravità **Media** **Classe di rischio 2**
Eventi relativi agli strumenti		
Azione di virus informatici o di programmi suscettibili di recare danno	**SI**	Danneggiamento o perdita dati. Frequenza: **Media** Gravità **Alta** **Classe di rischio 3**
Spamming o tecniche di sabotaggio	**SI**	Danneggiamento, sottrazione o perdita dati. Frequenza: **Bassa** Gravità **Media** **Classe di rischio 2**
Malfunzionamento, indisponibilità o degrado degli strumenti	**SI**	Danneggiamento o perdita dati. Frequenza: **Bassa** Gravità **Bassa** **Classe di rischio 1**
Accessi esterni non autorizzati	**SI**	Danneggiamento o perdita dati. Frequenza: **Irrilevante** Gravità **Alta** **Classe di rischio 2**
Intercettazioni di informazioni in rete	**SI**	Danneggiamento, sottrazione o perdita dati. Frequenza: **Bassa** Gravità **Bassa** **Classe di rischio 1**
Eventi relativi al contesto		
Accessi non autorizzati a locali ad accesso ristretto	**SI**	Danneggiamento, sottrazione o perdita dati informatici/cartacei. Frequenza: **Bassa** Gravità **Alta** **Classe di rischio 3**
Sottrazione di strumenti contenti dati	**SI**	Danneggiamento, sottrazione o perdita dati informatici e cartacei. Frequenza: **Bassa** Gravità **Alta** **Classe di rischio 3**
Eventi distruttivi, naturali o artificiali, nonché dolosi, accidentali	**SI**	Danneggiamento, sottrazione o perdita dati informatici e cartacei. Frequenza: **Irrilevante** Gravità **Alta** **Classe di rischio 2**
Guasto ai sistemi complementari/ausiliari	**SI**	Danneggiamento, sottrazione o perdita dati informatici e cartacei. Frequenza **Irrilevante** Gravità **Alta** **Classe di rischio 2**
Errori umani nella gestione della sicurezza fisica	**SI**	Danneggiamento o perdita dati informatici e cartacei. Frequenza: **Bassa** Gravità **Media** **Classe di rischio 2**

Valutazione d'impatto

Nome / sigla	N° / RIF	Categorie dati e persone	Valutazione
Gestione Personale	001	Personali, sensibili, sanitari e giudiziari Personale dipendente	La distruzione, la sottrazione o la perdita di dati potrebbe compromettere l'operatività dell'organizzazione. Difficilmente tali dati potrebbero arrecare danni significativi alle persone se non, appunto, la violazione della loro privacy. Per alcune tipologie di dati sensibili è quindi necessario prevedere una gestione tempestiva ed efficace dell'eventuale data breach, rafforzando le misure di sicurezza, e migliorando le procedure per il salvataggio e il recupero dati.
Gestione Professionisti	002	Personali, giudiziari Collaboratori e professionisti	La distruzione, la sottrazione o la perdita di dati potrebbe compromettere l'operatività dell'organizzazione. Per alcune tipologie di dati sensibili è necessario prevedere una gestione tempestiva ed efficace dell'eventuale data breach, rafforzando le misure di sicurezza, e migliorando le procedure per il salvataggio e il recupero dati.
Gestione Fornitori	003	Personali Aziende	La distruzione, la sottrazione o la perdita di dati potrebbe compromettere l'operatività dell'organizzazione.
Gestione Clienti	004	Personali Enti e privati	La distruzione, la sottrazione o la perdita di dati potrebbe compromettere l'operatività dell'organizzazione.
Servizi Residenziali	005	Personali, sensibili, sanitari e giudiziari Utenti e famiglie	La distruzione, la sottrazione o la perdita di dati potrebbe compromettere l'operatività dell'organizzazione. Difficilmente tali dati potrebbero arrecare danni significativi alle persone se non, appunto, la violazione della loro privacy. Per alcune tipologie di dati sensibili è quindi necessario prevedere una gestione tempestiva ed efficace dell'eventuale data breach, rafforzando le misure di sicurezza, e migliorando le procedure per il salvataggio e il recupero dati. Da valutare e gestire con più attenzione la dotazione di computer e dispositivi all'interno dei diversi servizi e progetti, implementando il lavoro e l'archiviazione su server e in cloud.
Istruzione e Formazione professionale	006	Personali Utenti	

Misure da predisporre e/o implementare

1. Prevedere ulteriori iniziative formative per il personale dei diversi servizi e progetti, per aumentare il grado di consapevolezza nella gestione dei dati personali e sensibili e per fornire strumenti e linee guida precisi e funzionali rispetto alla specificità e alla tipologia di dati e persone coinvolte.
2. Mettere a disposizione di tutto il personale un archivio in cloud con la documentazione privacy, la normativa di riferimento, la modulistica da utilizzare, sia per gli operatori già in servizio che per i neo assunti
3. Elaborare un Piano di Disaster Recovery, prevedendo prove e simulazioni a cadenza programmata.
4. Mappare i diversi progetti gestiti per conto di enti pubblici e provati, gestiti in autonomia o in raggruppamenti di imprese, al fine di verificare l'esistenza, la correttezza e l'aggiornamento delle nomine a Titolare, Contitolare, Responsabile o Subresponsabile, sia nel caso in cui è Per Noli srl a dover ricevere tale nomina, sia nel caso in cui è Per Noli srl, come Titolare, a dovere nominare altre persone fisiche o giuridiche.