



ASL Lecce

PugliaSalute

Posta Elettronica Ordinaria

Regolamento Per l'Utilizzo



ASL Lecce

PugliaSalute

Posta Elettronica
Ordinaria
Regolamento Per l'Utilizzo

EMISSIONE DEL DOCUMENTO

REGISTRO DELLE VERSIONI

N° Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
V. 1.0	mercoledì 5 aprile 2023		



1. Sommario

1. Sommario.....	2
2. Ambito di Implementazione.....	3
2.1. Premessa - Stato dell'Arte.....	3
2.2. Portale del Dipendente.....	3
2.3. Obiettivi.....	4
2.4. Vincoli Normativi e Regolamentari.....	4
2.5. Definizioni.....	4
3. Posta Elettronica Ordinaria.....	6
3.1. PEO come Strumento di Lavoro.....	6
3.1.1. Posta Elettronica Ordinaria – Implementazioni e Regole Comuni.....	6
3.1.2. Posta Elettronica Ordinaria – Caratteristiche.....	7
3.1.3. Posta Elettronica Ordinaria – Buone Prassi Operative.....	8
3.1.4. Posta Elettronica Ordinaria Istituzionale (Gruppo/Funzione/Servizio/Ruolo).....	8
3.1.5. Posta Elettronica Ordinaria Istituzionale – Attivazione/Disattivazione.....	9
3.1.6. Posta Elettronica Ordinaria Istituzionale – Cambio Password.....	10
3.1.7. Posta Elettronica Ordinaria Nominativa.....	10
3.1.8. Posta Elettronica Ordinaria Nominativa – Attivazione/Disattivazione.....	12
3.1.9. Posta Elettronica Ordinaria Nominativa – Cambio Password.....	13
3.1.10. Politiche di Sicurezza Perimetrali.....	13
3.1.11. Monitoraggio.....	14
3.1.12. Amministratori di Sistema.....	15
3.1.13. Help Desk - Assistenza.....	16
4. Privacy e Responsabilità.....	17
4.1. Informativa per il Trattamento di dati Personali.....	17
4.1.1. Titolare.....	17
4.1.2. Responsabile.....	17
4.1.3. Finalità del Trattamento.....	17
4.1.4. Basi Giuridiche.....	17
4.1.5. Periodo di Conservazione.....	17
4.1.6. Comunicazione dei Dati.....	18
4.1.7. Modalità del Trattamento.....	18
4.1.8. Destinatari.....	18
4.1.9. Diritti Degli Interessati.....	19
4.2. Comportamenti Sanzionabili.....	19



2. Ambito di Implementazione

2.1. Premessa - Stato dell'Arte

La ASL di Lecce, alla data di emissione di questo documento, ha attivato circa 240 caselle di Posta Elettronica Certificata e oltre 1.500 caselle di Posta Elettronica Ordinaria Istituzionale (vedi paragrafo § 3.1.4) a cui sono associati circa 3.100 diritti di accesso attribuiti ai collaboratori aziendali.

Le caselle PEC – in quanto concettualmente associate alla Gestione Documentale ed al Protocollo Informativo – non sono oggetto di trattazione all'interno di questo documento.

Per quanto riguarda le PEO Istituzionali, quanto sopra riportato, indica la loro diffusione pervasiva all'interno della prassi operativa aziendale anche rispetto alla componente di conduzione comune e informazione condivisa (vedi sempre paragrafo § 3.1.4).

2.2. Portale del Dipendente

In questo scenario si inserisce la prossima attivazione del Portale del Dipendente che costituirà interfaccia web per i servizi di seguito esemplificativamente e non esaustivamente individuati per tutti i collaboratori aziendali:

- Repository per cedolino
- Repository per CU
- Repository per cartellini presenze
- Curriculum individuale
- Curriculum aziendale
- Richieste/situazioni di assenze
- Richieste per omessa timbratura
- Richieste per eccedenze e chiusura mese
- Consultazione turni
- Cambio IBAN
- Cambio Residenza
- Cambio Domicilio



2.3. Obiettivi

La Direzione Strategica Aziendale, avendo a riferimento quanto riportato rispettivamente al paragrafo § 2.1 ed al paragrafo § 2.4, intende promuovere la disponibilità delle caselle di Posta Elettronica Ordinaria Nominativa (paragrafo § 3.1.7) per tutti i collaboratori aziendali in servizio.

In particolare l'obiettivo è quello di attivare una sorta di identità/domicilio digitale emesso, attribuito e, di conseguenza, riconosciuto, aziendali (vedi meglio paragrafo § 3.1.7), tanto al fine di rendere di più immediato ed efficace esito, la fruizione di alcuni specifici servizi aziendali da parte dei collaboratori.

2.4. Vincoli Normativi e Regolamentari

Il Garante per la Protezione dei Dati Personali ha più volte precisato la necessità di adottare policy e informative volte a rendere edotti i dipendenti sul trattamento dei dati effettuato dal Titolare tramite la strumentazione e/o i servizi aziendali.

In tale accezione le caselle di Posta Elettronica Ordinaria Nominative rappresentano il domicilio digitale del dipendente, uno "spazio" a disposizione, **in via esclusiva**, della persona: la sua invasione costituisce lesione della riservatezza.

Nel caso in specie il trattamento riguarda sia la raccolta sia la conservazione dei dati gestiti attraverso la casella nominativa oltre che la necessaria procedura di cancellazione sia della casella sia dell'account da eseguirsi in seguito all'interruzione del rapporto di lavoro.

Nell'ambito del rapporto di lavoro tra dipendenti e datore di lavoro, le caselle PEO Nominative sono di sicuro inaccessibili: l'eventuale accesso costituisce reato e violazione delle regole costituzionali sul segreto della corrispondenza.

Tali elementi sono posti alla base sia delle politiche di conduzione e di sicurezza delle caselle PEO Nominative sia dei contenuti informativi, relativi, in particolare, alla destinazione d'uso e ai vincoli d'utilizzo delle medesime, quivi contenuti.

2.5. Definizioni

Termine	Significato
E-mail	Abbreviazione di "electronic mail", la posta elettronica stessa
Mittente	La persona che invia un'e-mail



Destinatario	La persona o il gruppo di persone a cui l'e-mail è indirizzata
Oggetto	Una breve descrizione dell'e-mail che appare nella linea dell'oggetto dell'e-mail
Corpo	Il contenuto principale dell'e-mail, dove il mittente scrive il messaggio.
Allegato	Un file inviato insieme all'e-mail, come un documento, una foto o un video
Spam	E-mail indesiderata o non richiesta che viene inviata in grandi quantità
Filtro antispam	Software che identifica e blocca l'arrivo di e-mail indesiderate nella casella di posta in arrivo
Firma	Il testo personalizzato che compare alla fine di ogni e-mail inviata, contenente solitamente il nome del mittente, il titolo e l'azienda (logo)
Gestore di Posta Elettronica	Il software utilizzato per accedere e gestire la casella di posta elettronica
Server di Posta	Un server che gestisce l'invio e la ricezione delle e-mail attraverso la rete telematica
Crittografia	La crittografia end-to-end è un sistema di sicurezza che crittografa i messaggi in modo che solo il mittente e il destinatario possano leggerli. Ciò significa che laddove un hacker dovesse intercettare il messaggio, non potrebbe leggerlo senza la chiave di decrittazione
Filtro antivirus	Un filtro antivirus è un software che rileva e blocca i virus nelle e-mail. La maggior parte dei servizi di posta elettronica offre un filtro antivirus integrato
Protezione da Phishing	E' un sistema che identifica e blocca gli attacchi di phishing, in cui un hacker cerca di convincere il destinatario a rivelare informazioni personali o a cliccare su un link per installare malware
Backup e Ripristino	Il backup e il ripristino dei dati della posta elettronica sono importanti per proteggere i dati importanti in caso di problemi tecnici o di perdita di dati
Gestione delle politiche di sicurezza	Implementazione di politiche di sicurezza per la posta elettronica, come la gestione delle password, la formazione degli utenti e la definizione di procedure di sicurezza



3. Posta Elettronica Ordinaria

3.1. PEO come Strumento di Lavoro

La totalità delle caselle di posta elettronica ordinaria appartenenti al dominio @asl.lecce.it sono diretta espressione dell'Azienda Sanitaria Locale di Lecce e della sua struttura gerarchico-organizzativa.

Il loro utilizzo è da considerarsi strumentale all'attività lavorativa istituzionale.

La ASL di Lecce ha implementato due tipologie di caselle di posta elettronica ordinaria: le caselle di "Gruppo di Attività/Funzione/Servizio/Ruolo" individuate come **Caselle Istituzionali** e le caselle attribuite a tutto il personale dipendente individuate come **Caselle Nominative**.

Le peculiarità e le differenze tra le due tipologie di caselle sono di seguito meglio esplicitate.

3.1.1. POSTA ELETTRONICA ORDINARIA – IMPLEMENTAZIONI E REGOLE COMUNI

L'accesso alle caselle PEO aziendali è effettuato collegandosi all'indirizzo <https://mail.asl.lecce.it> utilizzando, per il Login, le specifiche credenziali custodite dal collaboratore.

La conduzione del servizio di posta elettronica ordinaria è effettuato attraverso l'utilizzo di risorse aziendali ed è sottoposto a comuni regole di sicurezza esplicitate nel paragrafo § 3.1.10.

Tutte le caselle PEO sono standardizzate pur nelle peculiarità delle due diverse tipologie individuate: la possibilità di modificare il layout delle stesse è, di fatto, inibito.

Sempre per motivi di sicurezza e di conduzione tecnica, è inibito l'utilizzo dei "Client" di posta elettronica quali, esemplificativamente, "Windows Live Mail", "Mozilla Thunderbird", ecc. : la gestione della posta è effettuato solo attraverso l'interfaccia web raggiungibile all'indirizzo in precedenza riportato.

La totalità della messaggistica scambiata in ingresso ed in uscita attraverso le caselle PEO aventi estensione @asl.lecce.it sono sottoposte alle politiche di backup – frequenza al mini-



mo giornaliera – ed alla implementazione della “business continuity” analogamente a quanto avviene per tutti i servizi software resi disponibili aziendalmente.

Per quanto attiene al processo di autenticazione le policy di sicurezza sono aggiornate attraverso indicazioni fornite dal Dirigente Responsabile di “Amministrazione Digitale Sicurezza e Privacy” (autenticazione a più fattori - uso di token con certificato digitale - chiavi di sicurezza) avendo a riferimento il bilanciamento degli interventi tra nuove minacce alla sicurezza e contro misure realmente implementabili.

3.1.2. POSTA ELETTRONICA ORDINARIA – CARATTERISTICHE

Per quanto l’evoluzione dei sistemi di gestione e di trasmissione dell’informazione abbiano compiuto notevoli progressi, la Posta Elettronica Ordinaria ha caratteristiche tecniche per le quali può essere classificata come strumento di lavoro non totalmente affidabile e parzialmente insicuro.

Tali considerazioni nascono da “mancanze” proprie dei protocolli tecnici di implementazione della PEO in conseguenza dei quali:

- non è possibile avere certezza dell’avvenuta consegna del messaggio mail
- non è possibile avere certezza che il messaggio e gli allegati che partono dal mittente sono esattamente quelli che arrivano al destinatario
- non è possibile sapere se il messaggio è stato intercettato e “letto”

Le caratteristiche sopra riportate sono proprie della PEC – Posta Elettronica Certificata – la cui genesi ha sopperito a dette mancanze.

La Posta Elettronica Ordinaria, di conseguenza:

- **non può essere utilizzata come strumento di notifica**
- **non dovrebbe essere usata come strumento di trasmissione di “dati sensibili”** (opinioni politiche, religiose, affiliazioni sindacali, inclinazioni sessuali, stato di salute) – se non in presenza di specifici accorgimenti tecnici -
- **non può essere sottoposta a registrazione di protocollo (protocollazione)**

E’ possibile approfondire tali informazioni fruendo della documentazione e delle registrazioni di specifici Webinar sull’argomento disponibili sulla Intranet Aziendale all’indirizzo



<https://intranet.asl.lecce.it>

3.1.3. POSTA ELETTRONICA ORDINARIA – BUONE PRASSI OPERATIVE

Pur in presenza di filtri di sicurezza (§ 3.1.10) è possibile ricevere mail da mittenti sconosciuti e/o che contengono messaggi inusuali, ovvero provenienti da mittenti noti ma che contengono allegati sospetti: al fine di evitare qualsiasi possibile infezione da virus/malware, si raccomanda di cancellare i messaggi **senza aprirli** ovvero allertare l'Help Desk interno (§ 3.1.13) per l'effettuazione di una verifica e/o bonifica del messaggio ricevuto.

Quale misura volta a prevenire possibili utilizzi illeciti della casella PEO, i collaboratori - in via cautelativa – sono tenuti ad allertare l'Help Desk quando, ai messaggi ricevuti, siano allegati file eseguibili e/o di natura incomprensibile e/o sconosciuta.

E' fissato un limite alla dimensione dei messaggi comprensivi degli allegati sia in partenza sia in arrivo. I messaggi che superano il limite non vengono accettati dal sistema di posta.

E' bene sottolineare che la casella di posta elettronica ordinaria è uno strumento di lavoro e come tale deve essere utilizzata esclusivamente ai fini dello svolgimento dell'attività lavorativa.

Non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, forum, newsletter o a qualsiasi forma di iscrizione a servizi **non** attinenti all'attività lavorativa.

E' necessario porre una particolare attenzione – e, eventualmente, richiedere un supporto interpretativo da parte dell'Help Desk – in presenza di mail il cui significato e le cui richieste possono corrispondere a messaggistica di phishing.

3.1.4. POSTA ELETTRONICA ORDINARIA ISTITUZIONALE (GRUPPO/FUNZIONE/SERVIZIO/RUOLO)

Le caselle di Posta Elettronica Ordinaria Istituzionale sono, come tali, destinate ad attività lavorativa ordinaria propria del gruppo di lavoro, della funzione e/o servizio di appartenenza ovvero del ruolo aziendalemente ricoperto.



ASL Lecce

PugliaSalute

Posta Elettronica Ordinaria Regolamento Per l'Utilizzo

Sono strumentali all'espletamento dei propri compiti ed attività all'interno del sotto insieme organizzativo: come tali sono destinate ad un utilizzo condiviso da parte di più utenti che accedono alla casella - ognuno con le proprie credenziali -.

E' possibile che, per motivi di servizio e/o di appartenenza, lo stesso collaboratore abbia accesso a più di una casella PEO: in tal caso, utilizzando le uniche credenziali a sua disposizione, egli ritroverà, in una unica interfaccia, l'elenco delle caselle a cui è associato per diritto.

Per l'accesso alla casella PEO Istituzionale attraverso il portale <https://mail.asl.lecce.it>, è necessario utilizzare, **esemplificativamente**, le seguenti credenziali:

Nome Utente: PLLPNC23D41E506C → Codice Fiscale

Password: L@w0rdch3n0np1ac3! → Password autodeterminata

In tale logica la casella PEO Istituzionale contiene una "firma" che riporta il Logo Aziendale, la struttura di appartenenza, l'eventuale sotto unità organizzativa e l'indicazione del Cognome e Nome del collaboratore a cui è stato associato il "diritto d'utilizzo".

3.1.5. POSTA ELETTRONICA ORDINARIA ISTITUZIONALE – ATTIVAZIONE/DISATTIVAZIONE

Per quanto indicato al paragrafo § 3.1.4 la PEO Istituzionale è strumentale all'attività effettuata all'interno dell'organizzazione aziendale: è il Dirigente/Direttore Responsabile della struttura a stabilire per quali esigenze funzionali e/o organizzative è necessario utilizzare la casella PEO Istituzionale.

Adoperando lo specifico modulo – disponibile all'indirizzo <https://intranet.asl.lecce.it> - il Dirigente/Direttore Responsabile di struttura suggerisce una nomenclatura da attribuire alla nuova casella e indica gli estremi dei collaboratori ai quali deve essere associato il diritto di accesso ed utilizzo della medesima.

Il modulo deve essere inviato all'indirizzo amministrazionedigitale@asl.lecce.it : il Dirigente Responsabile della struttura "Amministrazione Digitale Sicurezza e Privacy" vaglia la richiesta, standardizza la nomenclatura nel caso di richieste relative a nuove caselle, ed autorizza l'attivazione e l'emissione delle credenziali nei confronti dei collaboratori individuati.

Non esiste un limite tecnico e/o numerico rispetto all'attivazione delle caselle PEO Istituzionali se non dettato dai vincoli organizzativi e/o di opportunità stabiliti dal Dirigente/Direttore Responsabile della struttura organizzativa interessata.



Pari prassi operativa deve essere seguita nel momento in cui il collaboratore - perché ha cambiato struttura di appartenenza e/o gruppo di attività e/o ruolo, ecc. - perde il diritto all'accesso alla specifica PEO Istituzionale e ne deve essere richiesta disabilitazione, sempre attraverso lo specifico modulo.

3.1.6. POSTA ELETTRONICA ORDINARIA ISTITUZIONALE – CAMBIO PASSWORD

Le politiche di sicurezza aziendali che, al più del possibile, ottemperano alle prescrizioni della vigente normativa privacy ed alle linee guida nazionali ed internazionali sull'argomento, stabiliscono che, la password associata alle credenziali necessarie per l'accesso alla/e casella/e di Posta Elettronica Ordinaria Istituzionale, debba avere scadenza pari a 90 gg solari.

Il sistema di gestione invia, all'indirizzo mail indicato dal collaboratore ovvero all'indirizzo della PEO Nominativa attivata aziendali, una serie di messaggi di "ALERT" che informano l'interessato della prossima scadenza della password.

Nel caso in cui la stessa non viene aggiornata – con prassi operativa di seguito indicata – la casella PEO Istituzionale non risulterà più accessibile da parte del collaboratore.

La prassi operativa per l'aggiornamento della password prevede i seguenti passaggi:

1. Collegarsi al sito Intranet raggiungibile all'indirizzo <https://intranet.asl.lecce.it> **necessariamente da un dispositivo collegato alla rete aziendale**
2. Cliccare sulla voce di Menù posizionato in alto → "Lavoro Agile" e, successivamente sulla voce → "Cambio Password"
3. Procedere secondo quanto richiesto dallo specifico modulo software impostando la nuova password nel rispetto delle prescrizioni stabilite

3.1.7. POSTA ELETTRONICA ORDINARIA NOMINATIVA

La attribuzione – d'ufficio – di una casella di Posta Elettronica Ordinaria Nominativa - nomi.cognomi@asl.lecce.it - per tutti i nuovi dipendenti corrisponde alla assegnazione di una identità/domicilio digitale riconosciuto e utilizzabile – come tale – aziendali.

Tali caselle sono totalmente separate – sia concettualmente sia nelle modalità di accesso e di utilizzo – dalle caselle PEO Istituzionali.



Per quanto riportato ai paragrafi § 2.4 e § 3.1.4 la casella PEO Nominativa è destinata ai seguenti principali usi aziendali:

- destinataria di informative e/o comunicazioni di carattere generale
- destinataria dell'invio delle credenziali di attivazione e/o utilizzo di servizi e/o applicativi aziendali (Gestione Documentale, Protocollo Informatico, Gestione Presenze, MOSS, ecc.)
- destinataria dell'invio dei messaggi di alert relativi alla scadenza della password
- destinataria di informative relative alla formazione
- domicilio digitale del collaboratore destinatario da parte dell'Ufficio Formazione

Di seguito sono riportate le regole comportamentali relative all'utilizzo della casella PEO Nominativa:

1. La casella è personale: non è possibile condividere i messaggi in attività – di natura procedimentale - di gruppo e/o funzione aziendali in quanto la fruizione della casella è uni-nominativa
2. Ogni utente è totalmente responsabile delle informazioni che transitano e di quanto viene effettuato attraverso la propria casella PEO Nominativa
3. L'accesso alla casella è strettamente personale e non può essere delegato ad altri
4. In caso di assenza prolungata, laddove la casella nominativa fosse stata utilizzata per attività procedimentale vincolata a tempi ristretti e/o stabiliti, il collaboratore risponderà personalmente dell'eventuale ritardo derivante dal mancato accesso all'informazione da parte degli interessati - interni e/o esterni – dal procedimento
5. Quanto riportato nelle mail impegna sia il mittente sia l'azienda nei confronti dei destinatari con riguardo ai contenuti ed agli allegati dei messaggi
6. L'azienda si riserva di rivalersi sul collaboratore nel caso in cui il non corretto utilizzo della casella nominativa violi la normativa vigente e/o sia contrario alla regolamentazione, alle direttive ed agli interessi dell'Azienda
7. Non è consentito l'utilizzo dell'indirizzo di PEO Nominativa per la partecipazione a chat, newsletter o a qualsiasi forma di iscrizione a servizi **NON** attinenti all'attività lavorativa
8. Ogni casella ha una dimensione massima - fissata a 2Gb - raggiunta la quale non sarà più possibile utilizzarla



Il combinato disposto rispetto a quanto riportato, in particolare, ai punti 1 - 3 – 4, e ai paragrafi § 3.1.10 - § 2.1 , rendono la casella Nominativa non adatta ad un uso “istituzionale”, bensì destinata a ricevere informazioni relative a servizi aziendali, a corsi di formazione, newsletter o a qualsiasi ulteriore forma di servizio attinente all'attività lavorativa ed alla crescita professionale.

In tale logica la casella PEO Nominativa contiene una “firma” che riporta l’indicazione del solo Logo Aziendale e del Cognome e Nome del collaboratore a cui la stessa è attribuita.

In particolare, per l’accesso alla casella PEO Nominativa, è necessario utilizzare, **esemplificativamente**:

Nome Utente: pinco.pallo@asl.lecce.it → Indirizzo della Casella PEO Nominativa

Password: L@w0rdch3m1p1ac3! → Password autodeterminata

Laddove l’assenza del collaboratore si prolunghi per un intervallo temporale considerato non compatibile per l’attività di servizio e/o comunque rilevante, il Dirigente/Direttore Responsabile di Struttura produrrà specifica richiesta indirizzata al Dirigente Responsabile della struttura Amministrazione Digitale Sicurezza e Privacy affinché l’Help Desk possa accedere alla Casella Nominativa del lavoratore assente, tanto al fine di attivare l’invio automatizzato di un messaggio (risponditore automatico) - con contenuti concordati - alla ricezione di tutte le mail destinate alla specifica casella.

Tale intervento sarà sottoposto a tutti i vincoli stabiliti al paragrafo § 3.1.11 .

3.1.8. POSTA ELETTRONICA ORDINARIA NOMINATIVA – ATTIVAZIONE/DISATTIVAZIONE

La casella di Posta Elettronica Ordinaria Nominativa è associata all’intero periodo lavorativo del collaboratore aziendale e, di conseguenza, le tempistiche: la casella viene attivata – d’ufficio – all’atto della sottoscrizione del contratto di lavoro e viene disabilitata all’accesso – per essere, successivamente, cancellata – nel momento in cui il collaboratore è collocato a riposo (quiescenza).

Il periodo intercorrente tra la disabilitazione all’accesso e la cancellazione della casella è fissato a 60 gg solari, periodo stimato come congruo per consentire eventuali interventi di manutenzione straordinaria da parte dell’Help Desk.



Il periodo di conservazione dei dati trattati è pari all'intero periodo lavorativo del collaboratore a cui devono essere sommati 60 gg.

3.1.9. POSTA ELETTRONICA ORDINARIA NOMINATIVA – CAMBIO PASSWORD

Le politiche di sicurezza aziendali – in considerazione del fatto che la “conduzione” della casella è in capo al collaboratore interessato – non stabiliscono alcuna scadenza temporale per la password associata alle credenziali di accesso alla medesima PEO Nominativa.

Buona regola è uniformarsi a quanto stabilito per la PEO Istituzionale e procedere per un “cambio password” non oltre i 90 gg solari dall'ultimo aggiornamento effettuato.

La prassi operativa per l'aggiornamento della password prevede i seguenti passaggi:

1. Collegarsi al sito di accesso della mail all'indirizzo <https://mail.asl.lecce.it>
2. Accedere alla casella/e utilizzando le proprie credenziali
3. Posizionarsi in alto a destra (in corrispondenza della indicazione del nome della casella) e cliccare sul triangolo rivolto in basso
4. Selezionare la voce “Cambia password”
5. Inserire le informazioni richieste all'interno del Pop-Up (finestra a comparsa) per aggiornare la password (rispettando criteri minimi quali lunghezza di almeno 10 caratteri alfanumerici con combinazione di minuscole e maiuscole e presenza di almeno un carattere numerico)

N.B.: E' fortemente consigliato – vista la modalità con la quale sono rese disponibili le credenziali - procedere per il cambio della password al primo accesso alla casella PEO Nominativa

3.1.10. POLITICHE DI SICUREZZA PERIMETRALI

L'Azienda Sanitaria ha attivato una serie di interventi tecnico organizzativi tesi all'innalzamento del livello di sicurezza logica con riguardo alla totalità dei “dispositivi” che insistono sulla Rete Telematica ed all'insieme dei Servizi Software che, attraverso la medesima, sono erogati aziendali.

La sicurezza perimetrale è specificamente realizzata applicando al “bocchettone” virtuale, attraverso cui l'Azienda interagisce con il mondo esterno – Intranet – Infranet – Extranet -



una serie di implementazioni tecnico organizzative individuate complessivamente come “Sicurezza Perimetrale”.

Con particolare riguardo alla Posta Elettronica Ordinaria due principali interventi sono stati effettuati per “l’analisi” dei messaggi di Posta in ingresso ed uscita.

Il primo attiene alla verifica della provenienza dei messaggi promuovendoli come “consegnabili” (trusted) solo in presenza di un mittente censito in una White List e/o non appartenente ad una Black List: entrambe le liste sono aggiornate – in tempo reale – a livello internazionale. Tale implementazione assolve anche a funzionalità di filtro antispam.

Il secondo verifica la presenza o meno di software malevolo in allegato a qualsiasi mail, forzando l’esecuzione di tale allegato e verificandone gli esiti in un ambiente protetto che non può – di fatto – essere “contagiato”.

In entrambe le situazioni se il messaggio è considerato non adeguato è inserito in una specifica lista di quarantena ovvero semplicemente cancellato e, comunque, non consegnato al/ai destinatari aziendali.

3.1.11. MONITORAGGIO

L’Azienda Sanitaria non utilizza le tecnologie per il monitoraggio dei Sistemi di Elaborazione e di Gestione della Rete Telematica ai fini del controllo a distanza dei lavoratori (artt. 113, 114, 171 Codice Privacy - artt. 4 e 8, L. 20 maggio 1970, n.300 – Statuto dei Lavoratori così come modificato dal D. Lgs. 151/2015 [Jobs Act]), se non nei limiti consentiti dalla vigente normativa, e, comunque, previa specifica informativa ai dipendenti interessati.

Gli Amministratori di Sistema (vedi paragrafo § 3.1.12), attraverso l’utilizzo di apposita strumentazione e/o software specializzati, sono in grado di effettuare un approfondito monitoraggio relativamente all’utilizzo dei sistemi informativi e dei servizi software erogati aziendali.

A titolo esemplificativo e non esaustivo il monitoraggio riguarda gli:

- Accessi alla rete --> codice utente, data e ora evento, operazione, ingresso/uscita (login/logout)
- Utilizzo di Internet --> indirizzo IP postazione origine, indirizzo IP, sito Internet destinatario, data e ora evento



- Accessi agli applicativi --> codice utente, data e ora evento, tipo di operazione

Sempre all'interno del perimetro fissato al paragrafo § 3.1.12 e delle politiche di sicurezza e conduzione dettate dalla struttura Amministrazione Digitale Sicurezza e Privacy, gli Amministratori di Sistema sono nella condizione di effettuare una analisi aggregata del traffico di rete e della collegata tipologia di utilizzo.

Con specifico riferimento al servizio di Posta Elettronica Ordinaria gli Amministratori di Sistema, oltre alle informazioni relative all'utilizzo (postazione di lavoro, accesso/disconnessione, numero di messaggi in ingresso/uscita, ecc.), detengono la possibilità tecnica di accedere – anche al contenuto - delle singole caselle.

3.1.12. AMMINISTRATORI DI SISTEMA

Gli Amministratori di Sistema sono tenuti al segreto d'ufficio.

Tutte le informazioni a cui gli stessi possono avere accesso - durante l'espletamento delle attività - non possono essere comunicate ad alcuno e non possono essere memorizzate su supporti differenti da quelli d'origine e dai supporti utilizzati per il backup.

Per quanto attiene al servizio di posta elettronica ordinaria - gli Amministratori di Sistema - non accedono ai contenuti dei messaggi se non nel caso in cui l'intervento è richiesto dal Responsabile di Struttura (PEO Istituzionale), ovvero dal diretto interessato (PEO Nominativa).

Per motivate esigenze di natura tecnica e/o legale, esplicitate e comunicate dal Responsabile della struttura "Amministrazione Digitale Sicurezza e Privacy", le due condizioni sopra riportate sono sottoposte a deroga.

A salvaguardia di tutti gli interessati, l'Azienda Sanitaria ottempera all'obbligo di tenere traccia degli accessi logici effettuati dagli Amministratori di Sistema alla totalità dei "sistemi" dagli stessi amministrati.

Tali registrazioni hanno caratteristiche di completezza, inalterabilità e consentono una verifica relativamente alle caratteristiche di integrità e sono conservate per un periodo di tempo pari a 6 mesi.

Le registrazioni comprendono i riferimenti temporali, la descrizione dell'evento che le ha generate e vengono conservate in forma crittografata, tanto anche al fine di soddisfare quanto



indicato dal Garante per la Protezione dei Dati Personali, nel provvedimento del 27 novembre 2008, che prevede un "due diligence" in capo al Titolare relativamente agli "accorgimenti e misure, tecniche e organizzative, volti ad agevolare l'esercizio dei doveri di controllo da parte del titolare" sulle mansioni svolte dagli amministratori di sistema designati.

3.1.13. HELP DESK - ASSISTENZA

Le richieste di assistenza effettuate verso il servizio di Help Desk seguono due differenti modalità rispetto alla richiesta di intervento da parte degli Amministratori di Sistema:

1. Per la PEO Istituzionale è necessario procedere inviando un messaggio – attraverso indirizzo appartenente al dominio @asl.lecce.it – alla casella supportomail.istituzionale@asl.lecce.it
2. Per quanto attiene alla PEO Nominativa è necessario procedere inviando un messaggio – attraverso indirizzo appartenente al dominio @asl.lecce.it – alla casella supportomail.nominativa@asl.lecce.it



4. Privacy e Responsabilità

4.1. Informativa per il Trattamento di dati Personali

4.1.1. TITOLARE

Titolare del trattamento dei Tuoi dati personali è l'Azienda Sanitaria Locale di Lecce, con sede in via Miglietta n. 5, Telefono 0832-215111, e-mail: dirgen@asl.lecce.it, PEC: protocollo@pec.asl.lecce.it

4.1.2. RESPONSABILE

Il Responsabile per la Protezione dei dati Personali (RPD), individuato dal Titolare ai sensi dell'art. 37 del "GDPR", è contattabile al seguente indirizzo mail: dpo@asl.lecce.it

4.1.3. FINALITÀ DEL TRATTAMENTO

I Tuoi dati personali saranno trattati per la finalità di implementazione e gestione del servizio di Posta Elettronica Ordinaria Istituzionale e Nominativa. Tale servizio è considerato strategicamente rilevante ed è affidato a società terza specificamente individuata.

4.1.4. BASI GIURIDICHE

Per le finalità sopra indicate la base giuridica del trattamento è costituita dal beneplacito espresso, in assenza di alternative proporzionalmente attuabili, procedendo all'accesso alla casella di posta elettronica ordinaria utilizzando le credenziali a tal fine ricevute.

4.1.5. PERIODO DI CONSERVAZIONE

I Tuoi dati sono conservati per il tempo necessario al perseguimento delle finalità per le quali sono trattati, fatto salvo il maggior tempo necessario per adempiere ad obblighi di legge, in



ragione della natura del dato o del documento o per motivi di interesse pubblico o per l'esercizio di pubblici poteri.

4.1.6. COMUNICAZIONE DEI DATI

Il conferimento dei dati ai fini dell'erogazione del servizio di posta elettronica ordinaria (Istituzionale e Nominativa) è obbligatorio. Il rifiuto di fornire i dati richiesti comporta l'impossibilità ad accedere al servizio medesimo.

4.1.7. MODALITÀ DEL TRATTAMENTO

Il trattamento dei dati sarà effettuato in forma automatizzata e/o manuale, sia informatica che cartacea, con modalità e strumenti volti a garantire la massima sicurezza e riservatezza, nonché l'esattezza, l'aggiornamento e la pertinenza dei dati personali rispetto alla finalità dichiarata.

4.1.8. DESTINATARI

Esclusivamente per le finalità sopra specificate, tutti i dati raccolti ed elaborati potranno essere comunicati a figure interne autorizzate al trattamento in ragione delle rispettive mansioni e secondo i profili attribuiti agli stessi, nonché, nei casi stabiliti da leggi, regolamenti o per l'espletamento di funzioni istituzionali e/o di servizio, alle seguenti categorie di Soggetti esterni:

- Soggetti qualificati ad intervenire in controversie in cui è parte l'Azienda (compagnie assicurative, legali e consulenti, etc.) al fine di tutelare gli operatori e l'Azienda stessa nelle ipotesi di responsabilità
- Autorità Giudiziaria e/o Autorità di Pubblica Sicurezza, nei casi espressamente previsti dalla legge
- Imprese esterne alle quali è affidato il compito di svolgere specifiche operazioni necessarie per garantire i servizi dell'Azienda, nei limiti strettamente pertinenti alle finalità di cui sopra, tutti previamente nominati quali "Responsabili" del trattamento



4.1.9. DIRITTI DEGLI INTERESSATI

Sono garantiti i diritti di cui agli artt. 15 - 22 del "GDPR": chiedere all'Azienda di accedere ai propri dati personali e di rettificarli se inesatti, di cancellarli o limitarne il trattamento se ne ricorrono i presupposti, oppure opporsi per specifici e legittimi motivi. Viene garantito altresì il diritto di revocare il consenso prestato per le finalità di trattamento che lo richiedono, ferma restando la liceità del trattamento effettuato sino al momento della revoca.

Oltre ad esercitare i diritti sopra elencati contattando il Responsabile per la Protezione dei Dati (vedi sopra), si ha anche il diritto di proporre reclamo all'Autorità di Controllo competente in materia, Garante per la Protezione dei Dati Personali (www.garanteprivacy.it).

4.2. **Comportamenti Sanzionabili**

L'inosservanza delle presenti disposizioni potrà comportare conseguenze sul piano civile, penale e disciplinare. Le sanzioni disciplinari verranno contestate nel rispetto delle procedure previste dalle disposizioni legislative vigenti nonché dai Contratti Collettivi di categoria e dai Regolamenti e Codici di Comportamento Aziendali emanati in materia, con i provvedimenti previsti dai rapporti contrattuali in vigore e dalla vigente legislazione civile e penale