PROVINCIA DI PESCARA

DECRETO DEL PRESIDENTE

L'anno duemiladiciotto il giorno 17 del mese di Maggio nel palazzo della Provincia

IL PRESIDENTE

ANTONIO DI MARCO

con l'assistenza del Segretario Generale, Avv. CARLO PIROZZOLO

ha adottato il seguente decreto.

N° Decreto: **DDP-2018-0000066**

OGGETTO:

Linee Guida disciplinanti l'utilizzo degli strumenti e dei servizi informatici, di internet, della posta elettronica ordinaria e certificata della Provincia di Pescara

IL PRESIDENTE

Premesso che le risorse ICT costituiscono il principale strumento di lavoro posto a disposizione dei dipendenti delle Pubbliche Amministrazioni;
considerato che le Pubbliche Amministrazioni, in quanto datori di lavoro, sono tenute ad assicurare la funzionalità ed il corretto impiego degli strumenti ICT da parte dei propri dipendenti, definendone le modalità di utilizzo nell'organizzazione dell'attività lavorativa ed adottando le misure necessarie a garantire la sicurezza, la disponibilità e l'integrità dei sistemi informativi;
preso atto che:

- la Direttiva 2/09 del Dipartimento della Funzione Pubblica invita le Pubbliche Amministrazioni ad adottare tutte le misure di informazione, controllo e verifica consentite al fine di regolamentare la fruizione delle risorse ICT e responsabilizzare i dipendenti nei confronti di eventuali utilizzi non coerenti con la prestazione lavorativa e non conformi alle norme che disciplinano il lavoro alle dipendenze delle Pubbliche Amministrazioni;
- le Deliberazioni emanate in materia da parte del Garante per la protezione dei dati personali, ed in particolare la Deliberazione n 13 del 1 marzo 2007, hanno fornito le linee guida per l'utilizzo nei luoghi di lavoro della posta elettronica e di Internet;

valutato che è necessario contemperare l'utilizzo degli strumenti ICT con la protezione dei dati personali, tenuto conto che:

- compete al datore di lavoro assicurare la funzionalità ed il corretto impiego di tali mezzi da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in tema di diritti e relazioni sindacali;
- spetta ai datori di lavoro adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e di dati anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità: l'utilizzo di internet da parte dei lavoratori può infatti formare oggetto di analisi e profilazione mediante elaborazione di log file della navigazione web ottenuti tramite vari strumenti di registrazione delle informazioni;

rilevato, per quanto sopra esposto, che è opportuno adottare una policy interna rispetto al corretto uso degli strumenti informatici, della posta elettronica e di internet, che indichi le modalità di utilizzo dei suddetti mezzi da parte dei lavoratori;
dato atto che, nel solco delle disposizioni normative vigenti, e nell'ottica dell'applicazione del Regolamento Europeo 679/2016, è stato predisposto dalla responsabile del Servizio Sistemi Informativi e Agenda Digitale, l'allegato documento avente per oggetto *" Linee Guida disciplinanti l'utilizzo degli strumenti e dei servizi informatici, di internet, della posta elettronica ordinaria e certificata dell'Amministrazione Provinciale di Pescara"*
rilevato altresì che le linee guida formulate, oltre ad essere conformi alla normativa vigente, rispondono agli indirizzi dell'amministrazione in ordine all'utilizzo degli strumenti ICT, alla promozione dell'innovazione e alla progressiva informatizzazione dei procedimenti amministrativi nel pieno rispetto dei principi sul corretto utilizzo degli strumenti da parte dei dipendenti cui va garantita la tutela dei dati personali;
dato atto che il presente provvedimento non comportando nè impegno di spesa nè diminuzione di entrata non richiede il parere di regolarità contabile , espresso ai sensi delll'art 49 dlgs 267/2000, dal Dirigente del Settore Economico Finanziario;
acquisito il parere di regolarità tecnica espresso ai sensi e per gli effetti dell'art. 49, comma 1 del TUEL;

visto lo Statuto dell'ente, approvato con Delibera di Consiglio n. 38 del 20/11/2014, e in particolare l'art. 8 che stabilisce che "*Nell'esercizio delle competenze di cui ai commi precedenti, il Presidente, in particolare: a) approva il regolamento sull'ordinamento degli uffici e dei servizi*;"

DECRETA

1. che quanto in narrativa costituisce parte integrante e sostanziale del presente provvedimento;
2. di approvare il documento avente per oggetto *" Linee Guida disciplinanti l'utilizzo degli strumenti e dei servizi informatici, di internet, della posta elettronica ordinaria e certificata dell'Amministrazione Provinciale di Pescara"* secondo il testo allegato al presente provvedimento e di cui costituisce parte integrante;
3. di dare atto che il presente provvedimento con riferimento all'area funzionale di appartenenza non è classificato a rischio P.T.C.P;
4. di dare atto altresì che è richiesta la pubblicazione nella sezione Amministrazione Trasparente ai sensi del Dlgs 33/2013
5. di dichiarare il presente decreto immediatamente eseguibile ai sensi dell'art. 134, comma 4 del D.Lgs. 18/08/2000 n. 267.

Linee Guida disciplinanti l'utilizzo degli strumenti e dei servizi informatici, di internet, della posta elettronica ordinaria e certificata dell'Amministrazione provinciale di Pescara

INDICE

INTRODUZIONE

Le realtà professionali sono andate caratterizzandosi in questi ultimi anni per l'elevato uso delle tecnologie informatiche che se da un lato hanno consentito l'introduzione di innovative tecniche di gestione, dall'altro hanno anche dato origine a numerose problematiche relative all'utilizzo degli strumenti forniti ai propri collaboratori per lo svolgimento delle mansioni e compiti affidati. In questo senso, viene fortemente sentita la necessità di porre in essere adeguati sistemi di controllo sull'utilizzo di tali strumenti da parte dei dipendenti/collaboratori e di sanzionare conseguentemente quegli usi scorretti che, oltre ad esporre l'Amministrazione provinciale a rischi tanto patrimoniali quanto penali, possono di per sé considerarsi contrari ai doveri di diligenza e fedeltà previsti dagli artt. 2104 e 2105 del Codice Civile. I controlli sull'uso degli strumenti informatici, tuttavia, devono garantire tanto il diritto del datore di lavoro di proteggere la propria organizzazione, essendo i computer strumenti di lavoro la cui utilizzazione personale è preclusa, quanto il diritto del lavoratore a non vedere invasa la propria sfera personale, e quindi il diritto alla riservatezza ed alla dignità come sanciti dallo Statuto dei lavoratori e dal Codice sulla Privacy. lE LINEE GUIDA (quali quello proposto) ed in genere le "policies" che dettano le regole sull'uso degli strumenti informatici e telematici, non sono comunque sostitutive della procedura prevista dal 2° comma dell'art. 4 dello Statuto dei lavoratori in materia di controlli leciti, nei casi in cui questa procedura sia necessaria. Tuttavia, proprio l'adozione di un disciplinare che evidenzi la natura non personale della casella di posta assegnata e ne definisca le modalità d'uso ed i possibili controlli, rappresenta un utile strumento per evitare la configurabilità di tale reato. Alla luce delle considerazioni sopra espresse e tenuto opportunamente conto delle Linee guida emanate dall'Autorità Garante per la protezione dei dati personali, con propria deliberazione n. 13 del 1 Marzo 2007, sulla disciplina della navigazione in internet e sulla gestione della posta elettronica nei luoghi di lavoro, il Servizio Sistemi Informativi e Agenda Digitale ha elaborato le presenti Linee Guida al fine di disciplinare le condizioni per il corretto utilizzo degli strumenti informatici da parte dei dipendenti e/o collaboratori. Le Linee Guida di seguito proposte, essendo rilevanti ai fini delle eventuali azioni disciplinari attivabili dal datore di lavoro nei confronti del dipendente, sono state redatte tenendo opportunamente conto sia delle disposizioni contenute nella Legge. n. 300/1970 in tema di provvedimenti disciplinari, sia delle indicazioni emerse nelle prime sentenze di merito e di legittimità pronunciatesi sull'argomento. Vengono inoltre considerati gli specifici obblighi previsti dal Codice della Privacy (D.Lgs. n. 196/2003 e successive modifiche ed integrazioni) nonché gli obblighi previsti dal disciplinare tecnico sulle misure minime di sicurezza allegato allo stesso Codice.

Con riferimento alla normativa in tema di protezione dei dati personali, si ricorda come il Codice della Privacy stabilisca che l'attività di controllo debba essere rispettosa dei principi fondamentali di "proporzionalità" (art. 3), debba avvenire nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato (art. 2) e soprattutto, che di tale attività, debba essere fornita adeguata e preventiva informativa (art. 13).

Lo schema di Linee Guida ha lo scopo di informare gli interessati sulle finalità del controllo e sulle specifiche tecnologie adottate per effettuarlo. Particolare attenzione dovrà comunque venir prestata all'attività di controllo della navigazione internet qualora, mediante l'individuazione dei contenuti dei siti visitati, si determini un trattamento di dati sensibili per i quali deve sempre essere rispettato il principio dell'indispensabilità (art. 26, 4°comma lett. c) del Codice). Tra l'altro, se correttamente applicate e fatte rispettare, le Linee Guida possono risultare anche un efficace

strumento per limitare il rischio di insorgenza della responsabilità contabile, prevista dal D.Lgs. n. 165/ 2001.

TITOLO I

I.1 Oggetto e ambito di applicazione/finalita' del Linee Guida

Le presenti Linee Guida contengono disposizioni riguardanti i corretti modi d'uso della rete informatica dell'ente Provincia di Pescara e di tutte le risorse informatiche, in conformità e nel rispetto di quanto previsto dalla specifica normativa di settore e dalle ulteriori disposizioni emanate dall'ente stesso.

Finalità principale delle presenti Linee Guida consiste nel disciplinare le modalità di gestione e di utilizzo delle risorse informatiche, ed in particolare della Posta Elettronica Ordinaria e della Posta Elettronica Certificata (PEC) nell'ambito dell'Amministrazione provinciale di Pescara, ai sensi e per gli effetti della normativa di settore, e nello specifico ai sensi del DLgs 7 marzo 2005, n 82 (Codice dell'Amministrazione Digita - CAD -), successive modifiche e normativa connessa.

Le presenti Linee Guida si applicano a tutto il personale dipendente dell'Amministrazione provinciale di Pescara, senza distinzione di ruolo o livello, ed a tutti i collaboratori, a prescindere dal ruolo contrattuale con la stessa intrattenuto (collaboratori a progetto, consulenti, tirocinanti, borsisti etc).

Sono esentati dall'applicazione delle presenti Linee Guida, limitatamente a quanto necessario per il corretto svolgimento delle proprie funzioni, gli *Amministratori di Sistema*.

Pertanto, data la progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, al fine di non esporre l'ente Provincia di Pescara ai rischi di un coinvolgimento sia patrimoniale che penale, creando problemi alla sicurezza e problemi di immagine, l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che comunque normalmente dovrebbero essere adottati nell'ambito di un rapporto di lavoro, al fine di evitare che condotte inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

Per qualsiasi dubbio relativo all'applicazione pratica o all'interpretazione autentica delle disposizione contenute nelle presenti Linee Guida è possibile rivolgersi al personale del Servizio Sistemi Informativi compilando apposito quesito e inviandolo all'indirizzo di posta elettronica servizio.informatica@provincia.pescara.it

I. 2 Entrata in vigore, pubblicita' , revisione

Le presenti Linee Guida entrano in vigore alla data della loro approvazione con Decreto del Presidente, e saranno pubblicate nell'apposita sezione del sito web istituzionale denominata "Amministrazione Trasparente" garantendone la massima diffusione a tutto il personale.
Le Linee Guida potranno essere soggette a revisioni periodiche sulla base dell'evoluzione normativa e tecnologica nonché sulla base delle nuove esigenze di sicurezza e relative azioni

correttive che si dovranno eventualmente intraprendere, in occasione, per esempio, dell'entrata in vigore del regolamento europeo n 679/2016 - GDPR.
Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate alle presenti Linee Guida. Le proposte verranno esaminate dal Segretario Generale, con il supporto tecnico del Servizio sistemi Informativi.
Le eventuali revisioni apportate verranno approvate mediante Decreto e di tali revisioni sarà data tempestiva comunicazione ai dipendenti.

I.3 Definizioni

Ai fini delle presenti Linee Guida, si intende per:

- "trattamento" - qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
- "trattamento informatico" - trattamento effettuato con l'ausilio di strumenti elettronici;
- "dato personale" - qualunque informazione riguardante persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- "dati identificativi" - i dati personali che permettono l'identificazione diretta dell'interessato;
- "dati sensibili" - i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
- "dati giudiziari" - i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;
- "titolare" - la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
- "titolare della protezione dei dati (DPO o RDP): soggetto designato dal titolare o dal responsabile del trattamento per assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del Regolamento medesimo
- "responsabile" - la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;
- "incaricati/subresponsabili", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- "amministratore di sistema", la persona fisica dedicata alla gestione ed alla manutenzione di impianti di elaborazione o di sue componenti e tutte le figure equiparabili, quali gli amministratori di basi di dati, di reti informatiche, di apparati di sicurezza e di sistemi software complessi; soggetti che, pur non essendo preposti ordinariamente ad operazioni implicanti una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), possono, nelle loro consuete attività, essere concretamente referenti di specifiche fasi lavorative comportanti risvolti inerenti la protezione dei dati personali.

- "interessato", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
- "utente", soggetto (dipendente o amministratore politico) che accede ed utilizza i servizi e gli strumenti del sistema informatico dell'ente;
- "collaboratore", qualunque soggetto che, non essendo dipendente, e se preventivamente autorizzato, collabora con la Provincia di Pescara, a diverso titolo, per il conseguimento dei suoi fini istituzionali, ed ha accesso alle risorse informatiche dell'Ente;
- "comunicazione", il dare conoscenza dei dati personali ad uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal Responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- "dato anonimo", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- "banca di dati", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
- "comunicazione elettronica", ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;
- "reti di comunicazione elettronica", i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento ed altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;
- "rete pubblica di comunicazioni", una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;
- "misure minime", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione;
- "risorse informatiche", sono annoverate tra le risorse informatiche:

  - i server;
  - le workstation, i personal computer, i notebook e qualsiasi altra tipologia di elaboratore elettronico, compresi i dispositivi mobili;
  - le stampanti,
  - gli apparati di rete;
  - tutto il software e i dati acquisiti o prodotti da parte degli utenti o di terzi autorizzati;
  - file di qualsiasi natura, archivi di dati anche non strutturati ed applicazioni informatiche.

I. 4 Principi Ispiratori

I trattamenti devono rispettare le garanzie in materia di protezione dei dati e svolgersi nell'osservanza di alcuni cogenti principi sanciti nel Codice della privacy:

A. **il principio di necessità**, secondo cui i sistemi informativi ed i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite;

B. **il principio di correttezza**, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori. Le tecnologie dell'informazione (in modo più marcato rispetto ad apparecchiature tradizionali) permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa e ciò all'insaputa o senza la piena consapevolezza dei lavoratori, considerate anche le potenziali applicazioni di regole non adeguatamente conosciute dagli interessati;

C. **il principio di pertinenza e non eccedenza** in virtù del quale i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime. Il datore di lavoro deve trattare i dati "nella misura meno invasiva possibile"; le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere "mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza" (Parere n. 8/2001, cit., punti 5 e 12).

I.5 Linee guida generali

La Provincia di Pescara, consapevole delle potenzialità fornite dagli strumenti informatici e telematici, li mette a disposizione dell'Utente esclusivamente per finalità di tipo lavorativo.

Non è pertanto permesso utilizzare questi strumenti per altre finalità non connesse all'attività lavorativa o in modo che violino le leggi italiane vigenti in materia.

Ad esempio, non é consentito:

- Accedere a siti ed acquisire o comunque diffondere prodotti informativi lesivi del comune senso del pudore;
- Diffondere prodotti informativi lesivi dell'onorabilità, individuale e collettiva;
- Diffondere prodotti informativi di natura politica;
- **Diffondere in rete, o con qualsiasi mezzo di comunicazione, informazioni riservate di qualunque natura**;
- Svolgere ogni tipo di attività commerciale;
- Compiere attività che possano rappresentare una violazione della legge in materia di Copyright, fra le quali la copia non autorizzata di software, supporti audio e video, clonazione o programmazione di smartcard; **compiere attività che compromettano in qualsiasi modo la sicurezza delle risorse informatiche e della rete aziendale**.

La Provincia di Pescara adotterà ogni accorgimento tecnico necessario a tutelarsi da eventuali comportamenti non permessi, salvaguardando il rispetto della libertà e della dignità dei lavoratori; gli eventuali trattamenti effettuati saranno ispirati a canoni di trasparenza.

I.6 Titolarità

La Provincia di Pescara è titolare di tutte le risorse hardware e software messe a disposizione degli utenti.

L'hardware ed il software in dotazione alle Strutture che compongono l'Ente deve essere acquisito in accordo con le specifiche tecniche fornite dal Servizio Sistemi Informativi.

Le risorse informatiche assegnate devono essere custodite con cura evitando ogni possibile forma di danneggiamento.

Gli utenti assegnatari sono responsabili del corretto utilizzo degli strumenti messi loro a disposizione e della loro custodia e sono tenuti a segnalare tempestivamente al Servizio Sistemi Informativi eventuali situazioni anomale, guasti e/o difetti di funzionamento dei dispositivi hardware e software.

I.7 Competenze e responsabilità

Il Dirigente a cui afferisce il Servizio Sistemi Informativi è tenuto a:

- Elaborare le regole per un utilizzo ragionevolmente sicuro del sistema informativo dell'ente;
- Implementare, con l'ausilio di personale incaricato interno/esterno, le regole di sicurezza sul sistema informativo dell'ente;
- Monitorare, con l'ausilio di personale incaricato del Servizio Sistemi Informativi, e/o di personale incaricato interno/esterno, i sistemi per individuare un eventuale uso scorretto degli stessi, nel rispetto della privacy degli utenti;
- Segnalare prontamente ai Dirigenti delle Strutture interessate ogni eventuale attività non autorizzata sul sistema informativo dell'ente;
- Attenersi alle prescrizioni previste dal Garante per la Protezione dei Dati Personali ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema.

I Dirigenti dell'ente sono tenuti a:

- Informare il personale dipendente e/o assimilato sulle disposizioni in merito all'uso consentito delle risorse del sistema informativo dell'ente;
- Assicurare che il personale a loro assegnato si uniformi alle regole ed alle procedure descritte nelle presenti Linee Guida;
- Assicurare che i fornitori e/o il personale incaricato esterno si uniformino alle regole ed alle procedure descritte nelle presenti Linee Guida;
- Adempiere a tutti gli obblighi inerenti la responsabilità loro affidata in materia di trattamento di dati personali e sensibili gestiti dall'ente;
- Segnalare prontamente al Dirigente e al Responsabile del Servizio Sistemi Informativi ogni eventuale attività non autorizzata sul Sistema Informativo dell'ente.

Il personale del Servizio Sistemi Informativi e l'eventuale personale esterno incaricato che concorre alla gestione/implementazione del sistema informativo dell'ente è tenuto a:

- Garantire la massima riservatezza sulle informazioni acquisite direttamente o indirettamente nell'esercizio delle proprie funzioni;
- Segnalare prontamente al Dirigente e al Responsabile del Servizio Sistemi Informativi ogni eventuale attività non autorizzata sul sistema informativo dell'ente.

Gli Utenti del sistema informativo dell'ente sono responsabili per ciò che concerne:

- Il rispetto delle regole dell'ente per l'uso consentito del sistema informativo;
- L'uso delle credenziali di autenticazione loro assegnate secondo le modalità previste nelle presenti Linee Guida;

- La pronta segnalazione al competente Dirigente in merito ad ogni eventuale attività non autorizzata sul sistema informativo dell'ente di cui vengano a conoscenza.

TITOLO II STRUMENTI E SERVIZI INFORMATICI

II.1Credenziali di autenticazione

I sistemi di controllo degli accessi assolvono il compito di prevenire che persone non autorizzate possano accedere a un sistema informatico ed alle relative applicazioni.

Lo scopo è di cautelare l'ente ed i suoi dipendenti da ogni tipo di manomissione, furto o distruzione di dati oltre che di limitare l'accesso a specifici dati da parte di personale non autorizzato.

II.1.1 Password

Ove l'accesso al sistema avviene tramite autenticazione delle credenziali (normalmente nome utente e password), l'Utente dovrà:

- Custodire con diligenza le proprie credenziali e non comunicarle ad altre persone (es.: non scrivere la password su carta o post-it lasciandoli sulla scrivania o attaccati al monitor; non comunicare, né condividere con altri la propria password);

- Durante la digitazione della propria password, assicurarsi che nessuno stia osservando la tastiera con l'intenzione di memorizzarla.

La password deve essere composta da almeno otto caratteri e deve essere "robusta": una password si dice robusta quando è difficile ricostruirla e cioè quando risponde ad alcuni principi:

- All'aumentare della sua lunghezza, aumenta la difficoltà a carpirla;
- Include cifre, lettere e caratteri speciali come:**':;£$(,.ç@&/!**;

- Non contiene il proprio nome o cognome, il soprannome, la data di nascita, il nome di persone familiari, parole comuni, nomi di paesi, animali d'affezione etc;

- Non contiene parole che si trovano nei dizionari di qualsiasi lingua, anche se digitate al contrario, in quanto esistono software in grado di individuarle;

- Non sono composte da semplici sequenze di tasti sulla tastiera, come ad esempio "asdfghjkl", o da ripetizioni del proprio nome utente (ad es. se il proprio utente è rossi; la password "rossi rossi" sarà inopportuna), o da sequenze di numeri consecutivi (1234...)

- È composta da più parole contenenti errori ortografici o con sillabe combinate costituite da parole non correlate tra loro.

L'Utente s'impegna a comunicare quanto prima al Servizio Sistemi Informativi l'eventuale furto o smarrimento della propria password. In particolare, in caso di furto, l'Utente s'impegna a modificare tempestivamente la password utilizzando le procedure automatiche a sua disposizione.

In ogni caso, resta inteso che l'Utente sarà responsabile delle conseguenze derivanti dal furto, dalla perdita o dallo smarrimento di tale password.

II.2 Personal Computer

Il computer affidato all'Utente è uno strumento di lavoro fornito dall'ente e rappresenta una dotazione strumentale della sede ove è ubicato.

Il suo eventuale utilizzo non inerente l'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza dell'intera infrastruttura tecnologica della Provincia di Pescara.

Il computer può essere affidato ad uso singolo o condiviso, sulla base della richiesta effettuata dal Responsabile della Struttura e tenuto conto della prevalenza delle funzioni che devono essere espletate.

E' fornito con configurazione software predefinita che non può essere per alcun motivo modificata da parte dell'utente. Le richieste di installazione di nuovo software o di modifica della configurazione devono essere approvate dalla Struttura di appartenenza e dal Servizio Sistemi Informativi, che solo a seguito di tale accettazione provvederà ad effettuarle.

L'utente non può modificare le impostazioni autonomamente, di conseguenza:

a) *Non verranno forniti privilegi di "amministratore*", arginando in tal modo il pericolo di poter installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti;
b) *Non è consentita l'installazione sul proprio PC di mezzi di comunicazione propri* (come ad esempio modem e dispositivi Bluetooth);

c) *Non è consentito utilizzare strumenti software e/o hardware atti ad intercettare*, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;

d) *Non è consentito copiare sul proprio computer file contenuti in supporti magnetici, ottici e dispositivi usb non aventi alcuna attinenza con la propria prestazione lavorativa*;

e) *Il computer deve essere spento* (*ove necessario e possibile anche mediante scollegamento dalla presa elettrica*) ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di non utilizzo: lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso;

f) *occorre bloccare il computer o disconnettersi, in caso di postazioni condivise, qualora ci si allontani dalla propria postazione* (per il sistema operativo Windows premendo contemporaneamente i tasti Windows[1]+L (oppure Alt+Ctrl+Canc e cliccando su blocca computer) o in alternativa attivando la protezione sul proprio screensaver);

g) *Non è consentito utilizzare strumenti potenzialmente in grado di consentire accessi non autorizzati alle risorse informatiche* (es.: programmi di condivisione dati quali VNC, o software di monitoraggio della rete in genere);
h) *Non è consentito configurare o utilizzare servizi* quali DNS, DHCP, server internet (Web,FTP,…) diversi da quelli messi a disposizione da parte del Servizio Sistemi Informativi;
i) *Non è consentito intercettare pacchetti sulla rete (sniffing*); è conseguentemente vietato l'uso di software dedicati a carpire, in maniera invisibile, dati personali, password e ID dell'utente oppure atti a controllare ogni attività, ivi inclusa la corrispondenza ed i dati personali;
j) *Non è consentito impostare password nel bios* (salvo da parte del Servizio Sistemi Informativi dove necessario/opportuno);
k) *Non è consentito disassemblare il computer*, asportare, scollegare, aggiungere, spostare o semplicemente scambiare tra un PC e l'altro qualsiasi apparecchiatura in dotazione all'Utente salvo diretta e specifica indicazione del personale tecnico del Servizio Sistemi Informativi;

l) Non è consentito avviare il personal computer con sistemi operativi diversi da quello installato dal Servizio Sistemi Informativi incluse versioni live;
m) Non è consentito utilizzare connessioni in remoto per l'accesso a risorse dell'ente, al di fuori del perimetro aziendale e fatte salve le connessioni realizzate ed autorizzate da parte del Servizio Sistemi Informativi.

[1] I tasti con l'emblema di Windows posti ai due lati della barra spaziatrice.

II.2.1 Computer portatili (e dispositivi mobili)

L'Utente è responsabile dell'integrità del PC portatile affidatogli dal Responsabile della Struttura di appartenenza e dei dati ivi contenuti e deve custodirlo con diligenza sia durante gli spostamenti che nell'utilizzo nel luogo di lavoro.

Ai PC portatili (e dispositivi mobili) si applicano le regole di utilizzo previste per i personal computer.

Nel caso di utilizzo comune con altri Utenti, prima della riconsegna occorre provvedere alla rimozione definitiva di eventuali file elaborati.

I dischi dovranno essere criptati al fine di evitare, in caso di furto o di smarrimento, l'accesso a dati riservati e/o personali da parte di soggetti non autorizzati.

L'utente assegnatario che, venendo meno al dovere di diligenza nella custodia causi il danneggiamento o smarrimento delle dotazioni informatiche affidategli risponderà personalmente del danno patrimoniale arrecato.

Si ricorda che tutti i dischi o altre unità di memorizzazione locali non sono soggette a salvataggio da parte del personale incaricato del servizio Sistemi Informativi . La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente.

II.3 Privilegi di amministratore locale

Su specifica e motivata esigenza e richiesta, redatta in forma scritta e firmata, da parte del Dirigente della Struttura interessata al Dirigente del Servizio Sistemi Informativi, possono essere concessi a particolari utenti i privilegi di amministratore locale della propria postazione di lavoro.

Tali utenti saranno tenuti ad adottare le seguenti misure minime per mantenere inalterati gli attuali livelli di sicurezza informatica dei sistemi interessati e della rete aziendale:

- utilizzo di privilegi di amministrazione secondo la modalità e la regolamentazione prevista e richiamata nelle presenti Linee Guida;
- adozione e gestione di password definite, nella composizione e nella modalità di modifica, secondo la normativa vigente;
- tenere traccia, ovunque possibile, delle operazioni effettuate in occasione di nuove installazioni;

II.4 Rete

In assenza di specifica autorizzazione da parte delle Servizio Sistemi Informativi non è consentito accedere ai locali riservati alle apparecchiature di rete.

Non è consentito collegare alle prese di rete apparecchiature non autorizzate da parte del Servizio Sistemi Informativi, quali: hub, switch, ACCESS POINT o altre componenti personali.

Non è inoltre consentito installare o utilizzare qualsiasi altra apparecchiatura atta a gestire comunicazioni, salvo specifica autorizzazione rilasciata dal Servizio Sistemi Informativi quali, a titolo esemplificativo: modem, router, Internet key,…

Non è infine consentito effettuare spostamenti o modifiche di risorse collegate alla rete aziendale (es.: pc, stampanti, fotocopiatori e altro) senza una preventiva autorizzazione da parte del Servizio Sistemi Informativi.

Per l'accesso alla rete ciascun utente dev'essere in possesso delle specifiche credenziali di autenticazione.

II.5 Unità di archiviazione di rete (FILESERVER)

Gli spazi delle unità di rete messi a disposizione sono aree di condivisione e di archiviazione di informazioni strettamente lavorative e non possono pertanto essere utilizzate per la memorizzazione di file non attinenti ad attività lavorative. In queste aree dovranno essere salvati i documenti lavorativi afferenti la Struttura di appartenenza, al fine di renderli disponibili, in caso di necessità, agli altri utenti della Struttura.

Le attività di controllo statistico, amministrazione, backup e restore su queste unità sono competenza del personale del Servizio Sistemi Informativi.

IN NESSUNA RISORSA DI RETE È CONSENTITO SALVARE FILE AUDIO, VIDEO, ESEGUIBILI AD ECCEZIONE DI QUELLI STRETTAMENTE ATTINENTI AD ESIGENZE LAVORATIVE

Per tali tipologie di file ed archivi sono effettuati interventi di pulizia attivati d'ufficio da parte del Servizio Sistemi Informativi; vengono inoltre definiti ed attivati, a priori, filtri che ne vietano il loro salvataggio sui server dell'ente. Il Servizio Sistemi Informativi procederà alla rimozione immediata e senza nessun avviso di file di natura personale (foto, video, film, musica…etc)

Gli accessi alle unità di rete condivise devono essere autorizzati da parte del Responsabile del trattamento dei dati di pertinenza, il quale provvederà a richiedere al Servizio Sistemi Informativi dell'ente (in forma scritta) la creazione/rimozione dei diritti di accesso e ad effettuare periodicamente la verifica delle abilitazioni attive. Si specifica che saranno visibili solo le cartelle al cui accesso si è stati autorizzati, e che la presenza delle altre risorse presenti nel file server non sarà in alcun caso notificata.

II.6 Internet

L'utilizzo della connessione Internet aziendale è consentita per i soli scopi lavorativi e nell'ambito delle mansioni affidate ai singoli lavoratori.

A titolo *esemplificativo e non esaustivo*, non è consentito:

- l'upload o il download di software, di documenti o file di qualsiasi altra natura, se non strettamente attinenti all'attività lavorativa e previa verifica dell'attendibilità dei siti in questione;

- **ogni forma di registrazione utilizzando riferimenti della Provincia di Pescara a siti i cui contenuti non siano strettamente legati all'attività lavorativa**;

- la partecipazione a Forum non professionali, l'utilizzo di chat, di social network, di strumenti di condivisione, di bacheche elettroniche e le registrazioni in guestbooks anche utilizzando pseudonimi (nickname);
- l'effettuazione di ogni genere di transazione finanziaria (per es acquisti on line);

Al fine di prevenire, per quanto e ove possibile, comportamenti scorretti durante la navigazione in Internet, o per esigenze tecniche, l'ente si avvale di appositi filtri opportunamente configurati che impediscono l'accesso a siti non ritenuti idonei.

I filtri sopracitati limitano, per quanto possibile, l'accesso ai siti Internet che presentano i seguenti contenuti:

- illegali o non etici, stupefacenti, razzismo e odio, estremismo, violenza, occultismo, plagio;
- materiale per adulti, pornografia;
- giochi, scommesse, intermediazione e trading, download software freeware;
- social network, radio e tv via Internet (salvo i casi espressamente autorizzati dalla Dirigenza);
- peer to peer;
- malware, spyware, hacking, bypass proxy, phishing;
- qualsiasi altra tipologia di contenuti o siti che la Segreteria Generale riterrà di non dover rendere accessibile dalla rete aziendale, verrà preventivamente comunicata agli utenti.

II.7 Crittografia e controllo dei dati informatici

Fatto salvo quanto previsto dal D.lgs. 196/03 e s.m.i. in materia di archiviazione, gestione, trattamento e trasmissione di dati sensibili, è fatto divieto di applicare sistemi di crittografia dati, se non espressamente richiesto e/o autorizzato dal Responsabile di struttura.

II.8 Utilizzo e conservazione dei supporti rimovibili

Tutti i supporti di memorizzazione rimovibili (hard disk esterni, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati personali nonché informazioni costituenti know-how aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o recuperato successivamente alla cancellazione.

In ogni caso, i supporti contenenti dati personali devono essere adeguatamente custoditi, possibilmente in cassetti e armadi provvisti di chiusura.

A tal proposito si ricorda che l'utente è responsabile non solo della custodia dei supporti ma anche dei dati aziendali in essi contenuti.

Nel caso di utilizzo condiviso dei medesimi supporti da parte di più utenti, occorre provvedere alla cancellazione delle informazioni ivi contenute mediante opportuni programmi (es. CLEANER in modalità sovrascrittura avanzata).

Nel caso di smaltimento, i supporti dovranno essere prima distrutti mediante punzonatura o deformazione meccanica o distruzione fisica o demagnetizzazione.

II.9 Protezione antivirus

Il sistema informatico ed i PC collegati alla rete della Provincia di Pescara sono protetti da software antivirus autoaggiornantisi quotidianamente.

Ogni Utente è comunque tenuto a comportarsi in modo tale da ridurre il rischio di attacco al sistema informatico aziendale da parte di virus o attraverso qualsiasi altro software "aggressivo".

Ogni dispositivo magnetico di provenienza esterna all'ente dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale del servizio sistemi informativi.

Le stesse regole dovranno essere rispettate da parte di Soggetti terzi fornitori/gestori di apparecchiature e servizi informatici che vengono utilizzati a qualsiasi titolo all'interno della rete aziendale.

II.10 Teleassistenza

Per lo svolgimento di normali attività di manutenzione su personal computer connessi alla rete, il personale del Servizio Sistemi Informativi potrà utilizzare specifici software di connessione remota.

Tali programmi sono necessari per compiere interventi di assistenza informatica e manutenzione su applicativi ed hardware in uso presso l'Utente.

L'attività da remoto di assistenza e manutenzione avviene previa autorizzazione da parte dell'utente interessato e possibilmente mediante visualizzazione di un indicatore visivo sul monitor dell'utente che segnala la connessione in remoto del tecnico.

TITOLO III POSTA ELETTRONICA

III.1 Posta Elettronica Ordinaria

Il servizio di posta elettronica è un mezzo istituzionale di comunicazione dell'ente ed il suo utilizzo deve avvenire nel rispetto delle norme in materia di protezione dei dati personali.

La casella di posta elettronica assegnata all'utente è uno strumento di lavoro e le persone assegnatarie delle caselle sono responsabili del corretto utilizzo delle stesse.

Gli utenti hanno l'obbligo di procedere alla tempestiva lettura della corrispondenza pervenuta nella propria casella di posta nel corso dell'intera giornata lavorativa;

Sono attribuiti indirizzi di posta elettronica a:

- Strutture organizzative e per lo svolgimento di particolari funzioni (servizi o settori o specifiche linee progettuali).
- Utenti della Provincia di Pescara.
- per ragioni di sicurezza non è attribuibile un indirizzo di posta elettronica di dominio a collaboratori esterni.

L'uso degli indirizzi di Struttura deve essere dedicato alle comunicazioni ufficiali sia interne che esterne all'ente.

NON È CONSENTITO L'UTILIZZO DELL'INDIRIZZO DI POSTA NOMINATIVO O DI STRUTTURA PER SCOPI DIVERSI DA QUELLI PRETTAMENTE LAVORATIVI.

Di norma l'indirizzo di posta viene creato seguendo i seguenti criteri: nome.cognome@provincia.pescara.it;

servizio.nomeservizio@provincia.pescara.it;

settore.nomesettore@provincia.pescara.it

I casi di omonimia sono gestiti invertendo nome e cognome: cognome.nome@provincia.pescara.it

Nell'eventualità un account venisse "scalato", ossia a causa di un uso non conforme del titolare della casella di posta, la stessa venisse compromessa e ne fosse rubata l'identità, il Servizio Sistemi Informativi provvederà ad eliminare l'account corrotto (e tutto il suo contenuto non recuperabile) e a crearne un altro per lo stesso utente, costruito secondo i seguenti criteri: nomecognome@provincia.pescara.it

L'accesso al servizio di posta elettronica da parte di un Utente avviene mediante le credenziali di autenticazione (nome utente e password).

GLI UTENTI ASSEGNATARI DELLE CASELLE DI POSTA ELETTRONICA SONO I DIRETTI RESPONSABILI DEL CORRETTO UTILIZZO DELLE STESSE E RISPONDONO PERSONALMENTE DEI CONTENUTI TRASMESSI.

In particolare l'Utente è tenuto a rispettare quanto segue:

1. **non utilizzare il servizio per scopi illegali o non conformi alle presenti Linee Guida o in maniera tale da recar danno o pregiudizio all'ente o a terzi**;

2. **non utilizzare il servizio in modo da danneggiare, disattivare, sovraccaricare, pregiudicare o interferire con la fruibilità del servizio da parte degli altri utenti;**
3. non utilizzare la posta elettronica per inviare, anche tramite collegamenti o allegati in qualsiasi formato (testo, fotografico, video, grafico, audio, codice, ecc.), messaggi che contengano o rimandino ad esempio a: pubblicità non istituzionale, manifesta o occulta; prodotti di natura politica; comunicazioni commerciali private; materiale pornografico o simile; materiale discriminante o lesivo in relazione a razza, sesso, religione, ecc.; **materiale che violi la legge sulla privacy**; contenuti o materiali che violino i diritti di proprietà di terzi; altri contenuti illegali.
4. non utilizzare l'account aziendale quale riferimento telematico per l'accesso a siti che non siano attinenti ad attività lavorativa (per esempio siti di e-commerce).
5. conservare con pertinenza la segretezza delle proprie credenziali di accesso
6. conformarsi alle indicazioni tecniche fornite dal Servizio Sistemi Informativi

Di seguito si elencano alcune norme di comportamento che ciascun Utente è tenuto ad osservare al fine di preservare l'efficienza del servizio di posta elettronica e delle comunicazioni con esso veicolate:

- l'Utente è tenuto a visionare regolarmente la casella di posta elettronica di propria competenza;

- i messaggi devono essere preferibilmente di solo testo, evitando ove possibile ogni formattazione e inserzione di immagini;

- è necessario indicare sempre chiaramente l'oggetto, in modo tale che il destinatario possa immediatamente individuare l'argomento del messaggio ricevuto, facilitandone la successiva ricerca per parola chiave;

- **non superare la dimensione complessiva di 10 Megabyte degli allegati inviati con un singolo messaggio**;

- **limitare l'invio di messaggi di posta elettronica a indirizzi plurimi** (decine di destinatari) e trasmetterli solo in casi motivati da esigenze di servizio.
- L'Utente, infine, si impegna a non inviare messaggi di natura ripetitiva (catene di S.Antonio);
- l'Utente, in caso riceva messaggi di posta nei quali siano presenti link esterni, non dovrà aprirli, ma avvertire tempestivamente il servizio sistemi informativi per le opportune verifiche;
- l'Utente deve porre la massima attenzione nell'aprire il file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti);
- l'Utente deve leggere sempre i messaggi di *undeliverable* al fine di verificare la motivazione dell'impossibilità dell'invio, e provvedere in modo autonomo, per es cancellando dalle proprie liste gli account non più attivi;

I messaggi di posta elettronica rientrano tra i documenti informatici oggetto di conservazione (DPCM 3/12/2013 e Codice dell'Amministrazione Digitale). Il dettato normativo specifica la necessità di garantire, in particolare, che i messaggi di posta elettronica siano trasferiti nel sistema di gestione documentale per il tramite del protocollo informatico.

III.1.1 Le liste di distribuzione (mailing list)

Allo scopo di facilitare l'interscambio di informazioni relative a scopi istituzionali è previsto l'uso delle liste di distribuzione (mailing list).

Una lista generale di distribuzione comprendente tutti gli utenti è gestita centralmente da parte degli amministratori di posta.

Al momento della redazione delle presenti Linee Guida, le liste di distribuzione disponibili sono:

- "dipendenti" a cui afferiscono gli account di tutti i dipendenti dell'ente
- "posizioni organizzative" a cui afferiscono gli account degli incaricati di posizione organizzativa
- "dirigenti" a cui afferiscono gli account dei dirigenti dell'ente.

III.1.2 Regole d'uso, accesso alternativo e cessazione caselle mail

Le caselle di posta hanno una dimensione predefinita, estendibile solo in base alla disponibilità di spazio e a fronte di motivata richiesta, redatta per iscritto, dal Dirigente di Struttura; occorre pertanto mantenere in ordine la propria casella di posta badando a ripulirla con regolarità e salvando gli allegati ingombranti.

Al fine di garantire la continuità all'accesso dei messaggi da parte dei soggetti adibiti ad attività lavorative che richiedono la condivisione di una serie di documenti si consiglia e si incoraggia l'utilizzo abituale di caselle di posta elettronica condivise tra più lavoratori (gli account di servizio) e di non utilizzare quelle individuali.

In caso di assenza prolungata programmata del dipendente, si consiglia e si raccomanda al dipendente di attivare il sistema di risposta automatica ai messaggi di posta elettronica ricevuti indicando, nel messaggio di accompagnamento, le coordinate di un collega o della struttura di riferimento che può

essere contattata in sua assenza e/o altre modalità utili di contatto della Struttura organizzativa dell'ente presso cui presta la propria attività lavorativa.

Nell'ipotesi di assenza o impossibilità, temporanea o protratta nel tempo, del dipendente, qualora per ragioni di sicurezza o comunque per garantire l'ordinaria operatività aziendale sia necessario accedere a informazioni o documenti di lavoro presenti sul personal computer del dipendente, inclusi i messaggi di posta elettronica in entrata ed in uscita, il dipendente può delegare un altro dipendente a sua scelta (fiduciario) il compito di verificare il contenuto di messaggi ed inoltrare al responsabile della Struttura in cui lavora quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività deve essere redatto apposito verbale (protocollato) ed informato il dipendente interessato alla prima occasione utile.

In caso di assenza o impossibilità, temporanea o protratta nel tempo, del dipendente, qualora per ragioni di sicurezza o comunque per garantire l'ordinaria operatività aziendale sia necessario accedere a informazioni o documenti di lavoro presenti sul personal computer del dipendente, inclusi i messaggi di posta elettronica in entrata e in uscita, e il dipendente non abbia delegato un altro dipendente (fiduciario), secondo quanto sopra specificato, il responsabile della struttura cui afferisce il dipendente può chiedere all'Amministratore del Sistema ed al Dirigente Responsabile del Servizio Sistemi Informativi di accedere alla postazione e/o alla casella di posta elettronica del dipendente assente, in modo che si possa prendere visione delle informazioni e dei documenti necessari. Contestualmente, il responsabile della struttura deve informare il dipendente appena possibile, fornendo adeguata spiegazione e redigendo apposito verbale.

Le caselle di posta individuali hanno validità pari alla durata della permanenza in servizio del dipendente, fatte salve eventuali situazioni di congedo, distacco e comando.

Nel caso il cui il dipendente non presti più la sua attività lavorativa presso la Provincia di Pescara, la casella di posta elettronica sarà eliminata entro le 24 ore successive all'evento, ai sensi dei provvedimenti emanati dal Garante per la protezione dei dati personali n 13 del 1/3/2007, n 136 del 5/3/2015, n 456 del 30/6/2015, n 303 del 13/7/2016 e successivi.

Al fine di cui sopra il Servizio Personale, nelle sue varie competenze, provvede a comunicare al servizio sistemi Informativi, per iscritto, l'elenco degli utenti il cui account deve essere dismesso.

Non sarà pertanto più possibile accedere al contenuto di tale casella di posta, neanche per urgenti necessità lavorative. Si invitano pertanto i Dirigenti e i Responsabili di servizio affinché concordino con il lavoratore uscente un piano di salvataggio del contenuto della casella mail.

III.1.3 Gestione del servizio

Il Servizio di posta elettronica è gestito dal Servizio sistemi Informativi, in particolare il Servizio è tenuto a:

1. adottare le misure più idonee a garantire la continuità, la disponibilità e la sicurezza del servizio di posta elettronica ordinaria;
2. gestire i dati degli utenti nel rispetto della vigente normativa sulla tutela dei dati personali;
3. informare gli utenti, quando possibile con tempestività, di eventuali interruzioni tecniche di servizio che si rendessero necessarie per cause di forza maggiore;
4. monitorare i livelli di servizio del sistema al fine di garantirne la massima efficienza;
5. monitorare l'utilizzo del servizio da parte degli utenti al fine di evidenziarne usi scorretti e non consentiti;

Il Servizio Sistemi Informativi non effettua alcuna visura, controllo, censura, modifica, cancellazione dei messaggi di posta elettronica ricevuti/inviati dagli utenti, ovvero nel caso in cui ciò si renda necessario per adempiere ad una disposizione di legge, ad un ordine giudiziario o governativo.

III.2 Posta Elettronica Certificata Premessa e Riferimenti Legislativi

L'innovazione digitale impone non soltanto un continuo e necessario adeguamento tecnologico ed infrastrutturale, ma un vero e proprio ripensamento di processi, organizzazioni e ruoli in tutti i settori del pubblico e del privato.

La panoramica che segue mira esplicitamente ad evidenziare quali sono le prassi di utilizzo della PEC considerate corrette e valide giuridicamente, con l'intento di limitare l'incidenza delle prassi errate che rendono inefficaci, invalide o addirittura nulle le trasmissioni dei documenti e che spesso svelano la loro reale portata giuridica solo nel momento patologico del giudizio.

La Posta Elettronica Certificata (PEC) secondo la definizione contenuta nell'art. 1, comma 1, lettera v-bis, del D. Lgs. 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale) è un *"sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai terzi".*

La PEC, introdotta nel nostro ordinamento con il DPR. 68/2005 "Linee Guida per l'utilizzo della Posta Elettronica Certificata" e disciplinata all'interno del D.Lgs. 82/2005 (CAD) è, dunque, un sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica, attestante l'invio e la consegna di documenti informatici con valenza legale. Con questa modalità di invio il mittente ottiene dal proprio gestore di posta una ricevuta con precisa indicazione temporale, che costituisce prova legale dell'avvenuta spedizione del messaggio e degli eventuali documenti allegati allo stesso.

I soggetti che intendono fruire del servizio di PEC devono avvalersi dei gestori inclusi nell'elenco pubblico tenuto dall'AGID ai sensi dell'art. 14 del DPR 68/2005. Per accreditarsi presso l'AGID, i gestori devono possedere una serie di requisiti soggettivi ed oggettivi, nonché la certificazione di qualità richiesta dalla legge e devono, inoltre, garantire il rispetto delle "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata" di cui al D.M. 2 novembre 2005, assicurando in ogni caso livelli minimi di servizio (art. 13 DPR 68/2005).

III.2.1 Soggetti obbligati al possesso di indirizzo PEC

Ai sensi dell'art. 16 del DL 185/2008 sono tenuti a dotarsi di casella di posta elettronica certificata i seguenti soggetti:

- le Pubbliche Amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165 (a titolo esemplificativo e non esaustivo, amministrazioni dello Stato, scuole, regioni, provincie, comuni, comunità montane, università, IACP, Camere di Commercio, enti pubblici non economici nazionali, regionali e locali, ASL, ecc..) sono tenute a dotarsi di un indirizzo di PEC per ogni registro di protocollo;

- le imprese già esistenti e di nuova costituzione. In particolare le prime hanno dovuto provvedere a dotarsi di indirizzo PEC entro il 30 novembre 2011, mentre per le seconde la legge prevede l'impossibilità di perfezionare l'iscrizione al Registro delle Imprese in assenza di PEC (infatti, quest'ultimo è tenuto a sospendere il procedimento di iscrizione per quarantacinque giorni per consentire l'integrazione necessaria e trascorso inutilmente questo termine, la domanda si intende non presentata);
- i professionisti iscritti in albi ed elenchi istituiti con legge dello Stato, già dal 30 novembre 2009 hanno l'obbligo di dotarsi di un indirizzo di PEC e di darne comunicazione obbligatoria ai rispettivi Ordini e Collegi. Gli indirizzi PEC forniti dai professionisti agli Ordini di appartenenza alimentano il registro INI-PEC istituito presso il MISE, liberamente consultabile da chiunque.

Con l' intervento ad opera del D. Lgs. 26 agosto 2016, n.179 di riforma del CAD il legislatore ha stabilito che gli indirizzi di Posta Elettronica Certificata costituiscono mezzo esclusivo di comunicazione e notifica tra imprese, professionisti e PA.[1]

I pubblici elenchi nei quali possono essere ricercati i domicili digitali sono quelli previsti dall'art 16-ter del DL 179/2012, convertito in L 221/2012, cha fa riferimento a:

- indice dei domicili digitali della pubbliche amministrazioni e dei gestori di pubblici servizi (art 6-ter CAD): www.indicepa.gov.it (IPA);

- indice nazionale dei domicili digitali delle imprese e dei professionisti (art 6-bis CAD): www.inipec.gov.it;

Facendo seguito a quanto sopra si richiama **all'obbligo dell'utilizzo dei canali telematici per le comunicazioni con altre P.A., Imprese o professionisti**, nonché con privati cittadini se in possesso di domicilio digitale. Pertanto l'invio di posta per il tramite dei canali tradizionali (raccomandata, posta celere etc) è autorizzata solo in casi motivati in modo specifico, in quanto, diversamente si configurerebbe danno all'erario e illecito disciplinare.

La richiesta di invio di documentazione per il tramite dei canali tradizionali dev'essere formalizzata attraverso il modello " richiesta spedizione tramite posta ordinaria" (modulo No-PEC) allegato alle presenti Linee Guida.

III.2.2 Funzionamento della PEC

a) Invio di messaggio da una casella PEC ad un'altra casella PEC

Il mittente dotato di casella PEC, previa autenticazione, predispone e invia il messaggio, sottoponendolo così al suo gestore del servizio di PEC.

Il gestore del mittente verifica la correttezza formale del messaggio e l'assenza di virus; in caso di esito positivo, restituisce al mittente la "ricevuta di accettazione" e genera automaticamente la "busta di trasporto" con il file "postacert.eml" che contiene il messaggio originale e il file "daticert.xml" che riproduce l'insieme di tutte le informazioni relative all'invio (mittente, gestore del mittente, destinatari, data e ora dell'invio). La busta è firmata dal gestore tramite firma elettronica qualificata. Ciò permette al gestore del destinatario di verificare l'inalterabilità durante il trasporto. Se l'esito della verifica è sfavorevole, rilascia un "avviso di non accettazione" che riporta anche il motivo del rifiuto.

Il gestore del destinatario, una volta ricevuta la busta di trasporto ed effettuati i controlli sulla validità e assenza di virus, la accetta e consegna al gestore del mittente la "ricevuta di presa in carico", che attesta il passaggio di consegna tra i due gestori e successivamente deposita il messaggio nella casella di posta del

[1] Analoga norma si riscontra già in ambito di Processo Tributario Telematico (PTT) con l'art. 7, comma 2 del DM 163/2013 che dispone la coincidenza dell'indirizzo di PEC del professionista accreditato presso il SIGIT con quello presente in INI-PEC.

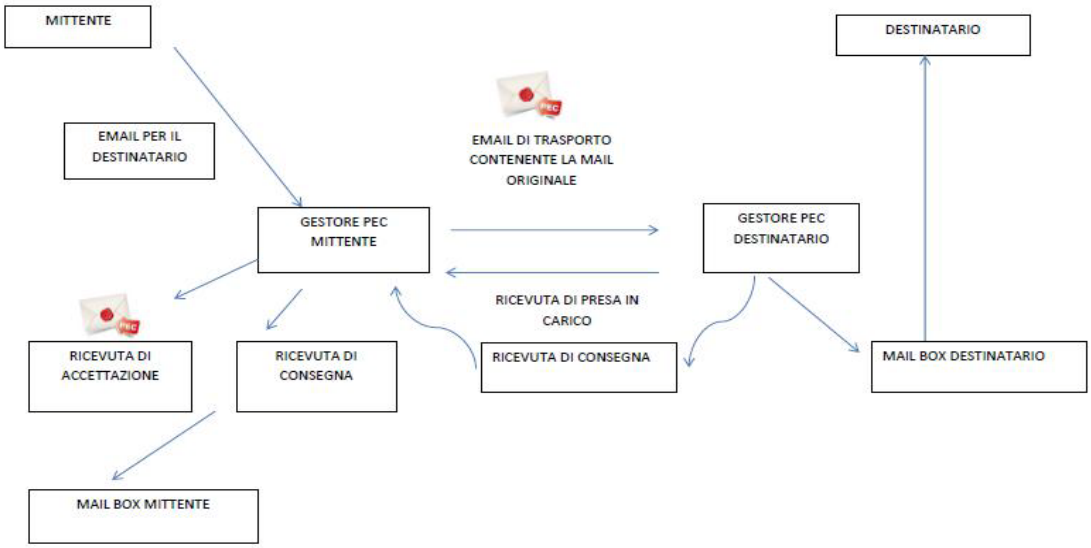
destinatario. Se la consegna va a buon fine, il gestore del destinatario invia a quello del mittente una "ricevuta di avvenuta consegna". Le ricevute di consegna possono essere di tre tipi, a seconda della scelta impostata dal mittente:

- completa (scelta consigliata): formata dal file "postacert.eml", contenente il messaggio originale completo di testo ed eventuali allegati, e il file "daticert.xml" che riproduce l'insieme di tutte le informazioni relative all'invio (mittente, gestore del mittente, destinatari, oggetto, data e ora dell'invio, codice identificativo del messaggio);
- breve (scelta non consigliata): formata dal file "daticert.xml" e un estratto del messaggio originale;
- sintetica (scelta non consigliata): formata dal solo file "daticert.xml".

Se il gestore del destinatario non riesce a consegnare il messaggio, ad esempio in quanto la casella PEC destinataria è satura o non più attiva, invia un "avviso di mancata consegna" che, ovviamente, il gestore del mittente inoltra a quest'ultimo.

Se il gestore del mittente non riceve nulla da quello del destinatario entro 12 ore dall'inoltro della busta di trasporto, ne informa il mittente; trascorse inutilmente e complessivamente 22 ore - e comunque prima che siano trascorse 24 ore - comunica al mittente la notizia che il messaggio non è stato consegnato.

Il destinatario (dotato di casella PEC), a sua volta, riceve la busta di trasporto con il file "postacert.eml" contenente il messaggio originale, completo di testo ed eventuali allegati, e il file "daticert.xml" che riproduce l'insieme di tutte le informazioni relative all'invio.



b) Invio di messaggio da una casella PEC a una casella di posta elettronica ordinaria

Il mittente dotato di casella PEC, rispetto all'ipotesi precedente, riceve dal proprio gestore esclusivamente la ricevuta di accettazione come sopra indicata.

Essendo il destinatario del messaggio possessore di una casella di posta elettronica ordinaria, il mittente possiede solo la ricevuta di accettazione che non rappresenta una attestazione certa del ricevimento del messaggio da parte del primo e che, dunque, non costituisce un documento valido in caso di contestazione.

Il destinatario dotato di casella di posta elettronica ordinaria visualizza la busta di trasporto con il file "postacert.eml", contenente il messaggio originale, completo di testo ed eventuali allegati, e il file "daticert.xml" che riproduce l'insieme di tutte le informazioni relative all'invio.

c) Invio di messaggio da casella di posta elettronica ordinaria a una casella di PEC

In questo caso il mittente dotato di casella di posta elettronica ordinaria non riceve notifiche dal sistema PEC.

Invece, il destinatario titolare della casella PEC riceve una busta di anomalia, in quanto il messaggio proviene da una casella di posta ordinaria e il file "postacert.eml" contenente il messaggio originale completo di testo ed eventuali allegati.

Si consideri, inoltre, che il servizio di posta del destinatario potrebbe essere stato configurato per non accettare invii da posta elettronica ordinaria (impostazione opzionale a cura del destinatario); in questo caso, il mittente riceve una comunicazione di impossibilità di ricezione indicante che l'indirizzo del destinatario non è abilitato alla ricezione di posta non certificata (scelta consigliata).

Ulteriori indicazioni tecniche

Si evidenzia che il gestore di PEC può prevedere limiti dimensionali per il singolo messaggio, ma deve comunque garantire la possibilità di invio di un messaggio ad almeno cinquanta destinatari e per il quale il prodotto del numero dei destinatari per la dimensione del messaggio stesso non superi i venti megabytes (art. 12 delle Regole tecniche).

Come già indicato in precedenza, i gestori firmano digitalmente tutto quanto da loro generato: ricevute, buste di trasporto e avvisi. Inoltre, hanno l'obbligo di registrare tutte le operazioni relative alle proprie PEC nel log del proprio sistema, di estrarre le registrazioni con cadenza giornaliera, apponendo una marca temporale e di conservarle per almeno 30 mesi, nel rispetto delle norme di legge in materia di conservazione.

Si ritiene utile specificare che il registro di log deve contenere le seguenti informazioni:

- il codice identificativo univoco assegnato al messaggio originale (Message-ID);
- la data e l'ora dell'evento;
- il mittente del messaggio originale;
- i destinatari del messaggio originale;
- l'oggetto del messaggio originale;
- il tipo di evento (accettazione, ricezione, consegna, emissione ricevute, errore, ecc.);
- il codice identificativo (Message-ID) dei messaggi correlati generati (ricevute, errori, ecc.);
- il gestore mittente

III.2.3 Validita' ed efficacia della PEC e Obbligo di protocollazione

Valore legale dell'invio e della consegna

Come si è detto, la PEC è un tipo particolare di posta elettronica che attribuisce al messaggio trasmesso il valore legale tradizionalmente riconosciuto alla raccomandata con avviso di ricevimento, essendo in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai terzi.

Per espressa previsione di legge, infatti, la trasmissione effettuata via PEC equivale alla notificazione per mezzo della posta e, se la trasmissione è effettuata in conformità al DPR 68/2005 ed alle Regole tecniche di riferimento, consente di opporre ai terzi la data e l'ora di trasmissione e di ricezione del documento[2].

In merito, il DPR 68/2005 specifica ulteriormente che *"La validità della trasmissione e ricezione del messaggio di posta elettronica certificata è attestata rispettivamente dalla ricevuta di accettazione e dalla ricevuta di avvenuta consegna"* (art. 4, comma 6). Dunque, sia la ricevuta di accettazione che la ricevuta di avvenuta consegna rappresentano prove "piene", ossia il giudice deve valutarle in conformità a quanto previsto dalla legge senza alcun margine di discrezionalità.

Nel dettaglio la ricevuta di accettazione, sottoscritta con firma elettronica qualificata e contenente i dati di certificazione del gestore di PEC del mittente, costituisce la prova legale, opponibile ai terzi, che il messaggio in una determinata data ed ora è stato accettato dal sistema ed inoltrato al gestore PEC del destinatario. L'attestazione è fisicamente costituita da una e-mail contenente un file xml (daticert.xml) con i dati di certificazione del gestore di PEC, l'indicazione di un codice identificativo univoco attribuito all'e-mail e la sottoscrizione del gestore.

Analogamente, la ricevuta di avvenuta consegna è rilasciata automaticamente al mittente dal gestore di PEC del destinatario, a fronte della ricezione di una busta di trasporto valida. La ricevuta fornisce al mittente la prova che il messaggio è effettivamente pervenuto nella casella di PEC del destinatario e che si trova nella sua disponibilità, a prescindere dal fatto che questi lo abbia letto oppure no. Si noti che la legge attribuisce valore legale non alla lettura effettiva del documento, ma soltanto al fatto oggettivo che il documento sia stato recapitato e si trovi nella materiale disponibilità del destinatario. Dal punto di vista giuridico, in questo caso, si determina una presunzione di conoscenza della comunicazione da parte del destinatario, analoga a quella prevista in tema di dichiarazioni negoziali dall'art. 1335 c.c. per il caso della raccomandata a/r.

Sul punto, la giurisprudenza ha avuto modo di affermare che in caso di inconvenienti tecnici che determinano l'impossibilità materiale della conoscenza *"spetta al destinatario, in un'ottica collaborativa,*

[2] Si veda l'art. 48, del D. Lgs. 82/2005 Codice dell'Amministrazione Digitale (Posta elettronica certificata):

"*1. La trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante la posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, o mediante altre soluzioni tecnologiche individuate con le regole tecniche adottate ai sensi dell'articolo 71.*

☐ *La trasmissione del documento informatico per via telematica, effettuata ai sensi del comma 1, equivale, salvo che la legge disponga diversamente, alla notificazione per mezzo della posta.*

☐ *La data e l'ora di trasmissione e di ricezione di un documento informatico trasmesso ai sensi del comma 1 sono opponibili ai terzi se conformi alle disposizioni di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, ed alle relative regole tecniche, ovvero conformi alle regole tecniche adottate ai sensi dell'articolo 71*".
DPR 11 febbraio 2005, n. 68 "Linee Guida sull'utilizzo della posta elettronica certificata".

rendere edotto il mittente incolpevole delle difficoltà di cognizione del contenuto della comunicazione legate all'utilizzo dello strumento telematico, pure ammesso dalla legge"[3].

Certificazione dell'integrità e immodificabilità del messaggio

Un'ulteriore valenza della PEC rispetto alla raccomandata tradizionale è rappresentata dal valore di attestazione in ordine all'integrità ed alla immodificabilità del messaggio. Queste caratteristiche sono assicurate dalla cd. "busta di trasporto" che, secondo la definizione delle Regole tecniche[4], è la busta creata dal gestore del mittente ed inviata al gestore del destinatario all'interno della quale sono inseriti il messaggio originale inviato dall'utente ed i relativi dati di certificazione[5]. Essa è sottoscritta dal gestore con firma elettronica qualificata che garantisce la provenienza, l'integrità e l'autenticità del messaggio di posta elettronica certificata. La "busta" è consegnata, immodificata, nella casella di PEC di destinazione per permettere la verifica dei dati di certificazione da parte del ricevente.

Valore di certificazione del contenuto dei messaggi

Inoltre, mentre la raccomandata fornisce unicamente la prova dell'invio di una comunicazione ma non del suo contenuto (v. Corte di Cassazione, sez. III, n. 10021/2005), la PEC consente in alcuni casi di fornire anche la dimostrabilità del contenuto inviato.

Per meglio comprendere il valore probatorio che può avere un messaggio di PEC, dunque, si deve innanzitutto ricordare che tutte le ricevute rilasciate dai gestori (di accettazione, di avvenuta consegna, busta di trasporto) sono sottoscritte con firma elettronica qualificata, idonea a rendere manifesta la provenienza e assicurare l'integrità e l'autenticità delle ricevute stesse. Si osserva inoltre che, mentre la ricevuta di accettazione è sempre di un solo tipo, la ricevuta di avvenuta o mancata consegna, come si è detto, può essere di tre tipi, a seconda dell'ampiezza dei contenuti: sintetica, breve o completa. Questa distinzione rileva anche sotto il profilo dell'efficacia probatoria del messaggio di PEC, poiché nel caso della ricevuta completa è possibile provare, oltre all'esistenza della comunicazione tra due soggetti, anche il contenuto del messaggio inviato. In pratica, il mittente che ha conservato la ricevuta di consegna completa è in grado di dimostrare quale sia il contenuto del messaggio (e degli allegati eventualmente presenti) inviato.

Si veda sul punto, tra tante altre sentenze, TAR Campania n. 1756 del 3 aprile 2013 in cui si rileva che la ricevuta cd. "breve" non restituisce l'intero allegato (cioè l'intero atto con firma digitale) ma solo un suo estratto codificato. Dunque, al fine di verificare in giudizio che effettivamente la notifica dell'atto sia andata a buon fine e che l'atto notificato con la PEC sia conforme a quello depositato in formato cartaceo, deve essere prodotta dall'avvocato notificante la c.d. ricevuta completa di avvenuta consegna: solo in questo modo si può dimostrare la notificazione dell'intero atto, e non soltanto di un suo estratto.

Un sistema alternativo di prova, utilizzabile in luogo delle ricevute, è costituito dalla richiesta dei "dati di log" dei messaggi al gestore di posta interessato che, ai sensi di legge, tiene il registro informatico delle

[3] Con la sentenza in forma semplificata 3 dicembre 2014, n. 610, la Sez. I del G.A. di Trieste - chiamata a decidere sulla legittimità di un provvedimento disposto, fra l'altro, sulla base di file digitali contenenti documentazione che non risultava apribile e dunque visionabile - ha chiarito come la trasmissione a mezzo PEC di istanze e dichiarazioni, se effettuata con il rispetto dei requisiti formali e normativamente fissati, determini una presunzione di conoscenza del contenuto della comunicazione in capo al destinatario. Da tale premessa ha tratto, quale logico corollario, il principio per cui incombe sul destinatario l'onere di informare il mittente nel caso in cui il contenuto del messaggio non risulti visionabile, non potendo tale problema tecnico legittimare l'adozione di un provvedimento negativo nei confronti del mittente incolpevole

[4] D.M. 2 novembre 2005 "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata".

[5] Sono i dati quali per esempio data e ora di invio, mittente, destinatario, oggetto, identificativo del messaggio, che descrivono l'invio del messaggio originale e sono certificati dal gestore di PEC del mittente ai sensi dell'art1, comma 1, lett. r) del DM 2 novembre 2005 contenente le regole tecniche per la PEC.

operazioni relative alle trasmissioni effettuate mediante PEC (invio, ricezione…). Il registro (log file), essendo marcato temporalmente con cadenza quotidiana e conservato dal gestore di PEC per almeno trenta mesi in condizioni di sicurezza, costituisce un documento informatico attestante, con validità legale, tutte le operazioni svolte dal gestore. Tali informazioni sono opponibili ai terzi e possono essere utilizzate dal mittente ove non abbia più la disponibilità delle ricevute dei messaggi di PEC. Si segnalano, tuttavia, alcune limitazioni da tenere presenti: il log file non contiene informazioni relative al contenuto dei messaggi, ma solo le informazioni relative allo loro trasmissione e quindi, attraverso questo sistema si potrà fornire in giudizio soltanto la prova della trasmissione, ma non del contenuto del messaggio inviato; inoltre, qualora la prova della trasmissione dovesse essere esibita oltre i trenta mesi di conservazione obbligatoria, il certificato di firma del gestore potrebbe scadere rendendo inutilizzabili i dati di log.

Per questi motivi è sempre fortemente raccomandata la corretta conservazione delle ricevute complete relative ad ogni invio di PEC.

Prova della paternità del documento trasmesso

Occorre tuttavia evidenziare che attribuire alla PEC l'idoneità a fornire prova dell'avvenuta spedizione di un messaggio, nonché del suo effettivo contenuto, non equivale ad attribuire anche la paternità del documento ad esso allegato al relativo mittente.

In generale, in materia di istanze e dichiarazioni da presentare alla pubblica amministrazione, l'art. 38 del DPR 445/2000 prevede espressamente che esse siano valide se effettuate in conformità alle previsioni dell'art. 65 del CAD. In sostanza, le istanze e le dichiarazioni da presentare alla PA sono equivalenti, da un punto di vista legale, a quelle sottoscritte con firma autografa apposta in presenza del dipendente addetto al procedimento:

A) se sottoscritte mediante la firma digitale o la firma elettronica qualificata;

B) se l'istante o il dichiarante è identificato attraverso il sistema pubblico di identità digitale (SPID), nonché attraverso uno degli altri strumenti previsti dalla legge;

C) ovvero sono sottoscritte e presentate unitamente alla copia del documento d'identità;

c-bis) ovvero se trasmesse dall'istante o dal dichiarante mediante la propria casella di posta elettronica certificata purché le relative credenziali di accesso siano state rilasciate previa identificazione del titolare, anche per via telematica in conformità con le regole tecniche adottate ai sensi dell'articolo 71, e ciò sia attestato dal gestore del sistema nel messaggio o in un suo allegato. In tal caso, la trasmissione costituisce dichiarazione vincolante ai sensi dell'articolo 6, comma 1, secondo periodo. Sono fatte salve le disposizioni normative che prevedono l'uso di specifici sistemi di trasmissione telematica nel settore tributario.

In pratica, la legge riconosce la provenienza del messaggio di PEC e dunque la paternità del documento inviato solamente nel caso in cui il titolare della casella sia stato identificato al momento del rilascio della stessa. Rientra in queste ipotesi la previsione contenuta nell'art. 7 del D.M. 23 dicembre 2013, n. 163 che, nell'ambito del Processo Tributario Telematico, prevede l'identificazione del titolare prima del rilascio delle credenziali di accesso alla PEC.

Nelle altre ipotesi, ossia quando tale identificazione non vi sia stata, la PEC varrà unicamente a provare la data e l'ora di trasmissione e ricezione del messaggio (e anche l'integrità del contenuto) ma la singola istanza e dichiarazione contenuta, per avere pieno valore probatorio, dovrà essere sottoscritta dall'intestatario con firma elettronica qualificata o digitale.

Si richiamano a questo proposito le norme in materia di validità ed efficacia probatoria del documento informatico contenute negli artt. 20 e seguenti del CAD. In primis, il nuovo comma 1° dell'art. 21 che riconosce al documento informatico sottoscritto con firma elettronica (semplice) il valore della forma scritta liberamente valutabile in giudizio sotto il profilo probatorio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità. Si segnala altresì la disposizione contenuta al comma successivo secondo la quale *"Il documento informatico sottoscritto con firma elettronica avanzata*[6]*, qualificata o digitale, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, ha altresì l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria. Restano ferme le disposizioni concernenti il deposito degli atti e dei documenti in via telematica secondo la normativa anche regolamentare in materia di processo telematico*".

Analogamente a quanto avviene per le istanze e le dichiarazioni da presentare alla PA, la firma qualificata e quella digitale sono le uniche tipologie di firma elettronica riconosciute dalla legge nell'ambito del Processo Tributario Telematico (D.M. 163/2013) in quanto idonee ad attribuire al documento informatico le caratteristiche dell'integrità e della immodificabilità. Anche qui, rileva come l'utilizzo del dispositivo di firma si presuma riconducibile al titolare salvo che questi dia prova contraria. Inoltre, sussistendo una presunzione in ordine alla identificabilità dell'autore, la conseguente paternità del documento firmato diviene non disconoscibile.

In conclusione, la PEC è un sistema di trasmissione idoneo a certificare l'invio e il ricevimento di un documento informatico in una determinata data ed ora. La ricevuta completa è inoltre idonea ad attestare l'integrità e l'immodificabilità del contenuto del messaggio e degli allegati trasmessi. Fermo quanto sopra espresso, per provare in giudizio la riconducibilità di un atto ad un autore è inoltre necessario che il documento sia sottoscritto da questi con firma elettronica avanzata, o qualificata (ad esempio: digitale).

Profili processuali e operativi: in particolare, la prova della notifica a mezzo PEC

Le comunicazioni e notificazioni di atti e provvedimenti sono eseguite mediante ufficiali giudiziari o altri pubblici ufficiali (ad es. messi comunali), oppure a mezzo servizio postale secondo quanto previsto dagli artt. 137 e ss. del c.p.c. (art. 3, R.D. n. 642 del 1907).

Tra le forme di notifica o comunicazione previste rientra anche la PEC. Infatti, la trasmissione del documento informatico per via telematica equivale, salvo che la legge disponga diversamente, alla notificazione per mezzo della posta ordinaria e la data e l'ora di trasmissione e di ricezione di un documento informatico sono opponibili ai terzi se conformi alle disposizioni di cui al D.P.R. 11 febbraio

[6] Le definizioni di firma elettronica avanzata e di firma elettronica qualificata prima contenute nell'art. 1 del CAD, risultano soppresse a decorrere dal 14 settembre 2016, per effetto dell'entrata in vigore del D.Lgs. 26 agosto 2016, n. 179 contenente la riforma del CAD. Tali definizioni sono invece contenute nell'art. 1, comma 1 bis del Linee Guida UE n. 910/2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche cd. "eIDAS". Nel CAD resta la seguente definizione di firma digitale contenuta nell'art. 1, comma 1, lett. s) "*un particolare tipo di firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici*".

2005, n. 68, ed alle relative regole tecniche[7]. Tuttavia, va precisato che il notificante deve attuare tutte le formalità previste dalla legge in materia e ha l'onere di fornire la prova della regolare notifica o comunicazione in caso di contestazione.

La prova della notifica può essere fornita mediante documento telematico o mediante documenti cartacei che riproducano esattamente tutti gli atti spediti, debitamente sottoscritti con firma digitale. Pertanto, al fine di dare prova della corretta (e perfezionata) notifica è necessario produrre, in mancanza di prova telematica (al momento non ancora ammessa):

1) la stampa dell'atto notificato in formato PDF con firma digitale, se si tratta di allegato;

2) le ricevute di accettazione e consegna completa della PEC.

3) il certificato di firma digitale del notificante;
4) il certificato di firma del gestore di PEC[8].

Inoltre, va evidenziato che qualsiasi atto destinato a produrre effetti giuridici deve essere recettizio e al momento della notifica deve contenere la relazione da parte del soggetto che procede alla notifica stessa, anche se il notificante intende avvalersi della notifica a mezzo posta certificata telematica.

L'assenza della relazione di notifica, della prova di un atto sottoscritto con firma digitale, della dichiarazione di conformità sui documenti cartacei depositati, determinano l'inesistenza dell'atto per nullità e/o inesistenza della notifica, in quanto non può essere ritenuta provata la spedizione e la ricezione dello specifico atto.

Protocollazione delle PEC

L'obbligo di conservazione dei messaggi di posta elettronica certificata è da ricondurre agli articoli 2214 e 2220 del Codice Civile.

Gli obblighi di conservazione delle PEC, in quanto documenti informatici, sono da ricercarsi anche all'art. 43 del CAD che al comma 1 prescrive in generale: *"i documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento di cui è prescritta la conservazione per legge o regolamento, ove riprodotti su supporti informatici sono validi e rilevanti a tutti gli effetti di legge, se la riproduzione e la conservazione nel tempo sono effettuate in modo da garantire la conformità dei documenti agli originali stabilite ai sensi dell'articolo 71"* (quelle attualmente vigenti sono contenute nel DPCM del 3 dicembre 2013). Nel successivo comma 3 dello stesso articolo si stabilisce, in particolare, che *"i*

[7] Gli atti e i provvedimenti inviati dalla PA alle imprese tramite tale strumento sono in grado di produrre gli effetti giuridici (cd. integrazione dell'efficacia) che l'ordinamento ricollega alla conoscenza dell'atto da parte del destinatario e consentono alla PA di assolvere agli obblighi connessi alla partecipazione del privato al procedimento (art. 48, co. 2, CAD e art. 149-bis c.p.c.). Quanto alla fase di integrazione dell'efficacia dei provvedimenti recettizi, limitativi della sfera giuridica del privato (es. sanzioni, espropriazioni, ordini) che, per produrre effetti, devono essere notificati o comunicati al destinatario (art. 21-bis, L. n. 41 del 1990), la notifica a mezzo PEC è idonea a rendere efficace il provvedimento nei confronti del destinatario medesimo. Anche nelle ipotesi in cui il provvedimento non sia recettizio (es. provvedimento ampliativo della sfera giuridica privata), la notifica tramite PEC è idonea a far decorrere comunque i termini processuali per l'eventuale impugnazione del provvedimento.

[8] Si veda testo integrale della sentenza emanata da CTP Avellino 556/2014. Tar Lazio - Roma, Sez. III bis, con decreto 12 novembre 2013, n. 23921 riguardo alla questione sui presupposti ed i requisiti di ammissibilità in giudizio per provare l'avvenuta notifica di un atto a mezzo PEC, ha ritenuto che la prova della notifica a mezzo PEC dovrà essere fornita in giudizio attraverso l'allegazione della ricevuta di consegna completa, che giustifica tale conclusione dall'esigenza di assicurare certezza dell'avvenuta ricezione dell'atto da parte del destinatario, in considerazione del carattere sostitutivo della procedura telematica rispetto a quella cartacea. TAR Campania - Napoli, Sez. VI, nella sentenza 3 aprile 2013 n. 1756, sostiene che la mancanza della firma digitale sul provvedimento notificato determina incertezza sulla amministrazione o e la riconducibilità in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata.

documenti informatici, di cui è prescritta la conservazione per legge o regolamento, possono essere archiviati per le esigenze correnti anche con modalità cartacee e sono conservati in modo permanente con modalità digitali, nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71".

Suggerimenti:

⇒ Per i messaggi PEC inviati: conservare la "ricevuta di consegna completa" formata dal file "postacert.eml", contenente il messaggio originale, completo di testo ed eventuali allegati, e il file "daticert.xml" che riproduce l'insieme di tutte le informazioni relative all'invio (mittente, gestore del mittente, destinatari, oggetto, data e ora dell'invio, codice identificativo del messaggio).

⇒ Per i messaggi PEC ricevuti: conservare la busta di trasporto con il file "postacert.eml", contenente il messaggio originale, completo di testo ed eventuali allegati, e il file "daticert.xml" che riproduce l'insieme di tutte le informazioni relative all'invio (mittente, gestore del mittente, destinatari, oggetto, data e ora dell'invio, codice identificativo del messaggio).

Inoltre, quando si è in presenza di un documento allegato al messaggio PEC firmato digitalmente, per evitare che alla scadenza del certificato (che non ha durata superiore a tre anni) la sottoscrizione perda i requisiti previsti dall'articolo 2702 del Codice Civile e venga declassata ai sensi dell'articolo 2712 C.C., è opportuno portare in conservazione il messaggio PEC e i relativi allegati sottoscritti digitalmente.

Costituiscono **PRATICHE** DI CONSERVAZIONE utilizzate frequentemente per messaggi PEC e documenti allegati, MA **NON CORRETTE**:

- l'archiviazione semplice delle PEC nel proprio computer o server. In questo caso non è garantito il valore legale in quanto non si è in presenza di conservazione a norma;
- la stampa su carta e l'archiviazione fisica del documento. La tradizionale conservazione della stampa del documento PEC non garantisce la conformità all'originale informatico.

III.2.4 Prospettive legislative

Prospettive de jure condendo: PEC e Regolamento europeo eIDAS

Per completare il quadro – normativo ed operativo – relativo alla PEC risulta necessario soffermarsi sul Regolamento eIDAS che, oltre ad intervenire in materia di firme elettroniche, ha determinato la nascita di servizi di identificazione elettronica, noti in inglese con il termine Registered Electronic Delivery (di seguito per semplicità "RED"), che si vengono ad affiancare alla PEC, che nel prossimo futuro avrà la necessità di coordinarsi con essi[9].

[9] La stessa novellata definizione di "*domicilio digitale*", attualmente presente nel CAD, è chiaramente finalizzata a tale obbiettivo anche al fine di superare l'annosa questione relativa alla non interoperabilità dei vari sistemi di PEC presenti nei vari Stati a livello europeo. Secondo l'art. 1, comma 1, lett. n-ter), CAD si intende per "domicilio digitale": l'indirizzo di posta elettronica certificata o altro servizio elettronico di recapito certificato qualificato di cui al Linee Guida (UE) 23 luglio 2014 n. 910 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, di seguito "Linee Guida eIDAS", che consenta la prova del momento di ricezione di una comunicazione tra i soggetti di cui all'articolo 2, comma 2, e i soggetti giuridici, che sia basato su standard o norme riconosciute nell'ambito dell'unione europea.

Il Regolamento eIDAS definisce il "servizio elettronico di recapito certificato" come "un servizio che consente la trasmissione di dati fra terzi per via elettronica e fornisce prove relative al trattamento dei dati trasmessi, fra cui prove dell'avvenuto invio e dell'avvenuta ricezione dei dati, e protegge i dati trasmessi dal rischio di perdita, furto, danni o di modifiche non autorizzate"[10]; nello specifico vengono definiti altresì i "servizi elettronici di recapito qualificato certificato"[11] quelli che "soddisfano i requisiti seguenti:

a) sono forniti da uno o più prestatori di servizi fiduciari qualificati;

b) garantiscono con un elevato livello di sicurezza l'identificazione del mittente;

c) garantiscono l'identificazione del destinatario prima della trasmissione dei dati;

d) l'invio e la ricezione dei dati sono garantiti da una firma elettronica avanzata o da un sigillo elettronico avanzato di un prestatore di servizi fiduciari qualificato in modo da escludere la possibilità di modifiche non rilevabili dei dati;

e) qualsiasi modifica ai dati necessaria al fine di inviarli o riceverli è chiaramente indicata al mittente e al destinatario dei dati stessi;

f) la data e l'ora di invio e di ricezione e qualsiasi modifica dei dati sono indicate da una validazione temporale elettronica qualificata.

Qualora i dati siano trasferiti fra due o più prestatori di servizi fiduciari qualificati, i requisiti di cui alle lettere da a) a f) si applicano a tutti i prestatori di servizi fiduciari qualificati."[12]

Merita soffermarsi su chi sia il prestatore di servizi fiduciari qualificato[13]: tale prestatore risulterà essere "qualificato" allorquando lo stesso "presta uno o più servizi fiduciari qualificati e cui l'organismo di vigilanza assegna la qualifica di prestatore di servizi fiduciari qualificato"[14].

~~Da tale, seppur sintetica, analisi~~ del testo normativo si può chiaramente evincere come i servizi RED e PEC siano a prima vista similari ma non identici; in particolare si può affermare che la PEC soddisfi i requisiti previsti dal Regolamento eIDAS per quanto concerne il servizio elettronico di recapito certificato, ma non soddisfi integralmente i requisiti previsti sempre dal medesimo Regolamento per quanto concerne il servizio elettronico di recapito certificato qualificato[15].

Tali discrasie normative dovranno essere corrette nel prossimo futuro attraverso una parziale revisione delle "regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata" attualmente in vigore, al fine di poter permettere al sistema di PEC del

[10] Art. 3, comma 1, n. 36, Linee Guida eIDAS.

[11] Art. 3, comma 1, n. 37, Linee Guida eIDAS.

[12] Art. 44, comma 1, Linee Guida eIDAS, Requisiti per i servizi elettronici di recapito certificato qualificati

[13] Ex art. 3, comma 1, n. 19, Linee Guida eIDAS il "*prestatore di servizi fiduciari*" risulta essere "*una persona fisica o giuridica che presta uno o più servizi fiduciari, o come prestatore di servizi fiduciari qualificato o come prestatore di servizi fiduciari non qualificato*

[14] Art. 3, comma 1, n. 20, Linee Guida eIDAS. L'organismo di vigilanza citato – meglio noto come "*organismo di valutazione della conformità*" – risulta essere "*un organismo ai sensi dell'articolo 2, punto 13, del Linee Guida (CE) n. 765/2008[19], che è accreditato a norma di detto Linee Guida come competente a effettuare la valutazione della conformità del prestatore di servizi fiduciari qualificato e dei servizi fiduciari qualificati da esso prestati*" (Art. 3, comma 1, n. 18, Linee Guida eIDAS).

[15] Nello specifico non risulta prevista la verifica certa dell'identità del richiedente la casella di PEC così come l'obbligatorietà, da parte del gestore, di sottoporsi a delle verifiche di conformità da parte degli organismi designati.

nostro paese di garantire l'operatività ed il valore probatorio di elevato livello che viene richiesto dalla novellata normativa europea.

III.2.5 Titolarità, competenze, responsabilità ed utilizzo delle PEC nell'ambito della Provincia di Pescara

La casella di Posta Elettronica Certificata istituzionale della Provincia di Pescara, inserita nell'Indice delle Pubbliche Amministrazioni (IPA) è:

provincia.pescara@legalmail.it

La provincia di Pescara fornisce inoltre a tutte strutture in cui è articolata la propria organizzazione una casella PEC per la comunicazione con tutti quei soggetti esterni muniti di PEC con cui la struttura intrattiene rapporti istituzionali.

Ulteriori caselle PEC potranno essere assegnate laddove finalizzate a specifiche applicazioni.

Per ogni casella PEC viene individuato, con determinazione dirigenziale, il soggetto o i soggetti utilizzatori, cui sono fornite le credenziali di accesso per l'utilizzo del servizio PEC; diversamente l'unico soggetto responsabile dell'utilizzo della specifica PEC rimane il Dirigente di Settore.

Il soggetto utilizzatore del servizio PEC è tenuto a seguire le indicazioni di corretto utilizzo specificate per la posta elettronica ordinaria, in particolare per quanto concerne la **conservazione dei messaggi di posta nel sistema di protocollazione informatica dell'Ente.**

Da ciò deriva che la **dismissione di una casella di posta elettronica certificata** vada obbligatoriamente preceduta dall'accertamento, da parte del responsabile indicato in determinazione o da parte del Dirigente di settore, dell'avvenuta protocollazione del suo contenuto.

La richiesta di dismissione va protocollata ed inviata al Servizio Sistemi Informativi, attraverso il modello specifico (allegato alle presenti Linee Guida); il Servizio Sistemi Informativi procederà tecnicamente alla richiesta di disattivazione presso il fornitore.

Si specifica che le caselle di posta elettronica certificata non appartengono al dominio dell'ente, ma l'ente si avvale di providers esterni, così come previsto dalla norma, pertanto il Servizio Sistemi Informativi non ha alcuna possibilità di intervenire sui server di tali caselle, né responsabilità tecniche od operative nell'ambito della gestione delle stesse.

La pubblicità degli indirizzi di posta elettronica certificata destinata ad essere noti è a cura della Segreteria Generale, che dovrà iscrivere ed aggiornare gli stessi nell'Indice delle Pubbliche Amministrazioni (IPA) e verificarne le concordanze con quanto prescritto in merito alla fatturazione elettronica.

Su richiesta, la Segreteria Generale potrà avvalersi della consulenza tecnica del Servizio Sistemi Informativi.

TITOLO IV Monitoraggio e controlli

La Provincia di Pescara adotterà ogni accorgimento tecnico necessario a tutelare l'ente da eventuali comportamenti non consentiti, salvaguardando il rispetto della libertà e della dignità dei lavoratori; gli eventuali trattamenti effettuati saranno ispirati a canoni di trasparenza e rispetteranno il principio di pertinenza e non eccedenza.

IV.1 Monitoraggi

La Segreteria Generale, attraverso il Servizio Sistemi Informativi, effettua monitoraggi periodici su dati anonimi allo scopo di verificare l'attuazione delle presenti Linee Guida, i possibili rischi alla sicurezza informatica e le possibili problematiche inerenti l'utilizzo degli strumenti informatici.

Questi monitoraggi si possono classificare in:

- analisi del traffico di rete: effettuati attraverso specifici log dei dispositivi di rete;
- analisi del traffico Internet: effettuati attraverso specifici log dei dispositivi di connessione ad Internet;
- inventario Hardware e Software: effettuati attraverso procedure prevalentemente automatiche per le apparecchiature collegate in rete ed in maniera semiautomatica per le altre macchine. Il monitoraggio delle risorse hardware e software non coinvolge in alcun modo i dati personali ed i documenti presenti sulle singole postazioni di lavoro e viene effettuato per finalità organizzative e gestionali.

I dati del traffico telematico saranno gestiti secondo le modalità e le tempistiche previste dalla normativa vigente in materia di sicurezza dei dati del traffico telefonico e telematico.

L'ente si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà pericolosa per la sicurezza del sistema informatico ovvero acquisita o installata in violazione delle presenti Linee Guida.

IV.2 Controlli

La Provincia di Pescara si riserva di effettuare controlli per verificare il rispetto delle Linee Guida.

Riguardo a tali controlli le presenti Linee Guida costituiscono preventiva e completa informazione nei confronti dei dipendenti.

In base al principio di correttezza (richiamato all'I.5. Linee Guida Generali) l'eventuale trattamento deve essere ispirato ad un canone di trasparenza, come prevede anche la disciplina di settore (Art. 4, secondo comma, Statuto dei lavoratori).

I dati devono essere gestiti soltanto dai soggetti preventivamente designati quali responsabili e incaricati del trattamento, come precisa l'Art. 30 del Codice sulla Privacy.

Nel caso in cui emerga un evento dannoso, una situazione di pericolo o utilizzi non aderenti alle presenti Linee Guida, che non siano stati impediti con preventivi accorgimenti tecnici o rilevati durante i monitoraggi o da attività di gestione degli strumenti informatici, la Segreteria Generale, attraverso il Servizio Sistemi Informativi, potrà adottare le eventuali misure che consentano la verifica di tali comportamenti preferendo, per quanto possibile, un controllo preliminare su dati aggregati riferiti all'intera Struttura organizzativa o a sue articolazioni.

Il controllo su dati anonimi terminerà in una comunicazione al Responsabile della Struttura analizzata che si preoccuperà di inviare un avviso generalizzato relativo a un utilizzo non corretto degli strumenti aziendali, invitando i destinatari ad attenersi scrupolosamente alle presenti Linee Guida.

Qualora le anomalie e irregolarità dovessero persistere, si procederà circoscrivendo l'invito al personale afferente alla Struttura in cui è stata rilevata l'anomalia.

In caso di reiterate anomalie o irregolarità, saranno effettuati controlli su base individuale.

In nessun caso, a eccezione di specifica richiesta da parte dell'Autorità Giudiziaria, verranno poste in essere azioni sistematiche quali:

- la lettura e la registrazione dei messaggi di posta elettronica (al di là di quanto tecnicamente necessario per lo svolgimento del servizio di gestione e manutenzione della posta elettronica);

- la riproduzione ed eventuale memorizzazione delle pagine web visualizzate dal lavoratore;

- la memorizzazione di quanto visualizzato sul monitor.

Oltre a ciò la Provincia di Pescara si riserva di effettuare specifici controlli sui software caricati sui personal computer utilizzati dai dipendenti al fine di verificarne la regolarità sotto il profilo delle autorizzazioni e delle licenze, nonché, in generale, la conformità degli stessi alla normativa vigente e, in particolare, alle disposizioni in materia di proprietà intellettuale.

Oltre a tali controlli di carattere generale, la Provincia di Pescara si riserva comunque le facoltà previste dalla normativa vigente di effettuare specifici controlli *ad hoc* nel caso di segnalazioni di attività che hanno causato danno all'Amministrazione, che ledono diritti di terzi o che, comunque, sono illegittime.

IV.3 RESPONSABILITA'

Le presenti Linee Guida assumono valore di direttiva e pertanto vincolanti per tutto il personale dell'Ente: il mancato rispetto o la violazione delle indicazioni ivi contenute è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dai vigenti CCNL, nonché con le azioni civili e penali conseguenti previste dalla normativa vigente in materia (in particolare Dlgs 297 16/4/94 e art 2043 CC).

Ogni dipendente dovrà assumersi la piena responsabilità per le proprie azioni e dovrà farsi garante per l'ente e tenerlo indenne da responsabilità e richieste di rimborsi di danni, avanzate da soggetti terzi.

TITOLO V Applicabilità a soggetti diversi dai dipendenti

Con riferimento ai collaboratori e/o prestatori d'opera (consulenti, stagisti, etc.), qualora questi per l'espletamento del loro incarico si servissero degli strumenti e servizi informatici della Provincia di Pescara, deve essere previsto nell'ambito del contratto l'obbligo di rispettare le presenti Linee Guida, con diritto dell'Amministrazione, nei casi di violazione di particolare gravità, di risolvere il contratto stesso, e comunque di chiedere i danni per l'eventuale nocumento subìto.

E' disposto l'obbligo per i collaboratori di sottoscrivere la specifica dichiarazione di manleva, allegata alle presenti Linee Guida.

Non è in alcun modo ed in nessuna forma consentito l'accesso da parte di personale esterno - sebbene anche contrattualizzato - al sistema di gestione documentale dell'Ente, in particolar modo è inibito l'accesso a detto personale al sistema di protocollazione informatica in uso all'ente.

esempio

Oggetto: procedura di disattivazione casella PEC

Si richiede la disattivazione della casella PEC _____

A tal fine, dichiaro che si è ottemperato alle disposizioni normative in merito alla gestione documentale e al protocollo informatico, in particole la gestione del contenuto della casella di posta è stato trattato ai sensi degli artt. 20, 40, 40bis, 43 e 44 del Codice dell'Amministrazione Digitale, così come integrato dal D.lgs 179/2016 e successive disposizioni.

Si autorizza pertanto il gestore ad effettuare la cancellazione della casella PEC e del relativo contenuto.

Parimenti si comunica la effettiva registrazione della/delle PEC di cui sopra presso la banca dati IPA e se ne conferma la rimozione, avendo avuto cura di verificare quanto prescritto e disposto in merito alle incidenze afferenti alla fatturazione elettronica.

Oppure

Si attesta altresì che le caselle PEC di cui si chiede la dismissione non sono/sono registrate presso la banca dati IPA.

Cordiali saluti

Allegato alle Linee Guida disciplinanti l'utilizzo degli strumenti e dei servizi informatici, di internet, della posta elettronica ordinaria e certificata dell'Amministrazione provinciale di Pescara"

DECALOGO PER UN UTILIZZO CONSAPEVOLE DELLA PEC

1) ACCERTARSI CHE LA CONFIGURAZIONE DELLA RICEVUTA DI AVVENUTA CONSEGNA PREVEDA QUELLA "COMPLETA"

2) RICORDARSI CHE L'ESITO POSITIVO O NEGATIVO DELL'INVIO VIENE COMUNICATO AL MITTENTE ENTRO 24 ORE

3) VERIFICARE SEMPRE CHE LA PROPRIA CASELLA DI PEC SIA CAPIENTE

4) NON ECCEDERE I LIMITI DIMENSIONALI DEL MESSAGGIO E DEGLI ALLEGATI, ABITUALMENTE PARI A 20 MEGABYTES COMPLESSIVI

5) L'UTILIZZO DELLA PEC E' OBBLIGATORIA PER LE COMUNICAZIONI CON AZIENDE, PROFESSIONISTI O ALTRE P.A. E NON E' CONSENTITO INVIARE POSTA ATTRAVERSO CANALI TRADIZIONALI (RACCOMANDATE, POSTA CELERE ETC)

6) SOTTOSCRIVERE SEMPRE CON FIRMA DIGITALE LA DOCUMENTAZIONE INVIATA VIA PEC. IN GENERALE, GLI ALLEGATI CHE NECESSITANO DI FIRMA, DEVONO ESSERE SOTTOSCRITTI CON FIRMA DIGITALE IN QUANTO LA PEC E' ESCLUSIVAMENTE UNA MODALITA' DI INVIO E NON HA VALORE DI SOTTOSCRIZIONE DEI DOCUMENTI

7) ALLEGARE IN GIUDIZIO, PER DIMOSTRARE L'INVIO O IL RICEVIMENTO DI UN DOCUMENTO TRAMITE PEC:

   a) LA STAMPA DELL'ATTO NOTIFICATO IN FORMATO PDF CON FIRMA DIGITALE, SE SI TRATTA DI ALLEGATO;
   b) LE RICEVUTE DI ACCETTAZIONE E CONSEGNA COMPLETA DELLA PEC;
   c) IL CERTIFICATO DI FIRMA DIGITALE DEL NOTIFICANTE;
   d) IL CERTIFICATO DI FIRMA DEL GESTORE DI PEC.

8) PROTOCOLLARE SEMPRE LE PEC E I RELATIVI ALLEGATI, EVITANDO LA SEMPLICE ARCHIVIAZIONE DEI FILE SU PC E/O LA STAMPA DELLE RICEVUTE. IN PARTICOLARE:

   a. PER LE PEC INVIATE: CONSERVARE LA "RICEVUTA DI CONSEGNA COMPLETA" FORMATA DAL FILE "*POSTACERT.EML"*, CONTENENTE IL MESSAGGIO ORIGINALE, COMPLETO DI TESTO ED EVENTUALI ALLEGATI E IL FILE "*DATICERT.XML"* CHE RIPRODUCE L'INSIEME DI TUTTE LE INFORMAZIONI RELATIVE ALL'INVIO (MITTENTE, GESTORE DEL MITTENTE, DESTINATARI, OGGETTO, DATA E ORA DELL'INVIO, CODICE IDENTIFICATIVO DEL MESSAGGIO).
   b. PER LE PEC RICEVUTE: CONSERVARE LA BUSTA DI TRASPORTO CON IL FILE "*POSTACERT.EML"* E IL FILE "*DATICERT.XML"*

9) RICORDARE CHE LA CONSERVAZIONE A NORMA E' NECESSARIA PER LE PEC CON ALLEGATI SOTTOSCRITTI CON FIRMA DIGITALE: SOLO COSI E' POSSIBILE MANTENERE IL VALORE LEGALE DI SCRITTURA PRIVATA DEGLI ALLEGATI ANCHE OLTRE L'EVENTUALE SCADENZA DEL CERTIFICATO DI SOTTOSCRIZIONE (QUEST'ULTIMO, DI NORMA, NON HA DURATA SUPERIORE A TRE ANNI)

10) COMUNICARE TEMPESTIVAMENTE EVENTUALI VARIAZIONI DELL'INDIRIZZO PEC ALL' IPA E RICORDARSI DI AGGIORNARE LA SEZIONE DEL SITO ISTITUZIONALE.

PROVINCIA
DI PESCARA

Allegato alle Linee Guida disciplinanti l'utilizzo degli strumenti e dei servizi informatici, di internet, della posta elettronica ordinaria e certificata dell'Amministrazione provinciale di Pescara"

Al Segretario Generale

p.c.

Al
Servizio Sistemi Informativi

OBBLIGHI DI RISERVATEZZA E GESTIONE DEI DATI

DICHIARAZIONE LIBERATORIA DI RESPONSABILITA'

Il/La sottoscritto/a _____

In qualità di (collaboratore esterno, consulente, tirocinante, altro...)_____
Indirizzo: _____

Data e luogo di nascita _____

Telefono _____ e-mail _____@_____pec_____

Durata dell' accesso: _____
Riferimento del responsabile interno (Dirigente e Responsabile di Servizio)

Consapevole che le dichiarazioni mendaci, la falsità negli atti e l'uso di atti falsi sono puniti con le sanzioni previste dalle leggi in materia;

dichiara

- di aver preso visione e di aver compreso e accettato quanto esposto nelle Linee Guida disciplinati l'utilizzo degli strumenti e dei servizi informatici, di internet, della posta elettronica ordinaria e certificata dell'Amministrazione Provinciale di Pescara";
- di sollevare la Provincia di Pescara e il Responsabile dei Sistemi Informativi dell'Ente da qualsiasi responsabilità inerente l'accesso e l'utilizzo delle strumentazioni informatiche in uso presso la Provincia stessa, per gli usi richiesti.
- di essere responsabile della conservazione, con la massima riservatezza e diligenza, del codice di identificazione (nome) e della parola chiave (password) che consentono l'accesso al dominio aziendale e di comunicare tempestivamente, in forma scritta, l'eventuale smarrimento della password di accesso alla Segreteria Generale dell'Ente, nonché al servizio Sistemi Informativi;
- di essere consapevole che la provincia di Pescara può utilizzare i dati contenuti nella presente autocertificazione esclusivamente nell'ambito e per i fini istituzionali propri della Pubblica Amministrazione;
di aver attentamente letto ed espressamente accettato tutti i termini e le condizioni di utilizzo del servizio espressamente indicate nel presente accordo.

Condizioni e norme di utilizzo dei servizi

1**. Oggetto**

1.1 Il presente accordo definisce le condizioni generali di gestione ed utilizzo degli strumenti e dei servizi informatici della Provincia di Pescara (in seguito "Ente");
1.2 Il servizio è gratuito, senza alcun onere e/o costo di installazione per l'utente del servizio;
1. 3 Con il primo utilizzo del servizio, l'utente dichiara di aver attentamente letto ed espressamente accettato tutti i termini e le condizioni di utilizzo del servizio espressamente indicate nel presente accordo.

PROVINCIA
DI PESCARA

1.4 In nessun caso l'Ente può essere ritenuto responsabile del mancato e/o inesatto adempimento da parte dell'utente di ogni eventuale procedura di legge e regolamento in relazione al presente accordo.

2. Durata del servizio e efficacia dell'accordo

2.1 Il presente accordo ha efficacia dalla data in cui l'Ente avvia il servizio sulla base e in seguito all'accettazione da parte dell'utente delle condizioni contenute nel presente accordo implicitamente.
2.2 L'Ente si riserva il diritto di sospendere e/o interrompere e/o variare, in qualsiasi momento e senza onere di preavviso, il servizio e non potrà comunque essere considerato responsabile nei confronti sia dell'utente che di terzi per la intervenuta sospensione ovvero interruzione. In tal caso, cesserà immediatamente ogni diritto dell'utente all'utilizzazione del servizio.
2.3 L'Ente potrà integrare e/o modificare unilateralmente, in qualsiasi momento e senza preavviso, le condizioni e i termini del presente accordo. Le eventuali modifiche e/o integrazioni devono essere comunicate all'utente, tramite comunicazione scritta.

3. Obblighi dell'utente

3.1 L'utente s'impegna a non consentire l'utilizzo del servizio a terzi, del cui comportamento si assume, ai sensi del presente accordo, comunque la responsabilità.
3.2 L'utente si impegna a non utilizzare il servizio per effettuare comunicazioni che arrechino danni o turbative all'Ente o a terzi o che violino le leggi e i regolamenti vigenti. In particolare, in via esemplificativa e non esaustiva, l'utente si impegna a non utilizzare in modo improprio gli strumenti messi a disposizione dall'Ente, arrecando danno per incuria o imperizia all'Ente.
3.3 L'utente si impegna a:

- utilizzare il servizio per i fini per cui è stato concesso;
- non trasferire a terzi i dati presenti nei data base a cui ha accesso se non effettivamente necessario e con relativa autorizzazione del referente di area;;
- non violare il segreto della corrispondenza personale e il diritto alla riservatezza;
- rispettare le regole e le indicazioni operative che gli verranno date dall'ente;

3.4 L'Ente si riserva il diritto di recedere unilateralmente e in qualsiasi momento, senza obbligo di alcuna motivazione, senza preavviso dal presente accordo qualora determini, a suo insindacabile giudizio, che l'utente abbia violato anche solo uno degli obblighi ivi indicati. Tale violazione potrà dare luogo anche ad azioni di rivalsa e/o risarcimento.

4. Responsabilità

4.1 L'utente è responsabile di ogni violazione del presente accordo e si impegna a manlevare, sostanzialmente e processualmente, l'Ente, ed a tenerlo indenne da qualsiasi pretesa anche di terzi a qualsivoglia titolo, comunque avente causa della violazione del presente accordo e/o dalla violazione di leggi o regolamenti o provvedimenti amministrativi.
4.2 L'utente si assume ogni responsabilità ed onere circa il contenuto e le forme delle comunicazioni realizzate tramite il servizio e si impegna a tenere indenne l'Ente da ogni pretesa o azione che dovesse essere rivolta all'ente medesimo da qualunque soggetto, in conseguenza a tali comunicazioni. Con tale presa di responsabilità, l'utente esonera espressamente l'Ente da qualunque responsabilità e onere di accertamento e/o controllo al riguardo.
4.3 L'utente s'impegna a tenere indenne l'Ente da tutte le perdite, danni, costi e oneri, ivi comprese le eventuali spese legali, che dovessero essere sostenute dal gestore in conseguenza dell'utilizzo del servizio messo a disposizione dell'utente.

5. Riservatezza

5.1 L'accesso al servizio avviene mediante un codice di identificazione dell'utente (username) e una parola chiave (password). L'utente è informato del fatto che la conoscenza delle proprie credenziali da parte di terzi consentirebbe a questi ultimi l'utilizzo del servizio in nome dell'utente medesimo. **L'utente è il solo ed unico responsabile della conservazione e della riservatezza delle proprie credenziali** e, conseguentemente, rimane il solo ed unico responsabile per tutti gli usi ad essa connessi o correlati, (ivi compresi danni e conseguenze pregiudizievoli arrecati all'ente e/o a terzi) siano dal medesimo utente autorizzati ovvero non autorizzati.
5.2 L'utente si impegna a comunicare quanto prima all'ente l'eventuale furto, smarrimento o perdita della password. In ogni caso, resta inteso che l'utente sarà responsabile delle conseguenze derivanti dal furto, dalla perdita o dallo smarrimento di tale password.
5.3 L'utente prende atto ed accetta l'esistenza del registro dei collegamenti (noto come "log") mantenuto dall'Ente, e l'Ente adotta misure tecniche ed organizzative necessarie a garantire la riservatezza di tale registro. Il registro dei collegamenti potrà essere esibito solo all'autorità giudiziaria, dietro esplicita richiesta.

6. Legge applicabile e foro competente

6.1 Il presente accordo è disciplinato dalle leggi dello Stato Italiano. Per quanto non espressamente previsto nel presente accordo si applicano le norme vigenti.
6.2 Per tutte le controversie che dovessero insorgere in relazione al presente accordo, incluse le controversie nell'interpretazione, efficacia, validità ed esecuzione dell'accordo sarà competente in via esclusiva il Foro di Pescara.
6.3 Nel caso in cui alcune disposizioni contenute nel presente accordo fossero ritenute nulle e/o invalide e/o inefficaci le restanti dovranno comunque ritenersi pienamente valide ed efficaci.

il richiedente dovrà fornire in allegato a questa dichiarazione, se non firmata digitalmente, la fotocopia del documento d'identità (Decreto decreto legge 27 luglio 2005 n.144).

In fede data_____

firma utente firma del garante interno

PROVINCIA DI PESCARA

Allegato alla Decreto n. DDP-2018-0000066 del 17/05/2018

Oggetto: Linee Guida disciplinanti l'utilizzo degli strumenti e dei servizi informatici, di internet, della posta elettronica ordinaria e certificata della Provincia di Pescara

Pareri espressi dai responsabili dei Servizi ai sensi dell'art. 49, 1° comma del Decreto legislativo n. 267 del 18 agosto 2000 – Testo unico delle leggi sull'ordinamento degli Enti locali:

Parere sulla regolarità tecnica: Positivo

Il sottoscritto, consapevole delle sanzioni penali cui incorre nel caso di dichiarazione mendace o contenente dati non rispondenti a verità, come stabilito dall'art. 76 del D.P.R. n. 445/2000, ai sensi di quanto previsto dall'art. 47 del medesimo D.P.R., dichiara di non trovarsi in una situazione di conflitto di interesse, anche potenziale, così come disposto dall'art. 6, comma 2 e dall'art. 7 del Codice di Comportamento di cui al D.P.R. n. 62/2013.

Pescara, lì 10/05/2018

Il Responsabile
Avv. CARLO PIROZZOLO

Parere sulla regolarità contabile: Privo di rilievo contabile

Il sottoscritto, consapevole delle sanzioni penali cui incorre nel caso di dichiarazione mendace o contenente dati non rispondenti a verità, come stabilito dall'art. 76 del D.P.R. n. 445/2000, ai sensi di quanto previsto dall'art. 47 del medesimo D.P.R., dichiara di non trovarsi in una situazione di conflitto di interesse, anche potenziale, così come disposto dall'art. 6, comma 2 e dall'art. 7 del Codice di Comportamento di cui al D.P.R. n. 62/2013.

Pescara, lì 17/05/2018

Il Responsabile
Dott.ssa VALENTINA LONGO

PROVINCIA DI PESCARA

Letto, approvato e sottoscritto:

Il Presidente Della Provincia
ANTONIO DI MARCO

Il Segretario Generale
Avv. CARLO PIROZZOLO

Certificato di pubblicazione e trasmissione ai capigruppo

Copia della presente deliberazione è stata pubblicata all'Albo Pretorio di questa Provincia, dove rimarrà affissa per 15 gg. consecutivi, dal giorno _____

La stessa viene trasmessa, in elenco, ai capigruppo consiliari ai sensi dell'art. 125 del D.lgs. n. 267/2000.

Pescara, lì _____

Il Responsabile
Dott.ssa ELISA GIZZARELLI

Certificato di esecutività

La presente deliberazione è divenuta esecutiva in data 17/05/2018

Essendo stata dichiarata immediatamente esguibile ai sensi dell'art.134, comma 4, del D.lgs. n. 267/2000.

Pescara, lì 17/05/2018

Il Responsabile
Dott.ssa ELISA GIZZARELLI

Certificato di avvenuta pubblicazione

Si attesta che la presente deliberazione è stata affissa all'albo pretorio per 15 giorni consecutivi dal _____ al _____

Pescara, lì _____

Il Responsabile
Dott.ssa ELISA GIZZARELLI
