Ministero dell'Ambiente e della Tutela del Territorio e del Mare

DIREZIONE GENERALE PER GLI AFFARI GENERALI ED IL PERSONALE

IL DIRETTORE GENERALE

Roma,

A tutto il personale del Ministero
dell'ambiente e della tutela del territorio
e del mare
Sede

OGGETTO: Adozione Regolamento per l'utilizzo della posta elettronica e della rete internet nel Ministero dell'ambiente e della tutela del territorio e del mare.

Si informa che, in attuazione delle previsioni di cui all'articolo 3.2 della deliberazione dell'1 marzo 2007 (G.U. n. 58 del 10 marzo 2007) del Garante per la protezione dei dati personali, contenente Linee Guida in materia di corretto utilizzo della posta elettronica e della rete internet nel rapporto di lavoro, lo scrivente, con decreto direttoriale n. DEC/SI/20/2010 del 29 marzo 2010, ha adottato l'allegato Regolamento.

Si ritiene utile far presente che sullo schema del Regolamento di cui trattasi, elaborato dalla competente ex Divisione III – Sistemi Informativi – della scrivente Direzione, è stato espresso in data 4 marzo 2010 il favorevole parere del Garante per la protezione dei dati personali, in esito alle procedure di consultazione preventiva avviate ai sensi dell'art. 154, commi 4 e 5, del Codice in materia di protezione dei dati personali (decreto legislativo 30 giugno 2003, n. 196).

Il Regolamento viene affisso nei previsti spazi a disposizione dell'Amministrazione, accessibili a tutti i lavoratori, pubblicato sul sito web del Ministero e diffuso a tutte le caselle di posta elettronica in uso al personale.

Cordiali saluti.

Nicola Stolfo

gdp

DEC/SI/20/2010

Ministero dell'Ambiente e della Tutela del Territorio e del Mare

DIREZIONE GENERALE PER GLI AFFARI GENERALI E DEL PERSONALE

IL DIRETTORE GENERALE

VISTO il decreto legislativo 30 marzo 2001, n. 165;

VISTO il Decreto del Presidente della Repubblica 3 agosto 2009, n. 140 "Regolamento recante riorganizzazione del Ministero dell'ambiente e della tutela del territorio e del mare";

VISTO il Decreto Ministeriale n. 135 del 2 dicembre 2009, relativo all'individuazione degli uffici di livello dirigenziale non generale del Ministero dell'ambiente e della tutela del territorio e del mare, registrato alla Corte dei Conti in data 12 gennaio 2010;

VISTA la Legge 20 maggio 1970, n. 300, recante *"Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e nell'attività sindacale nei luoghi di lavoro e norme sul collocamento"* (Statuto dei lavoratori);

VISTO il decreto legislativo 30 giugno 2003, n. 196, recante "Codice in materia di protezione dei dati personali";

VISTO il decreto del Ministro dell'ambiente e della tutela del territorio e del mare in data 22 maggio 2007, n. 105, recante *"Regolamento per il trattamento dei dati sensibili e giudiziari, in attuazione degli articoli 20 e21 del decreto legislativo 30 giugno 2003, n. 196"*;

VISTE le linee guida del Garante per la protezione dei dati personali, emanate con delibera n. 13 dell'1 marzo 2007 (G.U. n. 58 del 10 marzo 2007), in tema di corretto utilizzo della posta elettronica e della rete Internet nel rapporto di lavoro e, in particolare, il punto 3.2. *"Linee guida"*, laddove è previsto che: *"In questo quadro, può risultare opportuno adottare un Regolamento interno redatto in modo chiaro e senza formule generiche, da pubblicizzare adeguatamente (verso i singoli lavoratori, nella rete interna, mediante affissioni sui luoghi di lavoro con modalità analoghe a quelle previste dall'art. 7 dello Statuto dei lavoratori,.....) e da sottoporre ad aggiornamento periodico"*;

gdp

VISTO lo schema di Regolamento per l'utilizzo della posta elettronica e della rete internet nel Ministero dell'ambiente e della tutela del territorio e del mare, elaborato dalla competente Divisione III – Sistemi Informativi – della scrivente Direzione Generale, in attuazione di quanto previsto dal punto 3.2. delle sopra citate Linee guida;

SENTITE le OO.SS. di cui all'articolo 8, commi 1 e 2, del CCNL 1999 relativamente allo schema del Regolamento sopra citato, espressamente interessate con nota prot. n. 17565/PR4 in data 13 novembre 2009;

ACQUISITO sullo schema del Regolamento di cui trattasi il favorevole parere da parte dell'Autorità garante per il trattamento dei dati personali, emesso in data 4 marzo 2010, nell'ambito delle previsioni di cui all'art. 154, commi 4 e 5, del Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";

RITENUTO opportuno procedere all'adozione del Regolamento per l'utilizzo della posta elettronica e della rete internet nel Ministero dell'ambiente e della tutela del territorio e del mare, allegato al presente decreto quale sua parte integrante e sostanziale,

DECRETA

Articolo Unico

Per le motivazioni esposte in premessa, è adottato il Regolamento per l'utilizzo della posta elettronica e della rete internet nel Ministero dell'ambiente e della tutela del territorio e del mare, che si allega al presente decreto quale sua parte integrante e sostanziale.

Roma, 29 marzo 2010

Dott. Nicolino Storto

gdp

Ministero dell'Ambiente e della Tutela del Territorio e del Mare

DIREZIONE GENERALE DEGLI AFFARI GENERALI E DEL PERSONALE

REGOLAMENTO PER L'UTILIZZO DELLA POSTA ELETTRONICA E DELLA RETE INTERNET NELL'AMBITO DEL MINISTERO

IL DIRETTORE GENERALE

VISTA la Legge 20 maggio 1970, n. 300, recanti *"Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e nell'attività sindacale nei luoghi di lavoro e norme sul collocamento"* (Statuto dei lavoratori);

VISTO il decreto legislativo 30 giugno 2003, n. 196, recante "Codice in materia di protezione dei dati personali";

VISTO il Decreto del Presidente della Repubblica 3 agosto 2009 , n. 140, "Regolamento recante riorganizzazione del Ministero dell'ambiente e della tutela del territorio e del mare";

VISTO il decreto del Ministro dell'ambiente e della tutela del territorio e del mare in data 22 maggio 2007, n. 105, recante *"Regolamento per il trattamento dei dati sensibili e giudiziari, in attuazione degli articoli 20 e21 del decreto legislativo 30 giugno 2003, n. 196"*;

VISTE le linee guida del Garante per la protezione dei dati personali, emanate con delibera n. 13 dell'1 marzo 2007 (G.U. n. 58 del 10 marzo 2007), in tema di corretto utilizzo della posta elettronica e della rete Internet nel rapporto di lavoro e, in particolare, il punto 3.2. *"Linee guida"*, laddove è previsto che: *"In questo quadro, può risultare opportuno adottare un Regolamento interno redatto in modo chiaro e senza formule generiche, da pubblicizzare adeguatamente (verso i singoli lavoratori, nella rete interna, mediante affissioni sui luoghi di lavoro con modalità analoghe a quelle previste dall'art. 7 dello Statuto dei lavoratori,.....) e da sottoporre ad aggiornamento periodico"*;

RITENUTO, pertanto, opportuno adottare il Regolamento interno previsto dal punto 3.2. delle citate Linee guida;

ACQUISITO il parere dell'Ufficio Legislativo del Ministero dell'ambiente e della tutela del territorio e del mare;

PREMESSO che:

- la realtà lavorativa in questi ultimi anni si è andata connotando per la sempre più elevata diffusione delle tecnologie dell'informazione e della comunicazione, il che, se da un lato ha permesso di migliorare i livelli di efficienza, economicità ed efficacia dell'azione amministrativa, impone tuttavia l'esigenza di regolamentare le modalità di utilizzo di dette innovative tecnologie nell'organizzazione dell'attività lavorativa, con particolare attenzione all'utilizzo della posta elettronica e della rete Internet e alle connesse implicazioni in materia di trattamento dei dati personali, nonché in materia di controlli da parte del Datore di Lavoro circa il corretto utilizzo da parte dei lavoratori degli strumenti in parola, conformemente alle previsioni del decreto legislativo 30 giugno 2003, n. 196 (Codice della privacy), della Legge 20 maggio 1970, n. 300 (Statuto dei lavoratori) e alle linee guida del Garante per la protezione dei dati personali, emanate con delibera n. 13 del 1° marzo 2007 (G.U. n. 58 del 10 marzo 2007), in tema di utilizzo della posta elettronica e della rete Internet.

- Secondo le indicazioni fornite nell'ambito della "Premessa"delle citate Linee Guida del Garante per la protezione dei dati personali

  "a) compete ai datori di lavoro assicurare la funzionalità e 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;
  b) spetta ad essi 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 (artt. 15, 31 ss., 167 e 169 del Codice);
  c) emerge l'esigenza di tutelare i lavoratori interessati anche perché l'utilizzazione dei predetti mezzi, già ampiamente diffusi nel contesto lavorativo, è destinata ad un rapido incremento in numerose attività svolte anche fuori della sede lavorativa;
  d) l'utilizzo di Internet da parte dei lavoratori può, infatti, formare oggetto di analisi, profilazione e integrale ricostruzione mediante elaborazione di log file della navigazione web ottenuti, ad esempio, da un proxy server o da un altro strumento di registrazione delle informazioni. I servizi di posta elettronica sono parimenti suscettibili (anche attraverso la tenuta di log file di traffico e-mail e l'archiviazione di messaggi) di controlli che possono giungere alla conoscenza da parte del datore di lavoro (titolare del trattamento) del contenuto della corrispondenza;
  e) le informazioni così trattate contengono dati personali anche sensibili riguardanti lavoratori o terzi, identificati o identificabili.";

e, inoltre, con riguardo specifico alla "Tutela del lavoratore":

"Le informazioni di carattere personale trattate possono riguardare, oltre all'attività lavorativa, la sfera personale e la vita privata di lavoratori e di terzi. La linea di confine tra questi ambiti, come affermato dalla Corte europea dei diritti dell'uomo, può essere tracciata a volte solo con difficoltà.
Il luogo di lavoro è una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali (artt. 2 e 41,

secondo comma, Cost.; art. 2087 cod. civ.; cfr. altresì l'art. 2, comma 5, Codice dell'amministrazione digitale (d.lgs. 7 marzo 2005, n. 82), riguardo al diritto ad ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato)";

- scopo del presente Regolamento interno, quindi, è quello di organizzare il funzionamento e il corretto impiego degli strumenti elettronici e, in particolare, della posta elettronica e della navigazione in *Internet* da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo conto, in particolare: dei diritti dei lavoratori e della disciplina in tema di relazioni sindacali; della normativa in materia di protezione dei dati personali; delle esigenze di tutela della sicurezza, della disponibilità e dell'integrità dei sistemi informativi e dei dati, anche al fine di prevenire eventuali usi indebiti degli strumenti elettronici in parola;

- ulteriori finalità del presente Regolamento sono, da un lato, informare i lavoratori sulle finalità dei possibili controlli posti in essere dall'amministrazione a tutela della sicurezza della rete informatica e per prevenire usi impropri degli strumenti elettronici da parte del personale e, dall'altro, di sensibilizzare il medesimo personale su ulteriori aspetti, non meno rilevanti, relativi alla gestione dei sistemi informatici, quali il rispetto della normativa sulla tutela legale del software, e quella sulla tutela del *know-how* ministeriale, quando queste importanti informazioni di proprietà dell'amministrazione sono custodite nel sistema informatico.

SENTITE le OO.SS. di cui all'articolo 8, commi 1 e 2, del CCNL 1999 relativamente allo schema del presente Regolamento, espressamente interessate con nota prot. n. 17565/PR4 in data 13 novembre 2009;

ACQUISITO il parere sullo schema del presente Regolamento interno da parte del Garante per la protezione dei dati personali, ai sensi dell'art. 154, comma 5, del Decreto Legislativo 30 giugno 2003, n. 196, recante "Codice in materia di protezione dei dati personali";

Per quanto sopra premesso e considerato,

ADOTTA IL PRESENTE REGOLAMENTO INTERNO

Articolo 1
(Campo di applicazione)

1.1. Il presente Regolamento si applica a tutti i lavoratori dipendenti del Ministero dell'ambiente e della tutela del territorio e del mare, nonché a tutto il personale che a qualsiasi titolo – quindi a prescindere dal tipo di rapporto di lavoro e/o utilizzazione con lo stesso intercorrente - presti la propria attività lavorativa, anche saltuaria e/o consulenziale, presso le sedi dello stesso Ministero, di seguito, per brevità, denominato "Ministero", e che, per ragioni connesse all'espletamento del proprio lavoro, risulti comunque autorizzato e abilitato all'uso, anche solo occasionale e/o temporaneo, delle risorse informatiche dell'Amministrazione.

1.2. Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche, per "Utente" deve intendersi ogni dipendente e lavoratore, così come indicato al precedente comma 1, in possesso di specifiche credenziali di autenticazione e/o autorizzazione e che possa essere assegnatario di uno specifico indirizzo di posta elettronica e di cui al successivo articolo 3, comma 2.

Articolo 2
(Attività di conduzione sistemi)

2.1. Il Ministero rende noto, con l'approvazione e la diffusione del presente Regolamento a tutto il personale interessato, che il personale autorizzato e nominato quale Amministratore di sistema ai sensi del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", come modificato dal provvedimento del 25 giugno 2009, incaricato dal Ministero e/o appartenente alle Società appaltatrici per i servizi di conduzione dei sistemi informatici del Ministero (gestione postazioni di lavoro; *LAN Management; System Management;* ecc) e/o per i servizi di connettività e sicurezza nell'ambito del sistema pubblico di connettività, sono autorizzati a compiere interventi sul sistema informatico del Ministero medesimo diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione *hardware* etc.).

Nel rispetto dei principi di "non eccedenza" e di "pertinenza" (art. 11 del decreto legislativo 30 giugno 2003, n. 196) i controlli sull'uso di strumenti elettronici saranno prioritariamente di tipo aggregato, riferiti all'intera struttura lavorativa del Ministero o a sue aree, quindi di tipo anonimo, e si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti elettronici e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base individuale sono giustificati solo qualora le anomalie, nonostante le contromisure adottate in via generale dall'amministrazione per la eliminazione delle relative cause, risultino tuttavia persistenti, costituendo un pericolo per la sicurezza del sistema e/o per il regolare funzionamento delle attività di ufficio e/o, ancora, qualora l'utilizzo anomalo degli strumenti elettronici rilevato in sede di controllo possa integrare eventuali fattispecie di responsabilità sotto il profilo disciplinare, amministrativo-contabile, civile.

2.2. Il personale di cui al precedente comma 2.1 ha la facoltà di collegarsi e visualizzare da remoto il *desktop* delle singole postazioni dei *personal computer* al fine di garantire l'assistenza tecnica e la normale attività operativa, nonché la massima sicurezza contro virus, *spyware, malware,* etc. previa comunicazione e contestuale accettazione dell'intervento da parte dell'utente interessato. Di tali connessioni vengono conservati i log di accesso.

E' in ogni caso fatto divieto di effettuare controlli prolungati, costanti o indiscriminati sull'uso, da parte dei lavoratori, degli strumenti elettronici del Ministero.

Articolo 3
(Utilizzo del Personal Computer)

3.1. Il *personal computer* affidato all'Utente è uno strumento di lavoro e, in quanto tale, deve essere utilizzato con cura ed esclusivamente per finalità connesse allo svolgimento dell'attività lavorativa.

3.2. Il *personal computer* dato in affidamento all'Utente permette l'accesso alla rete informatica del Ministero solo attraverso specifiche credenziali di autenticazione, come meglio descritto al successivo articolo 4.

3.3 E' assolutamente vietato e non consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale di cui al precedente comma 2.1. ed a ciò autorizzato. E' altresì assolutamente vietato e non consentito agli utenti di 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. L'inosservanza della presente disposizione espone il Ministero a gravi responsabilità civili. Si evidenzia, inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul *software* che impone la presenza

nel sistema di *software* regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, possono integrare fattispecie di reato o di illecito amministrativo.

3.4. Non è consentito all'Utente modificare autonomamente le caratteristiche impostate sul proprio personal computer.

3.5. Ogni Utente deve prestare la massima attenzione in caso di eventuale utilizzo di supporti di origine esterna, avvertendo immediatamente il personale di cui al precedente articolo 2, comma 1, nel caso in cui siano rilevati *virus* ed adottando quanto previsto dal successivo articolo 10 del presente Regolamento relativo alle procedure di protezione *antivirus*.

3.6 L'Utente, anche in caso di allontanamento temporaneo dalla propria postazione di lavoro, dovrà seguire la procedura di "blocco" del personal computer, fermo restando che, al termine della giornata lavorativa, lo stesso personal computer dovrà essere sempre spento, unitamente alle altre apparecchiature informatiche collegate. I dati relativi all'accesso alla postazione informatica vengono automaticamente registrati e cancellati in forma automatizzata per un periodo pari a sei mesi. Tali dati possono essere trattati in via eccezionale e tassativamente solo ove ricorrano una o più delle seguenti ipotesi:

- necessità di aderire ad eventuali specifiche richieste di informazioni dell'Autorità Giudiziaria;
- su motivata richiesta dell'Utente assegnatario della postazione di lavoro e titolare delle credenziali di autenticazione per l'accesso alla rete informatica del Ministero;
- necessità dell'Amministrazione connesse a particolari esigenze di sicurezza.

L'eventuale ulteriore prolungamento dei tempi di conservazione dei dati riveste carattere eccezionale ed è consentito esclusivamente per il tempo strettamente necessario a realizzare le predette tassative esigenze e limitatamente alle sole informazioni indispensabili a tali fini.

Articolo 4
(Gestione ed assegnazione delle credenziali di autenticazione)

4.1. Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dalla Struttura competente per la gestione dei Sistemi Informativi del Ministero esclusivamente previa formale richiesta del Dirigente Generale o Responsabile dell'Ufficio/Direzione al quale sarà assegnato e presso cui andrà ad operare il nuovo Utente.

4.2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'Utente (*user id*), associato ad una parola chiave (*password*) riservata che dovrà venire custodita dall'Utente con la massima diligenza e non divulgata. Non è consentita l'attivazione della *password* di accensione (*bios*), senza preventiva autorizzazione da parte della Struttura competente per la gestione dei Sistemi Informativi del Ministero.

4.3. La parola chiave, formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti riconducibili all'incaricato.

4.4. È necessario procedere alla modifica della parola chiave a cura dell'Utente, incaricato del trattamento, al primo utilizzo e, successivamente, almeno ogni tre mesi.

4.5. La parola chiave scadrà automaticamente e potrà essere riattivata dall'Utente solo per il tramite del personale autorizzato della Struttura competente per la gestione dei Sistemi Informativi del Ministero.

4.6. L'utente, in caso di improvvisa o prolungata assenza o impedimento, può delegare un altro utente (c.d. fiduciario) all'accesso ai dati registrati negli strumenti elettronici in uso all'utente medesimo, se ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Dell'avvenuto conferimento della delega l'utente delegante deve informare tempestivamente il Dirigente /Responsabile dell'ufficio di relativa appartenenza.

Di ciascun accesso dovrà essere redatto apposito verbale e informato l'utente delegante alla prima occasione utile.

4.7. Anche in relazione alla necessità di contenerne e limitarne l'assegnazione al personale specificatamente autorizzato e di evitare l'uso improprio della rete informatica ministeriale, è fatto espresso e prioritario obbligo a ciascun Dirigente o Responsabile della Direzione/Ufficio di segnalare immediatamente al Dirigente responsabile della gestione dei sistemi informativi del Ministero la necessità di disattivazione delle credenziali di accesso alla rete e alla posta elettronica dell'indirizzo di posta elettronica in precedenza attribuite ad Utenti su richiesta del medesimo Dirigente/Responsabile qualora le motivazioni poste a base della stessa richiesta venissero meno (esempio cessazione del rapporto di consulenza e/o da organi collegiali, gruppi di lavoro, commissioni, segreterie tecniche comunque denominati). Tale adempimento potrà essere delegato dal Dirigente Generale o dal Responsabile dell'Ufficio a dirigenti assegnati alla propria Direzione/Ufficio.

4.8. La disattivazione delle credenziali di accesso alla rete e alla posta elettronica avverrà comunque da parte dell'Ufficio del Responsabile della gestione dei sistemi informativi qualora lo stesso non venga utilizzato per un periodo di novanta giorni consecutivi. Da tale disattivazione sono esclusi i dipendenti di ruolo e comandati.

Articolo 5
(Utilizzo della rete)

5.1. Per l'accesso alla rete del Ministero ciascun Utente deve essere in possesso della specifica credenziale di autenticazione.

5.2. È assolutamente vietato entrare nella rete e nei programmi con un codice d'identificazione Utente diverso da quello assegnato. La parola-chiave d'ingresso alla rete ed ai programmi è segreta. Si evidenzia che l'eventuale inosservanza di tale divieto, ricorrendone i presupposti di legge, può costituire reato, ai sensi dell'art. 615-ter del codice penale.

5.3. Le cartelle utenti presenti nei *server* del Ministero sono aree di condivisione di informazioni esclusivamente di servizio e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque *file* che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione e *back up* da parte del personale della Struttura competente per la gestione dei Sistemi Informativi del Ministero.

5.4. Tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno PC) non sono soggetti a salvataggio da parte del personale della Struttura competente per la gestione dei Sistemi Informativi del Ministero. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo Utente. L'Amministrazione provvederà a mettere a disposizione dell'Utente, previa richiesta, opportune aree del *file server* dedicate al salvataggio dei dati o supporti magnetici ove il *personal computer* sia dotato di unità di masterizzazione.

5.5. Il personale operante nell'ambito della Struttura competente per la gestione dei Sistemi Informativi del Ministero può in qualunque momento procedere alla rimozione di ogni *file* o applicazione che riterrà essere pericolosi per la Sicurezza sia sui *PC* degli utenti sia sulle unità di rete. Al di fuori dei casi di urgenza e di impellenti rischi per la sicurezza dei sistemi, il suddetto personale interviene previa comunicazione agli utenti interessati.

5.6. Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun Utente provveda alla pulizia degli archivi, con cancellazione dei *file* obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

Articolo 6
(Utilizzo e conservazione dei supporti rimovibili)

6.1. Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB come *pen drive,* etc.), contenenti dati personali nonché informazioni costituenti *know-how* dell'amministrazione, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

6.2. Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati personali, ciascun Utente dovrà contattare il personale della Struttura competente per la gestione dei Sistemi Informativi del Ministero e seguire le istruzioni da questo impartite.

6.3. In ogni caso, i supporti magnetici contenenti dati personali devono essere dagli utenti adeguatamente custoditi in armadi chiusi o, comunque, in luoghi non accessibili a terzi.

6.4. L'Utente è responsabile della custodia dei supporti e dei dati in essi contenuti.

Articolo 7
(Utilizzo di personal computer portatili)

7.1. L'Utente è responsabile del *personal computer* portatile assegnatogli e deve custodirlo con diligenza, sia durante gli spostamenti, sia durante l'utilizzo nel luogo di lavoro.

7.2. Ai *personal computer* portatili si applicano le regole di utilizzo previste dal presente Regolamento. con particolare attenzione alla rimozione di eventuali *file* elaborati prima della riconsegna. La cancellazione di tutti dati c *file* contenuti nel *personal computer* riconsegnato al Ministero dal soggetto affidatario resta ad esclusivo carico del medesimo affidatario. Ogni eventuale responsabilità per violazione della normativa vigente in materia di tutela della *privacy,* derivante dall'omessa cancellazione dei dati contenuti nel *personal computer* restituito dall'Utente affidatario, resta a carico di quest'ultimo, fermi restando gli obblighi ricadenti in capo all'Amministrazione, ai sensi dal Provvedimento del Garante per la protezione dei dati personali del 13 ottobre 2008, in materia di "Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali", per i casi di reimpiego, riciclo o smaltimento dei rifiuti elettrici ed elettronici.

7.3. I *personal computer* portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con la massima diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

7.4. La eventuale sottrazione o smarrimento del *personal computer* dovuti al mancato rispetto di adeguati criteri di custodia, sia all'interno che all'esterno della sede ministeriale, determineranno la necessità per l'Utente di rimborsare all'Erario il valore di mercato dell'apparecchiatura. Conseguentemente, la denuncia di smarrimento o sottrazione dovrà contenere anche l'espresso riferimento ai criteri di custodia posti in essere.

Articolo 8
(Uso della posta elettronica)

8.1. La casella di posta elettronica assegnata all'Utente è uno strumento di lavoro e, pertanto, è esclusivamente utilizzabile per finalità di servizio.

8.2. E' fatto divieto di utilizzare le caselle di posta elettronica cognome.nome@ministeroambiente.it nei seguenti casi :

- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es.mp3) non legati all'attività lavorativa;
- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a titolo personale a dibattiti, aste on line, concorsi, forum o mailing-list, etc.;
- la partecipazione a catene telematiche (dette anche "di Sant'Antonio"), ad appelli e/o petizioni (anche se possono sembrare veritieri e/o socialmente utili), a giochi e a qualsivoglia altra attività non riconducibile allo svolgimento dell'attività lavorativa. Se si

dovessero peraltro ricevere messaggi di tale tipo, si dovrà comunicarlo immediatamente al personale della Struttura competente per la gestione dei Sistemi informativi del Ministero. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi;

- utilizzare tecniche di "mail spamming" cioè di invio massiccio di comunicazioni a liste di distribuzione extra Ministero o di azioni equivalenti;
- allegare al testo delle comunicazioni materiale potenzialmente insicuro (ad es. programmi, scripts, macro), così come file di dimensioni eccessive
- in ogni altro caso in cui l'utilizzo della casella di posta di servizio risulti palesemente incoerente con la prestazione lavorativa e/o potenzialmente rischiosa per la sicurezza della rete informatica.

8.3. L'invio di *e-mail* a tutti gli indirizzi di posta elettronica è fattispecie di carattere eccezionale e rientrante nella esclusiva titolarità e disponibilità degli Uffici del Ministero. Tale generalizzato invio è eccezionalmente consentito ad un singolo Utente, previa formale, motivata e preventiva richiesta al Dirigente Responsabile dell'Ufficio/Direzione presso cui l'Utente medesimo presta la propria attività, con conseguente necessaria autorizzazione. La richiesta e l'autorizzazione dovranno essere successivamente trasmesse al Responsabile dell'Ufficio per la gestione dei sistemi informativi. In mancanza della predetta autorizzazione è vietato l'invio di *e-mail* a tutte le cassette di posta e/o a massicci gruppi di utenti.

8.4. La casella di posta elettronica, in quanto strumentale allo svolgimento ordinario dell'attività lavorativa, deve essere consultata quotidianamente dall'Utente, che deve nel contempo provvedere a mantenerla in ordine, cancellando documenti inutili e, soprattutto, allegati ingombranti.

8.5. È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario.

8.6. È obbligatorio porre la massima attenzione nell'aprire i *file attachment* di posta elettronica prima del loro utilizzo (non eseguire *download* di *file* eseguibili o documenti da siti *Web* o *Ftp* non conosciuti).

8.7. Al fine di garantire la funzionalità del servizio di posta elettronica e di ridurre al minimo l'accesso ai dati trattati dall'Utente, nel rispetto del principio di necessità e di proporzionalità (artt. 3, 11, e 22, del decreto legislativo 30 giugno 2003, n. 196), il sistema, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) potrà inviare automaticamente messaggi di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto della Struttura. In tal caso, la funzionalità deve essere attivata dall'Utente.

8.8. In caso di assenza non programmata (ad es. per malattia) la procedura di cui al precedente comma 8.7 - qualora non possa essere attivata dal lavoratore avvalendosi del servizio *webmail* entro due giorni – potrà essere attivata a cura del Ministero, su espressa richiesta dell'interessato o del Dirigente/Responsabile della Struttura di assegnazione, previa comunicazione all'utente interessato medesimo, per garantire il regolare andamento delle attività dell'Ufficio.

8.9. Come previsto dalla Linee Guida del Garante richiamate in premessa, l'utente, in caso di improvvisa o prolungata assenza e impedimento, può delegare un altro utente (c.d. fiduciario) a verificare il contenuto dei messaggi di posta elettronica e a inoltrare al Dirigente / Responsabile dell'Ufficio di appartenenza quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività dovrà essere redatto apposito verbale e informato l'utente interessato alla prima occasione utile.

I dati a cui il fiduciario accede dovranno essere trattati con estrema delicatezza, in particolare per quelli riferibili a terzi identificati o identificabili.

8.10. E' fatto comunque divieto di utilizzare la posta elettronica come luogo per scambio di opinioni da parte degli Utenti anche per materie afferenti la gestione ministeriale.

8.11. Il contenuto di comunicati, specialmente se inoltrati a tutte le cassette da parte delle Organizzazioni Sindacali a cui è stato attribuito, su specifica richiesta, un indirizzo di posta elettronica interno, deve essere sempre improntato al doveroso rispetto sia dell'Amministrazione pubblica in generale che del Ministero in particolare evitando apodittiche affermazioni che possano ledere l'onorabilità personale sia dei suoi Rappresentanti che di terzi. Anche in tale ambito dovranno evitarsi comportamenti che ripetuti nel corso di brevi periodi trasformino impropriamente il sistema di comunicazione informatica del Ministero, quale strumento di lavoro ministeriale, in un Forum di dibattito.
Al fine di evitare, altresì, l'anomalo appesantimento della gestione e conduzione del sistema di comunicazione informatica, i comunicati inoltrati a tutti gli indirizzi di posta elettronica dalle Organizzazioni Sindacali dovranno riguardare in via esclusiva questioni di interesse sindacale e del lavoro.
8.12. L'invio dei comunicati da parte delle Organizzazioni Sindacali dovrà avvenire in via esclusiva mediante l'utilizzazione dell'indirizzo di posta attribuito alla Sigla e non attraverso quella attribuita, quale dipendente ministeriale, al dirigente e/o rappresentante sindacale utilizzabile in via esclusiva per motivi di servizio.

Articolo 9
(Navigazione in Internet)

9.1. La navigazione in *Internet* costituisce uno strumento di lavoro e, pertanto, è utilizzabile esclusivamente per finalità di servizio, fatti salvi i casi in cui risulti consentito, ai sensi del presente articolo, l'uso di internet per l'assolvimento di incombenze amministrative o burocratiche del dipendente.
9.2. In questo senso, a titolo non esaustivo, l'Utente non potrà utilizzare Internet per:

- l'*upload* o il *download* di *software* gratuiti (*freeware*) e *shareware*, nonché l'utilizzo di documenti provenienti da siti *web* o *http*, se non strettamente attinenti all'attività lavorativa e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il personale operante presso la Struttura competente per la gestione dei Sistemi Informativi del Ministero);
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in *guest books* (libro degli ospiti), anche utilizzando pseudonimi (o *nicknames*) se non espressamente autorizzati;
- porre in essere attività in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
- utilizzare sistemi *Peer to Peer* (P2P), di *file sharing* (condivisione di *file* all'interno di una rete comune), *podcasting* (sistema che permette di scaricare in modo automatico documenti, generalmente audio o video) o similari, così come connettersi a siti che trasmettono programmi in *streaming* (come radio o TV via *WEB*), fatti salvi casi eccezionali in cui, per specifiche e motivate ragioni istituzionali e di servizio, detta autorizzazione venga formalmente richiesta al Dirigente Responsabile dell'Ufficio/Direzione presso cui il dipendente interessato presta servizio e la stessa venga appositamente rilasciata dalla Struttura competente per la gestione dei Sistemi Informativi del Ministero, previa opportuna verifica della compatibilità dell'attività richiesta con le complessive esigenze di sicurezza e di funzionamento della rete informatica del Ministero.

E' altresì vietato:

- utilizzare *internet provider* diversi da quello ufficiale del Ministero e la connessione delle postazioni di lavoro alle reti di tali provider con sistemi di connessione diversi (es. modem) da quello centralizzato, fatti salvi casi eccezionali in cui, per specifiche e motivate ragioni istituzionali e di servizio, apposita autorizzazione venga formalmente richiesta al Dirigente

Responsabile dell'Ufficio/Direzione interessato e la stessa venga appositamente rilasciata dalla Struttura competente per la gestione dei Sistemi Informativi del Ministero, previa opportuna verifica della compatibilità dell'attività richiesta con le complessive esigenze di sicurezza e di funzionamento della rete informatica del Ministero.

E' consentito all'utente l'uso di internet per l'assolvimento di incombenze amministrative o burocratiche, per il tempo strettamente necessario allo svolgimento delle relative operazioni, quali:

- adempimenti *on line* nei confronti di pubbliche amministrazioni o concessionari di pubblici servizi;
- rapporti con istituti bancari o assicurativi.

9.3. Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, il Ministero adotta uno specifico sistema di *web filtering* che consente di impostare *policy* in base ai tipi di *file*, ai protocolli, agli utenti e ai gruppi.

9.4. Le attività sull'uso del servizio di accesso ad *Internet* vengono automaticamente registrate e cancellati in forma elettronica attraverso i *Log* di sistema, che vengono conservati per un periodo pari a tre mesi.

9.5. Il trattamento dei dati contenuti nei *file* di *Log* può avvenire esclusivamente in forma aggregata o anonima in modo tale da precludere l'immediata identificazione degli utenti e/o delle loro attività.

9.6. I dati personali contenuti nei *Log* possono essere trattati in via eccezionale e tassativamente solo ove ricorrano una o più delle seguenti ipotesi:

- per corrispondere ad eventuali specifiche richieste di informazioni da parte dell'Autorità giudiziaria;
- quando si verifichi un evento dannoso o una situazione di pericolo che richiedano un immediato e necessario intervento;
- solo qualora l'utilizzo anomalo degli strumenti elettronici, nonostante le contromisure (in particolare: utilizzo di sistemi di web filtering; avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti di ufficio e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite) adottate dall'Amministrazione in via anonima o aggregata per l'eliminazione delle relative cause, risulti tuttavia persistente, costituendo perciò stesso un pericolo per la sicurezza del sistema e/o per il regolare funzionamento delle attività di ufficio e/o, ancora, qualora lo stesso utilizzo anomalo degli strumenti elettronici possa integrare fattispecie di responsabilità sotto il profilo disciplinare; amministrativo-contabile; civile e/o penale.

L'eventuale ulteriore prolungamento dei tempi di conservazione dei dati riveste carattere eccezionale ed è consentito esclusivamente per il tempo strettamente necessario a realizzare le predette tassative esigenze e limitatamente alle sole informazioni indispensabili a tali fini.

Articolo 10
(Protezione antivirus)

10.1. Il sistema informatico del Ministero è protetto da *software antivirus* aggiornato quotidianamente. Ogni Utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico ministeriale mediante *virus* o mediante ogni altro *software* aggressivo.

10.2. Nel caso il *software antivirus* rilevi la presenza di un *virus*, l'Utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare immediatamente l'accaduto al personale della Struttura competente per la gestione dei Sistemi Informativi del Ministero.

10.3. Ogni dispositivo magnetico di provenienza esterna all'Amministrazione viene automaticamente verificato mediante il programma *antivirus* prima del suo utilizzo e, nel caso venga rilevato un *virus*, dovrà essere prontamente consegnato al personale della Struttura competente per la gestione dei Sistemi Informativi del Ministero.

Articolo 11
(Divieti)

11.1. E' in ogni caso vietato al Ministero effettuare trattamenti di dati personali mediante sistemi *hardware* e *software* che mirano al controllo a distanza di lavoratori, svolti in particolare mediante:

a) la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio *e-mail*;
b) la riproduzione e l'eventuale memorizzazione sistematica delle pagine *web* visualizzate dal lavoratore;
c) la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
d) l'analisi occulta di computer portatili affidati in uso.

Articolo 12
(Interruzione e disattivazione d'ufficio dell'abilitazione all'accesso alla rete Internet)

12.1. Eventuali interruzioni del servizio di connessione alla rete Internet sono comunicate a tutti gli Utenti con avvisi interni da parte della competente Struttura per la gestione dei sistemi informativi.

12.2. L'abilitazione di un Utente all'utilizzo della rete Internet viene disattivata temporaneamente d'ufficio, previa notifica all'interessato, nei seguenti casi in cui risulti necessario accertare il ricorrere di eventuali ipotesi di responsabilità a carico dello stesso:

- se vi siano ragionevoli evidenze di uso non corretto del servizio da parte dell'Utente o, comunque, un uso diverso da quello di lavoro;
- se vi siano ragionevoli evidenze di modifiche e/o interventi tecnici non autorizzati sull'hardware e/o sul *software* impiegati dall'Utente per la connessione alla rete *Internet;*
- nel caso in cui vi siano ragionevoli evidenze che l'Utente abbia reso noti o disponibili a terzi, password, procedure di connessione, indirizzo I.P., ulteriori credenziali di accesso a servizi telematici di carattere istituzionale e di servizio e altre informazioni tecniche da considerarsi riservate;
- se vi siano ragionevoli evidenze di accesso dell'Utente a *directory*, a siti e/o *file* e/o servizi da chiunque resi disponibili, non rientranti fra quelli per lui autorizzati e, in ogni caso, qualora l'attività dell'Utente comporti danno, anche solo potenziale, al sito contattato;
- nel caso in cui l'Utente consenta l'accesso ad internet a terzi per il tramite del proprio *personal computer* e/o utilizzando le proprie credenziali di autenticazione;
- in ogni altro caso in cui sussistono ragionevoli evidenze di una violazione degli obblighi dell'Utente circa il regolare utilizzo degli strumenti elettronici di servizio.

L'abilitazione all'utilizzo della rete Internet viene in ogni caso disattivata d'ufficio se l'Utente non riveste più la qualità di dipendente, comandato o distaccato, o di collaboratore comunque autorizzato all'utilizzo della rete.

Articolo 13
(Sanzioni)

13.1. Il presente Regolamento riveste valenza e natura di Codice comportamentale e, quindi, è fatto obbligo a tutti gli Utenti di un suo puntuale rispetto. La violazione delle disposizioni di cui al presente Regolamento è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari, nelle forme e secondo le procedure previste dal vigente CCNL, nonché sotto il profilo civile, penale e/o amministrativo-contabile, laddove ne

ricorrano i presupposti di legge.

13.2. Con riferimento ai collaboratori e al personale comunque estraneo all'Amministrazione, qualora questi per l'espletamento dei rispettivi incarichi siano autorizzati a utilizzare gli strumenti elettronici considerati dal presente Regolamento, nell'ambito dei contratti e provvedimenti di conferimento dei relativi incarichi dovrà essere inserita un'espressa clausola che imponga l'obbligo in capo agli stessi lavoratori di rispettare il Regolamento in questione, con previsione del diritto del Ministero, nei casi di violazione accertata di particolare gravità, di risolvere il contratto stesso, con salvezza di ogni eventuale azione civile e/o penale a carico del contraente inadempiente, laddove ne ricorrano i presupposti di legge.

Articolo 14
(Entrata in vigore e pubblicità)

14.1. Il presente Regolamento, sottoscritto da parte del Dirigente Generale della Direzione Generale per i servizi interni, viene adeguatamente divulgato a tutto il personale a qualsiasi titolo in servizio presso il Ministero dell'ambiente e della tutela del territorio e del mare mediante affissione in luogo accessibile a tutti, analogamente a quanto previsto dall'art. 7 della legge 20 maggio 1970, n. 300 (Statuto dei Lavoratori), oltreché mediante diffusione elettronica a tutti gli indirizzi di posta elettronica in uso al personale medesimo e pubblicazione sul sito WEB del Ministero.

14.2. Il presente Regolamento entra in vigore il giorno lavorativo successivo alla data di diramazione a tutti gli indirizzi di posta elettronica e di contestuale affissione dello stesso nei luoghi aziendali previsti di cui al precedente comma 14.1. La data di avvenuta diramazione e affissione sarà debitamente attestata in calce al Regolamento ad opera della competente Direzione per i servizi interni del Ministero.

14.3. Fermo restando che la pubblicità del presente Regolamento è assolta tramite l'affissione di cui al precedente comma 14.1. e la diramazione a tutti gli indirizzi di posta elettronica, lo stesso Regolamento viene opportunamente portato a conoscenza degli Utenti sin dal momento della prima messa a disposizione dei medesimi degli strumenti elettronici forniti dal Ministero, così come delle Società appaltatrici di servizi informatici all'atto della sottoscrizione dei relativi contratti.

14.4. Il presente Regolamento è sottoposto ad aggiornamento biennale e comunque diramato almeno una volta all'anno mediante trasmissione a tutte le cassette interne di posta elettronica.

14.5 Le disposizioni del presente Regolamento restano applicabili, nelle more delle periodiche revisioni ed aggiornamenti, se ed in quanto compatibili con la vigente normativa in materia di trattamento dei dati personali.

Roma, 29 marzo 2010

IL DIRETTORE GENERALE
(Dott. Nicola Storto)