PROCEDURA PER L'USO DELLE RISORSE DEL SISTEMA INFORMATIVO

Agenzia del TPL di Brescia

02	05 Dic. 2018	Prima Emissione	Amministratore di Sistema	Titolare Trattamento dei Dati
Rev.	Data	Causale	Preparato da	Approvato da

Sommario

1 Premessa

La legislazione Europea prevede sanzioni per le organizzazioni che non definiscano e adottino regole di gestione del sistema informativo e policy di sicurezza e riservatezza per il trattamento dei dati personali. L'entrata in vigore del Regolamento (UE) 679-2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, introduce rilevanti obblighi a carico degli enti pubblici, sanzionati civilmente, imponendo di gestire i dati personali rispettando il diritto di libertà e riservatezza degli interessati, prescrivendo all'organizzazione un trattamento lecito e corretto nel rispetto delle finalità per la quale i dati sono stati acquisiti.
Il presente Regolamento si pone l'obiettivo di creare una "buona pratica" nella gestione delle risorse del sistema informativo improntata alla trasparenza e all'uniformità dei comportamenti. Esso intende, pertanto, garantire l'Agenzia del TPL di Brescia, che attraverso il regolamento intende definire delle regole di comportamento da parte degli utenti del sistema di gestione delle informazioni; ma anche i lavoratori che vengono, in tal modo, resi edotti della politica adottata in materia di utilizzo di risorse informatiche e di trattamento dei dati.

2 Gestione del Piano di Sicurezza

2.1 Distribuzione ai soggetti interessati

Il regolamento adottato dall'Agenzia del TPL di Brescia, ha lo scopo di disciplinare l'utilizzo delle risorse del sistema informativo dell'Agenzia.

Il regolamento si rivolge:

- ai dipendenti dell'ente;
- al personale non dipendente legato da un contratto di lavoro subordinato, di prestazione d'opera occasionale, da rapporti di collaborazione occasionali;

La presente Policy si rivolge anche a coloro prestano il proprio lavoro regolato da un contratto di servizio o di appalto presso la sede dell'Ente o in un luogo diverso collegandosi al sistema informativo dell'ente per il mezzo della tecnologia informatica.

Il presente manuale viene consegnato ai soggetti precedentemente identificati da parte dell'ufficio del personale dell'ente.
Eventuali variazioni del presente regolamento vengono rese disponibili nella cartella del server dell'ente.

2.2 Revisione del Piano di Sicurezza

L'emissione e la revisione del Regolamento di utilizzo delle Risorse del Sistema Informativo, è gestita dal Titolare che garantisce l'aggiornamento dello stesso in modo congruente con l'evoluzione dell'organizzazione dell'ente e delle tecnologie informatiche adottate.

3 Ruoli

I ruoli previsti nella gestione del sistema informativo dell'Ente e dal R-UE 679/2016 sono i seguenti:

Titolare: a cui competono le decisioni in ordine alle finalità, ai principi e alle modalità del trattamento dei dati;

Il **Responsabile del Sistema informativo** è incaricato Unitamente al DPO (data Protection Officer) ad:

- elaborare e stabilire le regole per un utilizzo ragionevolmente sicuro del sistema informativo dell'Ente, in attuazione delle direttive del titolare;
- rendere operative, mediante il personale del settore elaborazione dati e/o di personale incaricato interno/esterno, le regole di sicurezza sul sistema informativo dell'Ente;
- controllare i sistemi, con l'ausilio del personale del settore elaborazione dati e/o di personale incaricato, per individuare un eventuale uso scorretto, nel rispetto della privacy degli utenti;
- segnalare prontamente al Dirigente di riferimento, o al Titolare ogni eventuale attività non autorizzata sul sistema informativo.

I **Responsabili del Trattamento** dei dati sono tenuti a:

- informare i dipendenti sull'uso appropriato delle dotazioni informatiche messe a disposizione;
- informare il personale dipendente e/o assimilato sulle disposizioni in merito all'uso consentito delle risorse del sistema informativo dell'Ente;
- verificare che il personale loro assegnato si uniformi alle regole ed alle procedure descritte nel presente regolamento;
- verificare che i fornitori e/o il personale incaricato esterno si uniformino alle regole ed alle procedure descritte nel presente regolamento;
- adempiere a tutti gli obblighi inerenti la responsabilità in materia di trattamento di dati personali e sensibili;
- segnalare prontamente all'amministratore di sistema ogni eventuale attività non autorizzata sul sistema informativo.

L'amministratore del Sistema Informativo

Ha il compito di

- attuare le regole e le policy di sicurezza informatica dell'Ente.
- sovraintende al corretto funzionamento della rete informatica adottando policy e soluzioni tecnologiche condivise con il Responsabile dei Sistemi informativi.
- configura e gestisce gli apparati del sistema informativo dell'Ente
- assicurare la custodia delle credenziali per la gestione dei sistemi di autenticazione e di autorizzazione;
- predisporre e rendere funzionanti le copie di sicurezza (operazioni di backup e recovery) dei dati e delle applicazioni;

Gli **Utilizzatori del Sistema Informativo** sono responsabili per ciò che concerne:

- il rispetto delle regole per l'uso delle risorse del sistema informativo dell'Ente;
- ogni uso che venga fatto delle credenziali di autenticazione assegnate secondo le modalità indicate nel presente regolamento;
- la pronta segnalazione al competente Responsabile/Titolare di ogni eventuale attività non autorizzata sul sistema informativo di cui vengano a conoscenza.

4 Regole Generali

Gli utenti devono utilizzare le risorse del sistema informativo prestando attenzione a non compromettere il funzionamento e l'efficienza della rete informatica.
Devono inoltre prestare attenzione alle modalità con cui vengono utilizzate le banche dati di cui l'ente è titolare al fine di gestire in modo corretto, secondo principi di liceità e nel rispetto delle normative e regolamenti in tema di Trattamento dei Dati.
Gli strumenti assegnati dall'Agenzia ai dipendenti, nonché le risorse ed i servizi del sistema informativo (accesso ad internet e posta elettronica) devono essere utilizzati unicamente per scopi ***inerenti l'attività lavorativa***.
Il mancato rispetto o la violazione delle regole contenute nel presente Regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili.

5 Accesso alle risorse del Sistema informativo

Le autorizzazioni di accesso al sistema informativo sono assegnate in funzione del ruolo di ogni utente in relazione all'incarico e alle relative autorizzazioni al trattamento dei dati.
Le richieste di autorizzazione all'accesso al sistema informativo dell'Ente devono essere trasmesse dal Responsabile del Trattamento dei Dati al Responsabile dei Sistemi Informativi. Il personale autorizzato ad accedere al sistema informativo è soggetto al presente regolamento.
Il personale esterno incaricato dall'Ente (es. consulenti, stagisti, personale interinale) può accedere ai servizi del sistema informativo nei locali dell'ente previa accettazione del presente regolamento.
Le richieste di autorizzazione all'accesso devono essere trasmesse dal competente dirigente all'amministratore di sistema.
Tutti gli utenti devono prendere visione ed accettare i termini del presente regolamento tramite la sottoscrizione del "Modulo di presa visione ed accettazione del Regolamento".

5.1 Regole di autenticazione al sistema informativo dell'Agenzia del TPL di Brescia

Ciascun dipendente/utente è identificato con un username personale di identificazione a cui è associata una password per l'accesso.
La username e la password personale sono gli strumenti fondamentali per garantire la sicurezza di accesso alle banche dati e alle risorse del sistema informativo dell'ente, nonché dell'indirizzo di posta elettronica dell'Ente assegnato al singolo dipendente.
Sulla base delle regole di gestione dei codici di autenticazione, ogni utente è tenuto a determinare:

- la propria password personale di accesso alla rete dell'Ente,
- i codici di accesso agli applicativi software dell'ente,
- la password di accesso alla casella di posta elettronica

L'accesso e l'uso sia del personal computer dell'ente, che di ogni altro sistema informatico (applicativi software, posta elettronica inclusa) è consentito solo previa identificazione dell'utente stesso tramite username e successiva digitalizzazione della password personale di accesso alle risorse e ai servizi del sistema informatico.
L'Agenzia adotta vari livelli di autenticazione:

Password di rete
La Password è composta da almeno otto (8) caratteri alfanumerici, non deve contenere riferimenti agevolmente riconducibili alla persona (ad es. nomi dei familiari, date di nascita, ecc.) e va modificata al primo utilizzo e, successivamente, almeno ogni sei (6) mesi;

Password degli applicativi usati nei vari uffici
Valgono le stesse regole per la password di rete

Password di accesso alla posta elettronica
Valgono le stesse regole per la password di rete

Password di accesso alle banche dati esterne:
Valgono le stesse regole per la password di rete

La Password è un dato personale e non deve essere comunicata a terzi;
Rivelare la propria Password o altre credenziali individuali a terzi costituisce violazione sia dei diritti fondamentali degli interessati, ai quali si riferiscono i dati contenuti negli archivi, sia delle norme interne che impongono principi di corretta gestione delle informazioni, oltre ad esporre a rischio anche la riservatezza dei dati personali riferibili all'utente;
Si deve evitare di memorizzare le password di posta elettronica o di accesso a siti web attraverso le funzionalità messe a disposizione dalle applicazioni.
Qualora si sospetti che la propria password non sia più segreta e riservata è necessario contattare immediatamente l'Amministratore del Sistema e procedere a cambiare la password.
A parziale deroga di quanto previsto al punto precedente, per consentire il regolare svolgimento delle attività di lavoro, in caso di assenze pianificate (ferie, permessi e trasferte) di qualunque durata esse siano ogni dipendente/utente ha indicato il responsabile dell'Area designato per l'accesso agli strumenti informatici e banche dati dell'Agenzia, durante il periodo di assenza.

5.2 Accesso alle Banche Dati digitali

Ogni collaboratore è autorizzato ad accedere alle banche dati del sistema informativo dell'Ente rilevanti per la Sua funzione e le relative mansioni. L'autorizzazione all'accesso è perciò limitata in via esclusiva all'ambito, alla categoria di dati, alle modalità e al tempo stabilito dal relativo rapporto contrattuale e/o in eventuali comunicazioni successive;
Accessi ad aree del sistema informatico riservate ad altri Incaricati è vietata e le richieste di accesso dovranno essere preventivamente inviate, per iscritto, al Titolare, il quale è l'unico a poter autorizzare l'Amministratore delle password a consentire l'accesso ad altre aree;
E' vietato lasciare incustodito ed accessibile il computer durante una sessione di trattamento dei dati;
I dati devono essere conservati per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti e successivamente trattati;
Alla luce di ciò, in caso di allontanamento anche temporaneo dal posto di lavoro, l'incaricato dovrà verificare che non vi è possibilità da parte di terzi di accedere a dati personali per i quali era in corso un qualunque tipo di trattamento, sia esso cartaceo che automatizzato.

6 Comunicazione dei dati

La comunicazione di dati personali con altri enti pubblici è autorizzata nel caso questa sia definita ed autorizzata da normative nazionali o regionali o da regolamenti.
La trasmissione di dati a soggetti privati è autorizzata nel caso di un accordo di collaborazione in cui è previsto lo scambio di informazioni. In questo caso devono essere adottate delle procedure per verificare le regole di trattamento e le misure di sicurezza adottate dal fornitore.
I dati personali trattati potranno essere comunicati all'esterno delle sedi del Titolare solo con l'autorizzazione scritta dello stesso o del Responsabile, se designato.
La trasmissione di dati personali in Paesi non appartenenti all'Unione Europea, sono autorizzati solo se sussistono le condizioni previste dal Regolamento Europeo 679/2016 sul trattamento dei dati e successive aggiornamenti normativi o regolamenti che disciplinano la materia;
Nel caso di comunicazioni/trasmissioni all'estero di dati personali deve essere data evidenza attraverso l'informativa inerente il trattamento dei dati;

7 Utilizzo delle Risorse del Sistema Informativo

Ogni incaricato è responsabile del corretto utilizzo e della custodia dei mezzi informatici consegnati;
Le banche dati, le risorse e gli strumenti del sistema informativo devono essere utilizzate unicamente per scopi attinenti all'attività lavorativa.
Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
AL termine del rapporto di lavoro le attrezzature informatiche devono essere riconsegnate in buono stato con memorizzati i dati raccolti, prodotti ed elaborati durante l'attività lavorativa.

7.1 Utilizzo del Computer

Il Personal Computer affidato al dipendente è uno strumento di lavoro che deve essere usato in modo corretto. L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte dell'Amministratore del Sistema.
Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione esplicita dell'Amministratore del Sistema, perché sussiste il grave pericolo di portare Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.
Non è consentito l'uso di programmi diversi da quelli installati sul computer nel momento in cui lo stesso viene consegnato all'utente (D.lg. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore).
Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo previa autorizzazione esplicita dell'Amministratore del Sistema.
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.
Si devono mettere in atto accorgimenti tali per cui il computer non resti incustodito, durante una sessione di trattamento: può essere sufficiente che un collega rimanga nella stanza, durante l'assenza di chi sta lavorando con lo strumento elettronico, anche se la stanza rimane aperta e accessibile; può essere sufficiente attivare lo screen saver con password oppure chiudere a chiave la stanza, dove è situato lo strumento elettronico, durante l'assenza, anche se nella stessa non rimane nessuno.
Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, router, ecc.), se non con l'autorizzazione espressa del Responsabile dei Sistemi Informativi.
Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
Non è consentita la memorizzazione di documenti informatici di natura personale (fotografie, file di varia natura) sugli strumenti di elaborazione o di memorizzazione dell'Ente.

7.2 Utilizzo di Computer Portatili

L'assegnatario di un computer portatile deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
Ai PC portatili si applicano le regole di utilizzo previste per i Pc connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
Nel caso di spostamenti al di fuori della sede di lavoro non deve essere lasciato nel mezzo di trasporto o in luoghi non presidiati.

I PC portatili utilizzati all'esterno (convegni, seminari ecc), in caso di allontanamento, devono essere custoditi in un luogo protetto.
Se si ha in dotazione un PC Portatile, si devono seguire le procedure di aggiornamento del software di protezione da virus, non si devono custodire dati di particolare rilevanza sul computer; nel caso di furto verrebbe inevitabilmente compromessa la riservatezza degli stessi.

7.3 Utilizzo dei Supporti Removibili (CD, dischi/dispositivi USB)

Prima di collegare un supporto di memoria esterno ad un PC o a un server è necessario fare controllare il supporto al software antivirus, questo in modo particolare anche nel caso di copia di file memorizzati sul supporto removibile.
Tutti i supporti riutilizzabili (pendrive, CD/DVD, dischi usb) contenenti dati del''Ente e dati personali devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione logica.
I supporti magnetici contenenti dati personali devono essere custoditi ed utilizzati in modo tale da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti.
Una volta cessate le ragioni per la conservazione dei dati, i supporti non possono venire abbandonati, ma si devono porre in essere gli opportuni accorgimenti finalizzati a rendere non leggibili e non ricostruibili tecnicamente i dati in essi contenuti, al fine di impedire che essi vengano carpiti da persone non autorizzate al trattamento. Si devono quindi cancellare i dati, se possibile, o arrivare addirittura a distruggere il supporto, se necessario.
I supporti informatici contenenti dati personali devono essere custoditi in archivi chiusi a chiave.
Non è consentito scaricare file contenuti in supporti rimovibili non aventi alcuna attinenza con la propria prestazione lavorativa.
Tutti i file di provenienza incerta od esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo da parte di software antivirus.
Ogni incaricato deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'Amministratore di Sistema nel caso in cui siano rilevati virus ed adottando quanto previsto dal presente Regolamento relativo alle procedure di protezione antivirus.
Nel caso di utilizzo P.C. portatili accessibili per mezzo di smart card o tessere magnetiche in possesso a proprio uso esclusivo, ogni incaricato dovrà conservare (es. non abbandonandole sulla scrivania) e proteggere (es. non avvicinarle a fonti di calore) tali dispositivi con la massima cura. Per tutelarsi in caso di furto, è altresì necessario, per l'accensione del relativo strumento elettronico, associare a tali dispositivi una password.

7.4 Configurazione della postazione di lavoro e degli apparati di rete

La configurazione base dell'hardware e l'installazione del software nelle postazioni di lavoro e negli apparati di rete è stabilita e predisposta dal personale del settore elaborazione dati o da personale interno/esterno incaricato.
L'utente è tenuto a non modificare la configurazione base della postazione di lavoro assegnata e degli apparati di rete messi a disposizione.
Alcuni software di utilità, individuati e resi disponibili dal settore elaborazione dati attraverso la rete dell'Agenzia, potranno essere installati autonomamente dall'utente. L'installazione dei rimanenti software, dotati o meno di licenza d'uso a titolo oneroso, potrà essere effettuata solo dal personale del settore elaborazione dati o da personale interno/esterno incaricato allo scopo.

7.5 Utilizzo di hardware di proprietà personale

L'utente può connettere postazioni di lavoro o apparati personali alle reti Intranet ed Extranet dell'ente, solo con l'autorizzazione scritta del titolare.
L'utente può utilizzare dispositivi non autorizzati dall'amministratore di sistema per accedere ai soli servizi del sistema informativo erogati via Internet.

L'autorizzazione rilasciata dall'amministrazione di sistema indicherà le principali caratteristiche tecniche atte ad individuare univocamente l'hardware di proprietà personale connesso alla rete, la durata dell'autorizzazione ed il titolare delle credenziali di accesso rilasciate.
L'hardware sarà connesso alla rete e configurato a cura del settore elaborazione dati o di personale interno/esterno incaricato dal settore elaborazione dati.

7.6 Policy antivirus

Malware è un nome generico che indica qualunque forma di programmi informatici maligni e indesiderati che si nascondono sotto forma di altri file.
Il *malware* minaccia in modo concreto e continuativo la sicurezza informatica e la loro eventuale diffusione nei sistemi informatici dell'Ente può avere conseguenze molto onerose in termini di perdita di dati, mancata produttività dei dipendenti, danni all'immagine e/o alla reputazione.
Per questo, la Funzione IT ha implementato diversi controlli di sicurezza informatica che includono il rilevamento di virus, filtri contro lo spam, sistemi firewall. Benché tali forme di protezione agiscano in modalità automatica, è comunque importante conoscere i malware e saperne riconoscere gli effetti, in modo da poter contribuire alla protezione contro di essi.
I *malware* possono presentarsi in diverse forme:

- *Virus*. Può essere un programma informatico creato appositamente per replicarsi copiandosi in altri programmi presenti nel computer. Gli allegati a messaggi e-mail con estensioni come *.BAT, *.COM, *.EXE, *.SCR e *.SHS, sono un sistema comunemente utilizzato per infettare i computer attraverso l'apertura del file allegato da parte dell'utente. I virus possono alterare e danneggiare i dati, provocare il malfunzionamento dei sistemi o renderli del tutto inutilizzabili
- *Trojan horse*. Sono dei falsi programmi — file che possono risultare interessanti all'utente ma contengono codici maligni in grado di generare conseguenze come la perdita, o addirittura il furto di dati. Perché possano diffondersi occorre che essi vengano copiati sul proprio computer, ad es. aprendo un allegato di posta o scaricando un file da Internet. Essi sono usati per l'invio di e-mail di spam per indurre le persone a fornire informazioni personali, fare in modo che dati proibiti (es. immagini illegali) vengano inconsapevolmente archiviati sui computer, per lanciare attacchi a siti web per renderli indisponibili
- *Worm*. Sono programmi che si replicano automaticamente da un computer ad un altro senza alcun trasferimento di file. Tale caratteristica li distingue dai virus, che invece si diffondono attraverso file infetti (solitamente documenti di Word o Excel)
- *Spyware*. È un programma informatico che raccoglie segretamente informazioni dal computer sul quale risiede per inoltrarle ad altri senza il proprio permesso o consentire ad altri di accedere al computer infetto; gli *Adware* provocano reindirizzamenti non voluti a siti Internet specifici causando la comparsa di "pop-up" promozionali non desiderati sullo schermo del proprio computer. Spesso vengono installati sul computer poiché l'utente ha acconsentito ad installarli visitando un sito web o accettando i termini d'uso nascosti all'interno di un lungo accordo per un altro programma.
- *Bot* sono usati come strumenti di attacco remoto per prendere il controllo del computer e creare una rete di computer infetti (*Botnet*)

L'Agenzia del TPL di Brescia è impegnata per garantire che i propri sistemi informativi siano privi di *malware*.

Tuttavia è necessario che tutti i dipendenti s'impegnino ad applicare alcune semplici regole, esplicitate nei seguenti paragrafi, per evitare che i *malware* possano attaccare la rete informatica dell'Agenzia e reagire adeguatamente nel caso in cui si sospetti l'infezione del proprio computer.

7.6.1 Regole per prevenire la diffusione di malware

L'Agenzia del TPL di Brescia assicura che tutti gli Strumenti Informatici utilizzino il software antivirus più aggiornato; in ogni caso ciascun Utente deve prevenire la diffusione di malware adottando le seguenti regole di base:

- non disattivare mai il software per la scansione dei virus
- verificare attentamente quali dati vengono salvati sul proprio computer e la loro provenienza
- non aprire file non richiesti (es. mail o messaggi istantanei da fonti sconosciute o sospette), anche se provenienti da colleghi, chiedendo eventualmente conferma al mittente dell'invio dei file non richiesti
- non copiare, scaricare o installare file da fonti sconosciute, sospette o inaffidabili o da supporti rimovibili o freeware o shareware da Internet senza il permesso della funzione IT
- disabilitare le macro e non aprire mai allegati aventi estensioni non riconducibili a quelle normalmente utilizzate per il proprio lavoro (ad esempio, .doc, .pdf, .txt, .xls,. ppt,)
- verificare i messaggi che compaiono più di una volta nella posta in arrivo o contenenti collegamenti a siti web sconosciuti.

7.6.2 La comunicazione di possibili infezioni da malware

Nel caso in cui il software antivirus abbia rilevato la presenza di un virus o altro *malware* sul proprio computer, si ravvisi un malfunzionamento (ad es. improvvisa lentezza nell'eseguire le operazioni) è necessario contattare immediatamente L'ufficio CED attenendosi alle istruzioni che verranno impartite.

7.7 Utilizzo dei mezzi di trasmissione e riproduzione dei documenti

Nell'utilizzo di fax, stampanti, fotocopiatrici/scanner è importante adottare cautele nella trasmissione e riproduzione dei documenti contenenti dati personali e/o informazioni riservate, al fine di prevenire eventuali rischi di accesso ai dati da parte di soggetti non autorizzati sia interni che esterni.

Per quanto concerne l'utilizzo delle stampanti, l'ente mette a disposizione stampanti di rete che possono essere utilizzate contemporaneamente da più persone. A tal fine ciascun utente deve:

- non lasciare incustoditi presso il fax, la stampante di rete, la fotocopiatrice o lo scanner documenti contenenti dati personali;
- accertarsi, in caso di uso della fotocopiatrice, che non rimangano originali o copie nella macchina. In caso di cattiva qualità della stampa distruggere il supporto cartaceo e non riutilizzarlo come carta da riciclo;
- nel caso di trasmissione via fax di documenti contenenti dati personali, accertarsi telefonicamente dell'avvenuta ricezione. Una volta inviati i documenti, ritirarli immediatamente dalla macchina.

7.8 Utilizzo degli strumenti di telefonia fissa e mobile

Nell'uso di apparecchi telefonici, fissi o mobili, è possibile, anche involontariamente, rivelare informazioni che possono contenere riferimenti a dati personali e/o informazioni riservate riferite a clienti o dipendenti.

Si sottolinea quindi la necessità di applicare le seguenti accortezze:

- l'uso del telefono fisso deve avvenire utilizzando un tono di voce tale da non mettere in condizione colleghi o altre persone che possono trovarsi nelle vicinanze di comprendere l'oggetto della telefonata;
- nel corso di conference call le porte delle sale o degli uffici utilizzati devono essere chiuse.
- l'uso del telefono cellulare in spazi esterni o interni dell'Agenzia per telefonate di lavoro va effettuato tenendo conto del fatto che altre persone possano sentire la comunicazione.
- L'uso dei dispositivi di telefonia mobile per fini privati deve essere fortemente limitato a casi di effettiva e comprovata necessità.

7.9 Clear desk policy

L'uso di spazi comuni adibiti a riunioni e/o postazioni di lavoro richiede che ciascun dipendente:

- presti particolare attenzione a fogli, schemi, appunti o qualsiasi altro documento dal quale sia possibile dedurre anche indirettamente informazioni a carattere personale o comunque riservato riferibili a individui;
- al termine della riunione l'eventuale materiale cartaceo prodotto deve essere rimosso o distrutto.

Tale livello di attenzione va esteso anche alle attrezzature presenti nella sala (ad es. lavagne o altri supporti cartacei) evitando accuratamente di lasciare informazioni che possano ricondurre a soggetti individuati.
Nel caso di utilizzo di sistemi di videoconferenza è opportuno che vengano rispettate le seguenti cautele:

- l'accesso agli spazi adibiti a videoconferenza deve essere autorizzato
- ogni eventuale registrazione video deve essere effettuata in modo da evitare che informazioni riservate siano distribuite, diffuse o comunicate a soggetti estranei o non autorizzati.

7.10 Uso della posta elettronica

La casella di posta, **assegnata all'utente**, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
Si rammenta che i sistemi di posta elettronica non consentono al momento di garantire la riservatezza delle informazioni trasmesse, si raccomandano gli utenti un utilizzo accorto del servizio.
E' fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list non attinenti la propria attività o funzione svolta per l'Agenzia, salvo diversa ed esplicita autorizzazione.
E' buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per l'Ente, ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere visionata od autorizzata dal Titolare.
Per la trasmissione di file all'interno dell'ente è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati, se di dimensioni consistenti si consiglia di utilizzare le directory di scambio presenti sui file server, notificando a mezzo mail al destinatario la disponibilità del file stesso.
E' consigliabile controllare con il software antivirus i file allegati di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).
I dettagli delle regole di backup e di conservazione degli archivi di posta elettronica sono esplicitati nel piano di sicurezza o nella procedura di backup dell'Agenzia.
E' vietato inviare catene telematiche (o di "Sant'Antonio"). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente all'Amministratore del Sistema. Non si deve in alcun caso attivare gli allegati di tali messaggi.
Nel caso si assenza di un dipendente il responsabile di Area potrà avere accesso alla casella di posta elettronica del dipendente per motivi legati alla gestione delle attività lavorative dell'ufficio, dandone comunicazione al dipendente.
Con riferimento ai trattamenti effettuati sulla posta elettronica aziendale dopo la cessazione del rapporto di lavoro, come già precisato dal Garante in precedenti occasioni, in conformità ai principi in materia di protezione dei dati personali, gli account riconducibili a persone identificate o identificabili devono essere rimossi previa disattivazione degli stessi e contestuale adozione di sistemi automatici volti ad informarne i terzi ed a fornire a questi ultimi indirizzi alternativi riferiti all'attività professionale del titolare del trattamento (indirizzo dell'Ufficio).

I contenuti delle caselle di posta personale dei dipendenti che si dimettono vengono conservate per 1 anno al termine del quali i contenuti della casella verranno cancellati.

7.11 Uso della rete Internet e dei relativi servizi

L'ente ha installato apparati per il monitoraggio degli accessi alla rete di internet unicamente per scopi di sicurezza.
Il PC abilitato alla navigazione in Internet costituisce uno strumento necessario allo svolgimento della propria attività lavorativa. E' proibita la navigazione in Internet per motivi diversi da quelli funzionali all'attività lavorativa stessa.
E' fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal Responsabile dei Sistemi Informativi.
E' tassativamente vietata effettuare ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dai dirigenti o attinenti i compiti e le mansioni assegnate e con il rispetto delle normali procedure di acquisto.
E' da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
E' vietata la partecipazione a Forum non professionali, l'utilizzo di chat (esclusi gli strumenti autorizzati), di bacheche elettroniche anche utilizzando pseudonimi, se non attinenti l'attività lavorativa svolta.
Il Servizio Sistemi Informativi si riserva di applicare per singoli e gruppi di utenti politiche di navigazione personalizzate in base alle mansioni ed eventuali disposizioni concordate con il titolare e con i Responsabili, al fine di ottimizzare l'uso delle risorse, gli investimenti e le prestazioni delle connessioni esistenti.
Non è consentita la navigazione in siti ove sia possibile rivelare le opinioni politiche, religiose o sindacali dell'utilizzatore; non è consentito inoltre visitare siti e memorizzare documenti informatici dai contenuti di natura oltraggiosa e/o discriminatoria per sesso/etnia/religione/opinione e/o appartenenza sindacale e/o politica.
Nella prospettiva della prevenzione di cui al presente documento l'ente si riserva la facoltà di adottare software o apparati hardware volti a bloccare l'accesso a determinati siti a contenuto estraneo all'attività dell'ente. Questo tipo di sistemi con modalità automatiche di filtro e inibizione non comporta un controllo diretto o indiretto sulla posizione individuale, ma semplicemente può impedire l'accesso a determinati siti non funzionali all'attività istituzionale dell'ente, può impedire il downloading di materiale, funge da filtro per il virus detecting, impedisce l'invio o la ricezione di mail contenenti determinate parole (a sfondo sessuale o razzista) o di determinate dimensioni.
L'Agenzia ha attivato dei sistemi di monitoraggio del traffico web che salvano gli indirizzi delle pagine a cui un determinato computer ha avuto accesso. I file con i dati di navigazione vengono conservati per sei mesi e poi cancellati. L'amministratore di sistema ha la facoltà di accedere e controllare i dati della navigazione in modo anonimo per motivi di sicurezza della rete informatica e delle banche dati gestite dell'ente.

7.12 Gestione delle banche dati e dei file di ufficio

Ad ogni dipendente dotato di una postazione di lavoro fornita dall'ente è normalmente riservato uno spazio sul disco locale ed eventualmente una cartella personale sul server ed una o più cartelle condivise sui dischi accessibili attraverso la rete telematica dell'Ente. L'utilizzo di tali risorse è strettamente riservato all'archiviazione ed alla condivisione dei file necessari alla normale attività lavorativa.
Nel caso in cui non sia previsto o attivo il salvataggio automatico dei dati trattati sul proprio personal computer, lo stesso deve essere effettuato manualmente almeno settimanalmente nelle cartelle appositamente create sul server dell'Agenzia.
Per lo scambio e la condivisione temporanea di file viene messa a disposizione un'area dei dischi di rete denominata "Scambio".

L'utente è tenuto alla periodica (almeno ogni sei mesi) pulizia di tutti gli spazi assegnati, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati al fine di evitare, salvo casi eccezionali, un'archiviazione superflua.
Il personale del settore elaborazione dati ha la facoltà di rimuovere i file degli utenti, senza preavviso, in caso di necessità di spazio sui dischi di rete, spostandoli su altri dispositivi di memorizzazione, o di rinominare i nomi delle cartelle o dei file in caso di malfunzionamenti.
I dati contenuti nelle cartelle condivise dei dischi di rete, ad eccezione dell'area di scambio, vengono salvati periodicamente con delle procedure di backup a cura del personale del settore elaborazione dati. E' fatto obbligo per gli utenti del sistema informativo dell'Ente salvare i dati importanti su server di rete.
I dettagli delle regole di backup e di conservazione dei dati sono esplicitati nel piano di sicurezza o nella procedura di backup dell'Ente.
Le richieste di recupero dei dati vanno inoltrate, non appena se ne manifesti la necessità, al personale del settore elaborazione dati, che si riserva di verificare la possibilità di recupero dei dati compatibilmente con le esigenze di servizio

7.13 Sito Internet

I dipendenti dell'Agenzia autorizzati possono pubblicare pagine informative e modulistica sul sito internet istituzionale, utilizzando gli strumenti di redazione messi a disposizione dal sistema informativo.
I responsabili di ufficio che provvedono autonomamente alla redazione delle pagine pubblicate sul sito internet, sono responsabili dei contenuti pubblicati.
Qualora la redazione dei contenuti sia affidata a società esterne o a consulenti, i responsabili di settore devono validare ad approvare i contenuti pubblicati.
Il personale del settore informatico fornisce l'assistenza necessaria a garantire il funzionamento degli ambienti di redazione e pubblicazione, ma non è tenuto a fornire assistenza sulle pagine realizzate dagli utenti.
Il responsabile del sistema informativo, avvalendosi di procedure automatiche o manuali, può provvedere all'aggiornamento degli ambienti di redazione ed alla rimozione dei contenuti dall'area pubblica, senza necessità di preavviso.
Le regole di pubblicazione di dati od informazioni nell'albo pretorio e definito da un regolamento interno.

8 Gestione dei documenti cartacei

Gli incaricati del trattamento devono prelevare dagli archivi/armadi i soli atti e documenti loro affidati, che devono controllare e custodire, durante l'intero ciclo necessario per lo svolgimento delle operazioni di trattamento, per poi restituirli all'archivio/armadi, al termine di tale ciclo.
Per gli atti ed i documenti contenenti **dati personali particolari (sensibili)** o dati giudiziari, il controllo e la custodia devono avvenire in modo tale che ai dati non accedano persone prive di autorizzazione.
In questo caso è quindi necessario che l'incaricato del trattamento utilizzi **cassetti con serratura, o di altri accorgimenti** aventi funzione equivalente, nei quali riporli prima di assentarsi dal posto di lavoro, anche se temporaneamente. In tali cassetti i documenti potranno essere riposti al termine della giornata di lavoro, qualora l'incaricato debba utilizzarli anche nei giorni successivi; al termine del trattamento l'incaricato dovrà invece restituirli all'archivio.
Per gli accessi agli archivi contenenti dati sensibili che avvengono dopo l'orario di chiusura, è obbligatorio identificare e registrare coloro che vi accedono.

9 Trattamenti di dati ed informazioni relative all'uso del sistema informativo

9.1 Prevenzione

Ai fini della prevenzione degli accessi non autorizzati e degli abusi nell'utilizzo dei servizi offerti dal sistema informativo dell'Ente, saranno prese tutte le misure tecniche ed organizzative ritenute idonee, incluso l'utilizzo di strumenti automatici quali la registrazione degli accessi, gli strumenti di verifica del software e dell'hardware in uso sulle postazioni di lavoro e la registrazione dei collegamenti alle reti Intranet/Internet.
Nel pieno rispetto della normativa vigente, l'Agenzia si riserva il diritto di verificare l'attuazione delle disposizioni del presente regolamento anche attraverso l'analisi dei dati registrati nei file di log degli apparati del sistema informativo dell'Ente.

9.2 Registrazioni

Il sistema informativo dell'Ente è basato sul dominio di rete che gestisce tutte le risorse informatiche registrate in un dominio Active Directory.
I sistemi di elaborazione effettuano le seguenti registrazioni delle attività in file di log delle seguenti tipologie e con le seguenti politiche di conservazione:

- Per ogni sistema avviene la registrazione degli eventi legati alle applicazioni, alla protezione del sistema ed al sistema stesso. La conservazione ha durata limitata a 4 mesi al fine di poter analizzare eventuali problemi di sicurezza.
- I server del sottosistema di configurazione dinamica degli indirizzi di rete (DHCP – Dinamyc Host Configuration Protocol) conservano le registrazione delle allocazioni degli indirizzi di rete alle stazioni di lavoro. La conservazione ha durata limitata a 4 mesi.
- Il dispositivo di gestione degli accessi ad Internet, effettua la registrazione di tutti i dati di accesso ad Internet, inclusi i dati dell'indirizzo IP dell'utente e gli URL (Uniform Resource Locator) consultati. La conservazione ha durata limitata dallo spazio disco a disposizione e non superiore a 4 mesi.
- Il server di posta elettronica conserva tutte le mail degli utenti, nei limiti dello spazio disco a disposizione e delle regole di conservazione definite, e conserva le registrazioni degli elementi di descrizione del traffico di posta elettronica. I messaggi di posta elettronica vengono anche utilizzati per la classificazione dei messaggi di posta elettronica indesiderati (SPAM). La conservazione è regolamentata da un contratto con il fornitore di servizi.
- Tutte le registrazioni possono essere consultate unicamente dall'amministratore di sistema e dal titolare per scopi legati alla verifica del buon funzionamento del sistema informativo dell'Ente per motivi di sicurezza.

9.3 Controlli sull'Uso delle Risorse del Sistema Informativo

I dati registrati potranno essere aggregati per svolgere controlli finalizzati ad evitare abusi nell'uso di Internet o per determinare le cause di eventuali malfunzionamenti del sistema.
I controlli verranno effettuati dall'amministratore di sistema per verificare la sicurezza della rete dell'Ente e prevenire o risolvere eventuali problemi di sicurezza.
In particolare, l'Amministratore di Sistema per le verifiche seguirà le seguenti procedure:

- Internet: verranno visionati, attraverso specifica reportistica ottenuta tramite programmi di analisi Log e in forma anonima, le tipologie di accesso (https, ftp, ecc.), il numero di accessi e di visualizzazione delle pagine, le ore di utilizzo totali e le fasce orarie di utilizzo, i tentativi di intrusione dalla rete internet verso la rete dell'Ente o la singola postazione informatica dell'Agenzia.
- Posta elettronica: analisi dei flussi di ricezione e spedizioni e-mail dall'indirizzo di posta elettronica dell'Ente assegnato a ciascun utente, con esame dei dati relativi alla frequenza ed alla tipologia di anomalie nella spedizione/consegna del messaggio, oltre che nella ricezione dello stesso.

- Rete interna: verranno verificati i tentativi di intrusione ed accesso alle risorse dell'Ente (file e cartelle) protette, sia di quelle presenti in rete che non. Inoltre, sarà verificato il numero di accessi complessivi ed ogni tentativo di accesso negato a risorse dell'Ente protette.

Ogni abuso nell'uso del sistema informativo sarà comunicato alle figure indicate nel cap 3 Ruoli.
L'amministratore di sistema, su richiesta dell'autorità giudiziaria o delle forze di polizia, potrà in ogni momento fornire i dati registrati dal sistema.

10 Data Breach (violazione dei dati personali)

I dati personali conservati, trasmessi o trattati dall'ente possono essere soggetti al rischio di perdita, distruzione o diffusione indebita, ad esempio a seguito di attacchi informatici, accessi abusivi, eventi avversi, come incendi o altre calamità. Si tratta di situazioni che possono comportare pericoli significativi per la privacy degli interessati cui si riferiscono i dati.
Nel caso in cui l'utente del sistema informativo riscontri una violazione delle banche dati dell'ente contenenti dati personali ne deve dare immediata informazione al Titolare o al Responsabile dei sistemi informativi.
Il titolare deve avviare una procedura di comunicazione all'autorità garante del trattamento dei dati come previsti all'articolo.

11 Incarico per il Trattamento dei Dati

Il RE 679/2016, disciplina la gestione dei dati personali ed impone che all'interno di ogni ente sia costituita una gerarchia, comprendente le figure del titolare, del responsabile del trattamento, funzionale alla sua applicazione. Tale gerarchia non comporta alcuna modifica della qualifica professionale o delle mansioni assegnate ai dipendenti.
Ogni singolo Impiegato è autorizzato al trattamento di dati personali (dato che nell'ambito dello svolgimento delle proprie funzioni viene necessariamente a conoscenza dei contenuti delle banche dati presenti presso la propria unità operativa) nell'ambito delle mansioni ad esso assegnate. Le banche dati cui potrà accedere per il trattamento - previa abilitazione ed indicazione delle modalità di utilizzo - sono unicamente quelle previste per il ruolo assegnato identificato nel documento di incarico al trattamento dei dati.
Per il trattamento di dati deve intendersi: "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"

Brescia li 30 Set 2018

Il dipendente dell'Agenzia del TPL di Brescia per presa Visione