Privacy

FILM COMMISSION TORINO PIEMONTE

VIA CAGLIARI 42
10153 - TORINO (TO)
P.IVA 97601340017

REGOLAMENTO INFORMATICO PER IL TRATTAMENTO E LA SICUREZZA DEI DATI PERSONALI

Ai sensi del Decreto Legislativo 30 giugno 2003 n. 196 e s.m.i.
Codice in materia di protezione dei dati personali

Ai sensi dell'Allegato B del Codice
Disciplinare tecnico in materia di misure minime di sicurezza

Ai sensi del Provvedimento del
Garante per la protezione di dati personali, n.13 del 1° marzo 2007,
Gazzetta Ufficiale n.58 del 10 marzo 2007

N° Revisione	Data	Oggetto
0	04/12/2015	Emissione

Sommario

REGOLAMENTO INFORMATICO 1
PER IL TRATTAMENTO E 1
LA SICUREZZA DEI DATI PERSONALI 1
1 RIFERIMENTI NORMATIVI 2
1.1 PREMESSA 2
1.2 DISCIPLINARE INFORMATICO E INFORMATIVA 2
1.3 AMBITO 3
1.4 AGGIORNAMENTI 3
2 DEFINIZIONI 4
3 INCARICO DI TRATTAMENTO 6
3.1 DESIGNAZIONE DEGLI INCARICATI DEL TRATTAMENTO 6
3.2 ISTRUZIONI E PRESCRIZIONI GENERALI 6
4 BANCHE DI DATI E RELATIVI TRATTAMENTI 8
5 TRATTAMENTI CON STRUMENTI ELETTRONICI 9
5.1 AUTORIZZAZIONE ALL'UTILIZZO DELLA STRUMENTAZIONE ELETTRONICA 9
5.2 NORME DI COMPORTAMENTO 9
5.3 PERSONALE TECNICO ESTERNO 9
5.4 UTILIZZO DEGLI ELABORATORI ELETTRONICI 9
5.5 SISTEMA DI AUTENTICAZIONE E DI AUTORIZZAZIONE 10
5.5.1 Credenziali di autenticazione sugli elaboratori 11
5.5.2 Modalità di custodia 11
5.5.3 Accesso alla parola chiave di un incaricato 11
5.6 CREDENZIALI DI AUTENTICAZIONE PER PROGRAMMI E SITI WEB AD ACCESSO RISERVATO 12
5.7 POSTA ELETTRONICA 12
5.7.1 Risposta automatica in caso di assenza 12
5.7.2 Accesso straordinario e individuazione fiduciario 12
5.7.3 Accesso dopo la cessazione del rapporto di lavoro 13
5.7.4 Ulteriori indicazioni 13
5.8 NAVIGAZIONE IN INTERNET 13
5.9 MEMORIZZAZIONE DI DATI E DOCUMENTI ELETTRONICI 14
5.10 PROTEZIONE DA VIRUS 15
5.11 ULTERIORI SISTEMI DI PROTEZIONE 15
5.12 OSSERVANZA DELLE DISPOSIZIONI E CONTROLLI 15
RICEVUTA 1

1 Riferimenti normativi

1.1 Premessa

La riservatezza delle persone attraverso la corretta acquisizione, gestione e circolazione dei dati personali e mediante l'adozione di adeguate misure di sicurezza per la loro protezione è tutelata, a partire dal 1° gennaio 2004, dal Decreto Legislativo 30 giugno 2003 n. 196 *("Codice in materia di protezione dei dati personali"; nel seguito, "Codice Privacy").*

Il Codice Privacy disciplina il trattamento dei dati personali secondo le regole già dettate dalla Legge 31/12/1996 n. 675 *("Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali")* ora abrogata. Sotto l'aspetto delle misure minime di sicurezza da adottare per la loro protezione, sono state introdotte una serie di specifiche normative contenute nel *Disciplinare tecnico,* emanato in allegato "B" al testo del Codice Privacy, che sarà periodicamente aggiornato con appositi Decreti interministeriali, *"…in relazione all'evoluzione tecnica e all'esperienza maturata nel settore"*.

Le misure di sicurezza prescritte dal Codice Privacy sono intese nel senso più ampio e riguardano il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali che configurano i livelli di protezione necessari a ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Per l'adempimento di tali prescrizioni e per conseguire in ogni caso il migliore livello di protezione dei dati personali trattati, sono adottate e prescritte le misure di sicurezza illustrate nelle sezioni che seguono.

1.2 Disciplinare informatico e informativa

Il Provvedimento del Garante per la protezione di dati personali, n.13 del 1° marzo 2007, Gazzetta Ufficiale n.58 del 10 marzo 2007, definisce il disciplinare o regolamento informatico, come il documento redatto dal Titolare del trattamento e da far sottoscrivere ai lavoratori all'atto di assunzione o successivamente con atto separato, che disciplina l'utilizzo della strumentazione informatica aziendale.

Tale documento è idoneo sia a sollevare il titolare del trattamento, **MANERA PAOLO**, da eventuali responsabilità civili o penali relative ad un illecito utilizzo della strumentazione informatica da parte del personale, sia per i dipendenti, al fine di distinguere gli atti concernenti l'attività aziendale da quelli estranei alla stessa in relazione alla strumentazione informatica, fornendo garanzie circa il trattamento dei loro dati personali.

L'illecito utilizzo della strumentazione informatica aziendale può generare una serie di responsabilità sia penali che civili in capo al titolare del trattamento, **MANERA PAOLO**, qualora questo non dimostri di aver adoperato tutte le precauzioni al fine di evitarne il compimento. Il regolamento può pertanto definirsi come **strumento di prevenzione** in grado innanzi tutto di dimostrare l'attenzione e la volontà di **evitare eventi estranei all'attività lavorativa**, dall'altra come strumento di **indicazione per gli utenti su come utilizzare le risorse informatiche** aziendali senza per questo incorrere, anche in buona fede, in illeciti.

Inoltre, il disciplinare rappresenta un momento evolutivo, laddove intervenendo in modo puntuale, consente di individuare quali limiti e quali diritti sono vigenti all'interno dell'ambiente lavorativo.

In particolare, il disciplinare regola ed informa circa le corrette modalità di gestione del software affinché siano scongiurati i problemi connessi alla pirateria informatica ed alla violazione della legge sul diritto d'autore, come l'illecita riproduzione di programmi o il loro uso senza regolare licenza.

Per quanto riguarda Internet, l'uso improprio che se ne può fare costituisce sì un sottrazione di tempo al lavoro, ma può anche assumere forme più gravi, qualora la navigazione si concretizzi in illeciti penali, quali ad esempio lo scambio di contenuti illegali. Pertanto occorre procedere ad informare circa i sistemi

di tutela predisposti (blocchi, filtri, log, ecc.), salvo il rispetto di un generico principio di tollerabilità per le navigazioni di breve durata anche se non attinenti la materia lavorativa.

In relazione alla posta elettronica, occorre distinguere tra caselle ad uso personale o lavorativo e tra procedure per l'accesso straordinario ai messaggi e per l'archiviazione delle comunicazioni.

Con l'entrata in vigore del Codice in materia di protezione dei dati personali (D.Lgs. 196/2003), inoltre, emerge essenziale impartire istruzioni agli operatori circa le modalità e le precauzioni da adottare in occasione del trattamento dei dati: dalla segretezza, alla riservatezza di taluni, alle modalità di salvataggio. Centrale è inoltre l'indicazione relativamente alla custodia, conservazione e controllo dei dati informatici, o all'uso di credenziali di autenticazione, o del divieto relativo all'utilizzo di supporti informatici estranei all'ambito aziendale.

Il regolamento informatico individua in modo specifico l'esatta destinazione della strumentazione informatica, evitando a priori che possano nascere equivoci relativamente al duplice utilizzo della stessa (aziendale e personale) e ne informa in maniera precisa e chiara gli utilizzatori (art. 13, D.Lgs. 196/2003), richiedendone il consenso (art. 23, D.Lgs. 196/2003) per il trattamento delle tracce che l'utilizzo del sistema genera in riferimento alla loro stessa attività.

1.3 Ambito

Le norme di seguito riportate all'interno del Regolamento hanno valore di ordine di servizio.

Tutti i soggetti (incaricati e non) che operano nell'ambito del titolare del trattamento, MANERA PAOLO, compresi i dipendenti, i collaboratori non dipendenti, i consulenti esterni, gli addetti alle manutenzioni che per effetto della loro attività possono avere accesso ai dati, gli ospiti e tutti coloro che accedano all'interno delle sedi e dei locali nella disponibilità giuridica del titolare del trattamento, **MANERA PAOLO**, ed utilizzino le strutture messe a disposizione sono tenuti al rispetto scrupoloso del Regolamento, nell'ambito delle proprie competenze e attività.

L'inosservanza di tali norme potrà essere suscettibile di provvedimenti, commisurati alla gravità della violazione.

1.4 Aggiornamenti

Con l'emanazione di successive versioni del Regolamento tali misure di sicurezza verranno tempestivamente adeguate, nel costante rispetto delle prescrizioni minime previste dalla legge, in relazione all'evoluzione della tecnologia ed alle concrete esperienza maturate nel frattempo.

2 Definizioni

Ai fini del Codice Privacy si intende per:

“autenticazione informatica”, l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

“banca di dati”, qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

“credenziali di autenticazione”, i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l' autenticazione informatica;

“dato personale”, qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

“dati identificativi”, i dati personali che permettono l'identificazione diretta dell'interessato;

“dati sensibili”, i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, ***nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale***;

“trattamento”, qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

“titolare”, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

“responsabile”, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

“incaricati”, le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

“misure minime”, il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;

“parola chiave”, componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;

“profilo di autorizzazione”, l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

“sistema di autorizzazione”, l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

“strumenti elettronici”, gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

“**servizio di comunicazione elettronica**”, i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni;

“**utente**”, qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali

3 Incarico di trattamento

3.1 Designazione degli incaricati del trattamento

Il titolare del trattamento, MANERA PAOLO, nell'ambito della propria attività, **conferisce**, previa identificazione e classificazione delle attività svolte, **la designazione a incaricato del trattamento dei dati personali** ai sensi dell'art. 30 del Codice Privacy, nell'ambito dei principali, criteri, procedure, obblighi ed istruzioni di seguito impartite.

L'incarico viene conferito in relazione alla natura dei trattamenti svolti, alle modalità di trattamento ed ai mezzi utilizzati nell'ambito della propria unità operativa, e viene correlato ai compiti ed alle funzioni svolte in modo tale da poter raggruppare, per classi omogenee di comportamento, uniformi profili di autorizzazione al trattamento, a loro volta rapportati ai profili di autorizzazione per l'accesso ai dati ed ai relativi trattamenti con strumenti elettronici.

La designazione a incaricato non dipende dalla forma contrattuale attraverso cui si svolge l'incarico e pertanto si estende anche a quei soggetti che funzionalmente possono svolgere, anche occasionalmente o temporaneamente, operazioni di trattamento dei dati.

Nel caso in cui un soggetto tratti dati personali **senza aver ricevuto formale lettera di incarico** attraverso uno dei modelli previsti nel DPS (MOD_IT, MOD_CAT, MOD_EXT, MOD_ADS, MOD_RGSE, MOD_MTZ, ecc.) **deve immediatamente informare il Responsabile della sicurezza del trattamento, MANERA PAOLO**.

I soggetti (es. addetti alla gestione e manutenzione degli strumenti elettronici) che non hanno necessità di effettuare trattamenti di dati personali, ma che in via accidentale ed eccezionale potrebbero comunque trovarvisi in presenza, ricevono comunque designazione a incaricati del trattamento con formale prescrizione di specifiche misure di sicurezza per l'accesso al sistema mediante gli strumenti elettronici messi a loro disposizione e con l'indicazione di considerare tutti i dati come confidenziali e soggetti al più rigoroso segreto d'ufficio.

3.2 Istruzioni e prescrizioni generali

Nell'effettuare le operazioni di trattamento, **ogni incaricato** – oltre alla normativa di cui ai capitoli successivi – **dovrà osservare le seguenti istruzioni e prescrizioni generali di comportamento**:

- potrà accedere ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti a ciascuno assegnati;

- dovrà operare garantendo la massima riservatezza delle informazioni di cui viene in possesso, considerando tutti i dati personali come confidenziali e, di norma, soggetti al segreto d'ufficio;

- dovrà trattare e custodire i dati, indipendentemente dalla loro natura, evitando che essi siano esposti a rischi di perdita o distruzione anche accidentale, che ad essi possano accedere persone non autorizzate, che su di essi vengano svolte operazioni di trattamento non consentite o non conformi ai fini per i quali sono stati raccolti e per i quali vengono trattati;

- dovrà astenersi dall'eseguire trattamenti per fini non previsti tra i compiti assegnatigli dal diretto responsabile dell'unità organizzativa di appartenenza, o comunque riferiti a disposizioni e Regolamenti;

- dovrà astenersi dallo svolgere qualsiasi attività che non sia espressamente compresa nel proprio profilo di abilitazione, operando con la massima diligenza ed attenzione in tutte le fasi del trattamento, dalla esatta acquisizione dei dati, al loro eventuale aggiornamento, alla conservazione ed eventuale cancellazione o distruzione;

- dovrà curare che nessun dato personale, su supporto magnetico, digitale o cartaceo, venga lasciato incustodito o trasportato al di fuori delle aree di lavoro in cui avvengono i trattamenti; tale materiale, durante le normali operazioni di lavoro, non dovrà risultare visibile a persone che non siano incaricate degli stessi trattamenti e, a fine lavoro, verrà conservato in armadi o cassetti che, nel caso di documenti contenenti dati "sensibili" o "giudiziari", dovranno essere chiusi a chiave, senza lasciare le chiavi in vista.

4 Banche di dati e relativi trattamenti

Le banche di dati personali costituite presso **il titolare del trattamento, MANERA PAOLO,** ed i trattamenti che su di esse sono svolti nell'ambito della normale attività, sono oggetto di censimento che viene costantemente tenuto aggiornato, anche al fine di adottare le misure di sicurezza previste dal Codice Privacy.

Al fine di assicurare nel tempo il rispetto di tali prescrizioni, e di mantenere la massima efficacia delle misure di sicurezza adottate per la protezione di tali dati contro ogni possibile rischio, si dispone che quando si manifestasse, per qualsiasi motivo, l'esigenza di costituire una nuova banca di dati personali (o di introdurre nuove finalità o modalità di trattamento per quelle già in essere), dovrà esserne richiesta preventiva autorizzazione al **Responsabile della sicurezza del trattamento, MANERA PAOLO**, illustrandone i motivi, le finalità e le modalità di gestione.

5 Trattamenti con strumenti elettronici

5.1 Autorizzazione all'utilizzo della strumentazione elettronica

Con il presente regolamento, ai sensi del D.Lgs. n. 196 del 30 giugno 2003, si autorizzano gli incaricati del trattamento all'utilizzo della strumentazione elettronica in dotazione (computer, stampanti, fax, scanner, fotocopiatori, dispositivi di rete, ecc.) per lo svolgimento dei compiti assegnati ed in particolare per il trattamento dei dati personali entro il proprio ambito e secondo le istruzione ricevute

5.2 Norme di comportamento

Si ribadisce e si sollecita l'adozione dei corretti comportamenti per l'utilizzo degli elaboratori elettronici, delle credenziali di autenticazione, della posta elettronica, della navigazione in internet e della memorizzazione di dati e documenti elettronici, secondo quanto stabilito dal Titolare del trattamento, MANERA PAOLO, in accordo e sotto la supervisione del Responsabile della sicurezza del trattamento, MANERA PAOLO e del Responsabile della gestione e manutenzione della strumentazione elettronica PAPA ALFONSO.

Tutti gli incaricati devono essere a conoscenza delle modalità e procedure in vigore (regolamento) nell'utilizzo del sistema informativo interno.

5.3 Personale tecnico esterno

Il Titolare del trattamento, MANERA PAOLO, si avvale di personale tecnico per compiere le operazioni di manutenzione, installazione, configurazione e controllo che si rendessero necessarie; in particolare gli addetti (persone o ditte, interne o esterne) autorizzati ad operare sono:

- COMPUTER'S TIME
- CSI PIEMONTE
- IT.GATE SPA
- PAPA ALFONSO
- TECNONET SPA

ciascuno nel proprio ambito, come definito nel Documento Programmatico Sulla Sicurezza.

5.4 Utilizzo degli elaboratori elettronici

L'elaboratore elettronico in dotazione è uno strumento di lavoro, adeguato alle necessità, ai compiti ed agli incarichi di competenza di ciascun incaricato.

È fatto tassativo divieto dell'utilizzo dello strumento per scopi differenti e/o personali.

Qualora siano svolti da qualsiasi utente, per fini esclusivamente personali, trattamenti di dati personali non riconducibili al titolare del trattamento, MANERA PAOLO, seppur utilizzando strumenti e apparecchiature elettroniche messe a disposizione da quest'ultimo, si richiama l'attenzione sul fatto che, in ogni caso, tale trattamento è soggetto a precise regole, ai sensi del codice Privacy, in tema di responsabilità e di sicurezza dei dati, che competono personalmente al soggetto che lo effettua.

In particolare, l'art. 5, comma 3, dispone: "Il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali è soggetto all'applicazione del presente codice solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione. Si applicano in ogni caso le disposizioni in tema di responsabilità e sicurezza di cui agli articoli 15 e 31".

E l'art. 15 (Danni cagionati per effetto del trattamento) dispone: "1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile. 2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11."

Per quanto riguarda l'art. 31 (Obblighi di sicurezza) vale: "1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o

perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta."

Infine, l'art. 11 (Modalità del trattamento e requisiti dei dati) recita: "1. I dati personali oggetto di trattamento sono: a) trattati in modo lecito e secondo correttezza; b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi; c) esatti e, se necessario, aggiornati; d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati; e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati. 2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati."

Il Responsabile della gestione della strumentazione elettronica (d'ora in avanti e per brevità, il Responsabile) può disporne secondo necessità, sostituendo, aggiornando, rimuovendo o adeguando in tutto o in parte le componenti hardware e/o software di cui esso si compone, senza necessità di preavviso e di richiesta di consenso da parte dell'utilizzatore.

Il Responsabile è l'unico che può provvedere o autorizzare l'installazione, l'aggiornamento e la configurazione di dispositivi hardware e/o software sui programmi in uso, sugli elaboratori elettronici, sulla rete informatica e più in generale sull'intero sistema informativo.

In particolare, in modo non esaustivo, si intende stigmatizzare i comportamenti relativi ai seguenti divieti:

- Non è consentito modificare le caratteristiche hardware e software impostate sull'elaboratore.
- Non è consentita l'installazione di programmi diversi da quelli autorizzati.
- Non è consentita la riproduzione, la duplicazione, il salvataggio o lo scarico (download o file sharing) di programmi informatici o file di ogni tipo (testo, immagini, video, audio, eseguibili) in violazione delle norme sul diritto d'autore, ai sensi delle Legge n. 128 del 21 maggio 2004.
- Non è consentita l'installazione di ulteriori dispositivi (masterizzatori, modem, ecc.) rispetto a quelli in dotazione.
- Non è consentito l'uso di qualsiasi dispositivo esterno rimovibile (ad es. USB pen drive), se non quelli aziendali o quelli autorizzati per l'uso all'interno della rete aziendale per motivi attinenti esclusivamente alla propria attività.

L'utilizzatore che abbia necessità di apportare modifiche software o hardware all'elaboratore in dotazione, installando nuovi programmi o dispositivi, deve farne preventiva richiesta al Responsabile.

Quanto memorizzato sui supporti magneti, ottici ed elettronici potrebbe essere oggetto di analisi, controllo e duplicazione da parte del Responsabile o da personale tecnico autorizzato, per migliorare l'affidabilità del sistema informativo e la disponibilità dei dati.

Qualora fossero individuate componenti hardware e/o software (programmi, documenti, dispositivi esterni, ecc.) non corrispondenti ai criteri di sicurezza e di operatività individuati dal Responsabile o non esplicitamente autorizzati, tali componenti potrebbero essere rimossi e l'utilizzatore potrebbe essere coinvolto negli accertamenti e nelle verifiche del caso.

5.5 Sistema di autenticazione e di autorizzazione

L'accesso ai dati personali per il loro trattamento con strumenti elettronici è gestito da un **sistema di autenticazione informatica**, che prevede:

- l'assegnazione di **credenziali di autenticazione** ad ogni singolo incaricato;
- il superamento di una **procedura di autenticazione** relativa a uno specifico trattamento o a un insieme di trattamenti;

5.5.1 Credenziali di autenticazione sugli elaboratori

Le credenziali di autenticazione utilizzate sugli elaboratori consistono in un codice, associato a una parola chiave riservata, da inserire al termine dell'avvio del sistema operativo dell'elaboratore medesimo.

Codice e parola chiave sono anche definiti login e password e sono atti all'identificazione personale dell'utilizzatore di un elaboratore elettronico, nella sua qualità di incaricato al trattamento.

È prescritto di adottare le necessarie cautele per assicurare la segretezza della password, evitando di comunicarla ai colleghi e/o a terzi e di trascriverla o annotarla in modo evidente o comunque visibile.

La parola chiave deve essere composta da almeno otto caratteri alfanumerici (lettere maiuscole e minuscole, cifre numeriche, segni di punteggiatura) oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non deve contenere riferimenti agevolmente riconducibili al codice (login) e/o all'incaricato. La password deve essere modificata al primo utilizzo e successivamente ne sarà richiesto il cambio, a scadenza prefissata, a cura dei server aziendali.

Si potrà modificare autonomamente la parola chiave, seguendo le istruzioni del Responsabile o del personale tecnico autorizzato, preposti a fornire l'adeguata assistenza.

Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica. Inoltre le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

Si ribadisce inoltre di non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento, ma di provvedere al blocco dell'utilizzo del medesimo, attivando la funzionalità di richiesta delle credenziali di autenticazione per il ripristino di una sessione di lavoro sospesa (screen saver con password).

5.5.2 Modalità di custodia

La custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza.

I soggetti incaricati della custodia delle copie delle credenziali sono:

- MANERA PAOLO

Per la custodia delle copie delle credenziali degli elaboratori, è adottata una **modalità cartacea**, in quanto non esiste la possibilità o troppo complesso il metodo che permette di ripristinare il contenuto della password ad un valore noto attraverso comandi impartiti al sistema di autenticazione informatica stesso.

L'utente titolare della password comunica i dati necessari all'**incaricato della custodia delle copie delle credenziali di autenticazione**, il quale predispone, per ogni utenza, una busta sulla quale è indicato il nome dell'incaricato, l'elaboratore elettronico in uso e, all'interno della busta, la credenziale usata, secondo il modello MOD_PWD del DPS (Documento Programmatico per la Sicurezza).

L'**incaricato della custodia delle copie delle credenziali di autenticazione** conserva le buste con le credenziali in luogo chiuso e protetto.

5.5.3 Accesso alla parola chiave di un incaricato

Per assicurare la disponibilità di dati o strumenti elettronici in caso di assenza prolungata o impedimento che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, il Responsabile del trattamento osserva la seguente procedura:

nel caso di password in custodia con modalità cartacea, **l'incaricato della custodia** accede al sistema utilizzando la password dell'utente assente..

Di norma, l'utente titolare della credenziale di autenticazione, oggetto di accesso straordinario, è **informato dell'operazione** svolta, mediante la consegna di un apposito verbale, ed è invitato a **provvedere immediatamente a sostituire la password in essere**, anche prima della scadenza naturale prevista.

5.6 Credenziali di autenticazione per programmi e siti web ad accesso riservato

Alcuni programmi o siti web necessari per svolgere l'attività lavorativa forniscono un ulteriore livello di autenticazione, oltre a quello dell'elaboratore.

Alcuni siti web sono concessi in uso al Titolare del trattamento, il quale, a sua volta, mette a disposizione ciascun sito, a seconda delle necessità, agli incaricati autorizzati che vi accedono con profilo di autorizzazione univoco previa autenticazione mediante codice identificativo e parola chiave condivisa da tutti gli incaricati autorizzati e assegnata dall'amministratore del sito.

5.7 Posta elettronica

Qualora ad un incaricato del trattamento, per l'adempimento delle proprie mansioni, sia affidata una casella di posta elettronica, valgono le seguenti indicazioni:

- l'utilizzo della posta elettronica è strettamente limitato all'uso lavorativo;
- la posta elettronica non può essere impiegata per l'invio e la ricezione di comunicazioni di carattere personale, anche se l'indirizzo identificativo può contenere parti che richiamano al nominativo del destinatario;
- non è possibile garantire la riservatezza dei messaggi inviati e ricevuti, essendo tutte le comunicazioni entranti o uscenti, passibili di analisi, controllo, duplicazione e archiviazione da parte del Responsabile o da personale tecnico autorizzato, al fine di migliorare l'affidabilità del sistema informativo e la disponibilità dei dati e di tutelare l'organizzazione nei rapporti con terzi;
- è vietato spedire e ricevere comunicazioni inerenti l'attività lavorativa (compreso inoltro di documenti aziendali) su caselle di posta personali, non aziendali, salvo specifica autorizzazione.

5.7.1 Risposta automatica in caso di assenza

In caso di assenze pianificate o prolungate si dovrà personalizzare il seguente testo di esempio inserendolo nelle regole fuori sede della posta elettronica: "***Sono assente dall'ufficio, per comunicazioni…*** (da completare con ***inviare il messaggio a*** indirizzo di posta elettronica nominativo/di gruppo ovvero ***contattare il numero……***)." Si precisa che questa disposizione in caso di assenza improvvisa e prolungata potrà essere attivata dai gestori del sistema.

5.7.2 Accesso straordinario e individuazione fiduciario

Inoltre, qualora si manifestassero improrogabili necessità legate all'attività lavorativa, durante un'assenza prolungata o non prevista, il personale tecnico autorizzato dal Responsabile verificheranno il contenuto dei messaggi e inoltreranno al Responsabile quelli ritenuti rilevanti ai fini lavorativi. Di tale attività sarà redatto apposito verbale, di cui sarà data copia all'incaricato interessato dal provvedimento.

L'utente può, in aggiunta, indicare con apposita delega un fiduciario, nell'ambito della unità organizzativa di appartenenza, nella persona del responsabile dell'Unità ovvero altro addetto. Il fiduciario, controfirmata la delega per accettazione, in caso di necessità avrà il compito di verificare il contenuto dei messaggi e curare l'inoltro alle competenti funzioni aziendali di quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Anche in questo caso il fiduciario deve redigere apposito verbale e consegnarlo alla prima occasione utile all'utente interessato.

5.7.3 Accesso dopo la cessazione del rapporto di lavoro

In caso di cessazione del rapporto di lavoro dell'incaricato del trattamento, affidatario di una casella di posta elettronica, il personale tecnico autorizzato dal Responsabile provvederà ad assegnare tale casella ad un altro incaricato (non necessariamente il fiduciario).

Nel caso in cui l'indirizzo identificativo di tale casella contenga parti che richiamano al nominativo dell'ex-incaricato, la casella sarà affidata ad altri solo temporaneamente (massimo 6 mesi) e successivamente dismessa (entro 18 mesi dalla cessazione); sarà eventualmente attivato un messaggio di risposta automatico per informare il mittente dei nuovi recapiti da utilizzare e/o del fatto che la casella sarà dismessa. I messaggi potranno essere modificati ed adeguati nel tempo.

L'archivio dei messaggi inviati e ricevuti per tramite della casella sarà mantenuto secondo le politiche delle caselle attive.

Eventuali messaggi di carattere personale che non abbiano contenuti afferenti all'ambito lavorativo, indirizzati all'ex-incaricato saranno tempestivamente rimossi dall'archivio della posta elettronica e, per quanto possibile, resi irrecuperabili.

5.7.4 Ulteriori indicazioni

In ogni comunicazione elettronica inviata all'esterno, è consigliabile apporre in calce la seguente dicitura:

"La presente e-mail è riservata ed è rivolta unicamente al destinatario sopra evidenziato. I dati sono trattati dal mittente, dai collaboratori del gruppo di lavoro, dagli incaricati autorizzati, nel rispetto del D.Lgs. 196 del 30 giugno 2003; qualora persone non evidenziate quali destinatari ricevessero codesta e-mail sono pregati di informare tempestivamente la nostra struttura e di rimuovere il messaggio. Tutte le comunicazioni, sia in uscita che in ingresso, potrebbero essere conosciute ed archiviate da parte dell'organizzazione di appartenenza del mittente."

Si ritiene utile portare a conoscenza alcune norme di comportamento che salvaguardano gli elaboratori dall'infezione di virus informatici ed evitano un sovraccarico del servizio di posta elettronica:

- Nel caso di mittenti sconosciuti, di messaggi insoliti oppure di messaggi provenienti da mittenti conosciuti ma che contengono allegati sospetti (file con estensione .exe .scr .pif .bat .cmd), è opportuno cancellare i messaggi senza aprirli.

- Controllare gli allegati di posta elettronica prima del loro utilizzo: non eseguire download di file eseguibili o documenti da siti web o ftp non conosciuti.

- Evitare la diffusione incontrollata di "Catene di Sant'Antonio" (messaggi a diffusione capillare e moltiplicata).

- Utilizzare formati compressi (*.zip, *.jpg) per l'invio di allegati pesanti.

- Nel caso in cui si debba inviare un documento all'esterno è preferibile utilizzare un formato protetto da scrittura (*.pdf).

- L'iscrizione a "mailing list" esterne è concessa solo per motivi professionali. Prima di iscriversi occorre verificare in anticipo se il sito è affidabile.

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili.

5.8 Navigazione in internet

La navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. Sia durante che al di fuori dell'orario di lavoro, è assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa. Il Responsabile e personale tecnico autorizzato possono adottare politiche adattative, restrittive e di verifica sulla

navigazione, monitorando statisticamente il traffico in base a criteri su sorgente, destinazione, tipologia, durata, fascia oraria, ecc.

Inoltre vigono i seguenti divieti:

- Non possono essere utilizzati modem/router privati per il collegamento alla rete.
- E' fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato.
- E' vietato, in particolare, scaricare o effettuare streaming di contenuti multimediali (musicali, video, fotografici, ecc.) che non siano attinenti all'attività lavorativa.
- E' vietata la partecipazione a social network e forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati) e di bacheche elettroniche, la registrazione in guest books anche utilizzando pseudonimi (o nicknames).
- E' proibita l'effettuazione di ogni genere di transazione finanziaria, di remote-banking, di e-commerce, salvo i casi autorizzati.
- E' vietata la consultazione di siti con contenuti pornografici o comunque illegali, non leciti e lesivi del decoro e della morale.

Utilizzando sistemi informativi per esigenze produttive, organizzative o di sicurezza sul lavoro (ad es., per rilevare anomalie, per manutenzioni, per garantire le comunicazioni elettroniche, ecc.), è indispensabile l'uso di sistemi che consentono indirettamente un controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori, nel rispetto dello Statuto dei lavoratori (art. 4, comma 2). Tali sistemi registrano le connessioni, ovvero tengono traccia dell'ora, dell'elaboratore richiedente e della risorsa richiesta e potrebbero eventualmente memorizzare il contenuto della risposta. A meno di particolari esigenze tecniche o di sicurezza, circoscritte comunque a periodi di tempo limitati, tali sistemi sono programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovraregistrazione come, ad esempio, la cd. rotazione dei *log file*) i dati personali relativi agli accessi ad Internet e al traffico telematico.

5.9 Memorizzazione di dati e documenti elettronici

L'accesso ai dati memorizzati in locale sui singoli elaboratori risulta sempre protetto dalla procedura di controllo degli accessi che, come descritto ai paragrafi precedenti, richiede l'utilizzo delle credenziali di autenticazione per ottenere l'accesso ai dati e la verifica dei privilegi di accesso gestiti dal sistema di autorizzazione.

Il salvataggio di dati, documenti e file rilevanti per l'attività lavorativa, utilizzabili da altri utenti o comunque da salvaguardare, deve essere effettuato utilizzando le cartelle condivise del server di rete.

Nessuna procedura è implementata per il salvataggio automatico dei file residenti negli elaboratori locali. Pertanto tutti i documenti creati e/o modificati non devono essere salvati sul "Desktop" o "Scrivania" o su altra cartella locale, ma solo ed esclusivamente sugli archivi di rete.

Alcune particolari categorie di dati, denominati "sensibili", devono essere sottoposti ad una tutela particolare: i dati relativi a origine razziale ed etnica, le convinzioni religiose o filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni o ad organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale. Nel caso di trattamento dei sopraindicati dati sensibili, Ella dovrà inoltre attenersi alle seguenti misure di sicurezza:

- E' vietato l'uso di supporti di archiviazione removibili non autorizzati per la memorizzazione dei dati.
- E' vietato il salvataggio dei documenti aziendali su supporti diversi da quelli forniti ed autorizzati.

- Eventuali supporti di memorizzazione removibili (floppy disk, nastri, usb pen drive, ecc.) contenenti dati sensibili, possono essere riutilizzati solo se i dati precedentemente contenuti non sono più in alcun modo recuperabili (i dischi quindi devono essere formattati ed i nastri riscritti).

5.10 Protezione da Virus

Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus, spyware, trojan, malware o mediante ogni altro software aggressivo.

Per la protezione contro i rischi di intrusione e l'azione di programmi pericolosi, su tutti gli elaboratori è installato uno specifico software antivirus.

L'aggiornamento del software antivirus è effettuato in automatico, con cadenza giornaliera, mediante l'apposita funzione del prodotto utilizzato.

Il modulo "Autoprotezione" del software antivirus è installato con modalità residente in memoria e risulta perciò sempre attivo, assicurando una costante protezione automatica contro l'ingresso o la propagazione all'esterno di virus od altri programmi pericolosi attraverso le normali attività del posto di lavoro.

La funzione di autoprotezione non deve essere disabilitata da parte dell'Utente; qualora particolari esigenze ne rendessero necessaria la temporanea disattivazione, l'interessato dovrà farne richiesta al Responsabile, che in tal caso disporrà il costante monitoraggio del posto di lavoro per tutto il periodo in cui esso opera privo di protezione.

5.11 Ulteriori sistemi di protezione

Qualora un utente intenda ulteriormente proteggere specifici documenti informatici memorizzati sul suo posto di lavoro (in locale o in rete), dovrà sempre utilizzare le utilità di sistema rese disponibili dai singoli programmi applicativi, e in tal caso dovrà provvedere alla custodia cartacea della password utilizzata, informando il Responsabile.

5.12 Osservanza delle disposizioni e controlli

E' obbligatorio attenersi alle disposizioni di cui sopra, a quelle in materia di Privacy, contenute nel Documento Programmatico sulla Sicurezza, per quanto concerne il trattamento di dati personali con strumenti elettronici e non.

Il mancato rispetto o la violazione del regolamento potrebbe comportare provvedimenti disciplinari, anche gravi, mentre l'inosservanza delle misure di sicurezza per i dati personali, sanzioni amministrative o addirittura azioni civili e penali.

Nel rispetto dei principi di pertinenza e non eccedenza, le verifiche sugli strumenti informatici saranno realizzati nel pieno rispetto dei diritti e delle libertà fondamentali degli utenti e dei regolamenti aziendali. Il tecnico preposto effettua verifiche periodiche su ciascuno strumento informatico in dotazione agli utenti al fine di garantire il funzionamento ottimale degli strumenti e verificare il rispetto del presente Regolamento. I controlli sono effettuati con cadenza almeno semestrale e avvengono con gradualità per reparto, ufficio, gruppo di lavoro, ecc. in modo da individuare l'area da richiamare all'osservanza delle regole

In caso di successive, perduranti anomalie, ovvero ravvisandone comunque la necessità, il Titolare si riserva di effettuare verifiche anche su base individuale, comunque finalizzate esclusivamente alla individuazione di eventuali condotte illecite. In nessun caso verranno realizzate verifiche prolungate, costanti o indiscriminate, fatte salve le verifiche atte a tutelare gli interessi di FILM COMMISSION TORINO PIEMONTE.

RICEVUTA

La preghiamo di restituirci copia della presente RICEVUTA firmata per ricevuta ed accettazione del REGOLAMENTO INFORMATICO PER IL TRATTAMENTO E LA SICUREZZA DEI DATI PERSONALI

Distinti saluti.

MANERA PAOLO

Luogo e Data: _____

Io sottoscritto (nome e cognome) _____

dichiaro di aver ricevuto copia del

REGOLAMENTO INFORMATICO PER IL TRATTAMENTO E LA SICUREZZA DEI DATI PERSONALI

e di averne preso visione e di averlo compreso ed accettato integralmente.

In fede

R