PRIVACY – CODICE DI CONDOTTA SUL TRATTAMENTO DEI DATI PERSONALI

Ai sensi dell'art. 4 numero 7 del Reg. UE 2016/679 ("**GDPR**") «il titolare del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri».

Il titolare del trattamento dei dati personali è Cinecittà S.p.A. – Sede legale: Via Tuscolana, 1055 - 00173 Roma (ITALIA), nella persona dell'Amministratore Delegato Dott. Nicola Maccanico (di seguito il "Titolare del trattamento dei dati personali" o "Titolare"),

Responsabile per la Protezione dei Dati Personali è l'Avv. Luca Sanna, domiciliato presso "Studium Cives – Studio Legale" – Via Cistoforo Colombo, 348 – 00145 - Roma ("RPD" o "DPO") e contattabile all'indirizzo mail dpo@cinecittaluce.it.

Privacy Officers che coadiuvano il Responsabile per la Protezione dei Dati Personali sono la Dott.ssa Fabiola Solvi e il Dott. Ludovico Schiavo.

L'ufficio del DPO è contattabile all'indirizzo e-mail dpo@cinecittaluce.it.

Ai sensi dell'art. 4 numero 8 del GDPR è definito «responsabile del trattamento» "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento" (il "**Responsabile**" o il "**Responsabile del Trattamento**"); il responsabile del trattamento è nominato tra soggetti che per esperienza, capacità e affidabilità diano idonea garanzia del rispetto delle disposizioni in materia di trattamento dei dati personali, ivi compreso il profilo della sicurezza.

La figura del Responsabile del Trattamento dei dati personali non è stata indicata all'interno dell'organigramma sociale e dunque coincide con la figura del Titolare del Trattamento.

Infine, l'articolo 29 del Reg. UE. 2016/679 prescrive che chiunque agisca sotto la autorità del Titolare del trattamento ovvero sotto quella del responsabile del trattamento e che abbia accesso a dati personali non possa trattare tali dati se non è istruito in tal senso dal Titolare, salvo che lo richieda il diritto dell'Unione Europea o degli Stati membri. Tale articolo è completato dall'art. 2-*quaterdecies* del D.Lgs. n. 196/2003 (Codice Privacy italiano) il quale stabilisce che «Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta». Si tratta dei cd. Designati autorizzati al trattamento (ovvero la figura che nel vecchio testo del Codice privacy italiano precedente l'entrata in vigore del GDPR era denominata dell'"Incaricato").

A tal proposito Cinecittà S.p.A. ha inteso nominare quale autorizzati al trattamento tutto il personale che svolge qualsivoglia attività in tal senso, attraverso l'individuazione di due tipologie di autorizzati:

- gli autorizzati di I Livello, coloro i quali svolgono un primo livello di trattamento sorvegliando e vigilando l'applicazione delle prescrizioni di cui al GDPR nei confronti degli Autorizzati di secondo livello. Tali soggetti sono stati individuati nelle figure dirigenziali della società, con competenze che naturalmente si riverberano nelle rispettive aree di competenza (gli "**Autorizzati di I Livello**").
- gli autorizzati di II Livello, coloro che – quadri e impiegati - in ragione della propria mansione, trattano dati personali. L'individuazione dei soggetti autorizzati può avvenire anche mediante la documentata preposizione di una persona fisica ad una unità per la quale è stato individuato l'ambito del trattamento consentito agli addetti all'unità medesima (gli "**Autorizzati di II Livello**").

Cinecittà S.p.A. individua tre tipologie di dati personali che possono essere trattati:

a) **Art. 4 n. 1 GDPR:**

«dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

b) **Art. 9 GDPR:**

«Categorie Particolari»: sono i dati sensibili ovvero quei dati personali idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;

c) **Art. 10 GDPR:**

Dati Personali relativi a condanne penali o reati

I trattamenti svolti in seno a Cinecittà S.p.A. possono essere di due specie:

a) trattamenti di primo livello, che riguardano attività trasversali e sono svolti utilizzando la rete e il sistema informativo automatizzato della Società;

b) trattamenti di secondo livello: sono quelli specifici delle singole unità di trattamento, che sono monitorati e gestiti direttamente dai singoli Autorizzati di I Livello.

Con la designazione scritta il soggetto autorizzato può procedere al trattamento dei dati personali che sia strumentale allo svolgimento delle mansioni contrattuali per cui è stato assunto (il riferimento è alla categoria di appartenenza) ovvero necessario alla cura delle attività, all'esecuzione dei compiti e al perseguimento degli obiettivi propri di ciascuna area o servizio di appartenenza, ovvero affidati dal proprio responsabile con ordine di servizio o altra comunicazione.

Si ricorda che ogni incaricato del trattamento, nel trattare i dati personali, deve rispettare i seguenti principi:

1) principio di finalità: il trattamento deve essere svolto per scopi determinati, espliciti e legittimi.

Con riferimento alla Società, questo limite è ancor più pregnante, considerato che Cinecittà S.p.A. è autorizzato al trattamento finalizzato unicamente al raggiungimento del proprio oggetto sociale.

2) principio di proporzionalità e minimizzazione: i dati oggetto di trattamento, devono essere pertinenti, non eccedenti e completi rispetto agli scopi istituzionali perseguiti. La pertinenza attiene al merito dell'attività di trattamento; la non eccedenza alla quantità dei dati che possono essere raccolti e trattati in riferimento allo scopo perseguito; infine, la completezza attiene alla tutela dell'identità personale dell'interessato, che ha interesse a che il suo profilo e le informazioni detenute non siano parziali. Ove il trattamento riguardi categorie particolari di dati ovvero dati relativi a condanne penali o reati, occorre verificare caso per caso che i dati (di questa specie) siano indispensabili rispetto alla finalità perseguita;

3) principio di sicurezza: i dati oggetto di trattamento devono essere protetti attraverso l'adozione di misure di sicurezza.

Di seguito vengono riportate una serie di regole e di istruzioni, che devono essere osservate da ciascuna persona fisica preposta allo svolgimento delle operazioni di trattamento di dati personali.

ISTRUZIONI PER LO SVOLGIMENTO DELLE OPERAZIONI, CARATTERIZZANTI IL PROCESSO DI TRATTAMENTO:

- **raccolta/profilazione:** prima di procedere alla raccolta dei dati personali, deve essere fornita l'informativa all'interessato o alla persona o ente presso il quale si richiedono e raccolgono i dati personali di una persona fisica. Occorre procedere alla raccolta dei dati con la massima cura, verificandone l'esattezza, nonché la pertinenza, la completezza e la non eccedenza rispetto alle finalità del trattamento, secondo quanto previsto dalla legge o dai regolamenti e le istruzioni del responsabile della struttura;

- **registrazione:** non lasciare cd-Rom, dvd, fogli, cartelle e quant'altro a disposizione di estranei;

- **conservazione**: i documenti o gli atti che contengono categorie particolari di dati (ovvero i dati sensibili) o "giudiziari" devono essere conservati in archivi ad accesso controllato; pertanto, occorre

garantire che armadi, schedari e contenitori siano muniti di serratura ovvero che l'autorizzato del trattamento che riceva cittadini e utenti sia sempre presente nella propria stanza o luogo di lavoro, evitando che le informazioni trattate possano essere visualizzate e rese conoscibili a terzi. Sarà cura di ciascun responsabile del trattamento provvedere affinché venga escluso un accesso ad archivi e a dati da parte di soggetti che non siano autorizzati al trattamento;

- **utilizzo:** i dati possono essere utilizzati solo da coloro che sono stati espressamente autorizzati al trattamento. L'utilizzo dei dati deve avvenire solo per scopi determinati, espressi e legittimi e si deve evitare un utilizzo per scopi diversi rispetto a quello istituzionali dell'ente o non compatibili con gli stessi, con riferimento alle attività affidate e di competenza dell'unità di trattamento di appartenenza;

- **blocco:** questo può essere conseguenza di una espressa richiesta da parte dell'interessato ovvero può essere ordinato dal Garante per la protezione dei dati personali;

- **comunicazione:** con tale espressione, secondo quanto previsto dalla legge, si intende il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione. Ciò che caratterizza l'operazione di comunicazione è il fatto che, considerato il rapporto diretto tra titolare e interessato (ad esempio un cittadino utente, un dipendente), un soggetto determinato (in posizione di terzietà rispetto a questo rapporto bilatero) possa in qualunque forma conoscere dati personali riferiti all'interessato medesimo;

- **comunicazione di dati cd. comuni**: Qualora il richiedente i dati personali sia un soggetto pubblico, la comunicazione dei cd. dati comuni potrà avvenire, pur in mancanza di espressa previsione di legge o di regolamento, ove sia necessaria per l'esercizio di una finalità istituzionale dell'ente destinatario della comunicazione stessa. In tal caso, tuttavia, occorrerà segnalare la circostanza al proprio responsabile, affinché proceda alla comunicazione preventiva al Garante per la protezione dei dati personali;

- **comunicazione di categorie particolari di dati:** Tali dati possono essere comunicati a soggetti determinati solo ove sia espressamente previsto da una legge, che autorizzi tale operazione, in conformità al parere del Garante per la protezione dei dati personali;

- diffusione: per diffusione si intende il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione. La pubblicazione di qualsiasi atto (all'albo pretorio o in una bacheca, ovvero in Internet), che contenga dati personali, costituisce una forma di diffusione di informazioni personali.

- **cancellazione**: L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti: i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; l'interessato revoca il consenso su cui si basa il trattamento e se non sussiste altro fondamento giuridico per il trattamento; l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento; i dati personali sono stati trattati illecitamente; i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione.

Qualora sia richiesta la cancellazione del dato, e sussistano motivi di accoglimento positivo, e qualora sia esaurita la finalità del trattamento, la documentazione deve essere distrutta con modalità che non permettano la ricostruzione e la fruibilità dei dati contenuti nel documento. I dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR.

ISTRUZIONI PER IL CORRETTO UTILIZZO DEGLI STRUMENTI PER IL TRATTAMENTO:

Tutti gli Autorizzati, che a qualunque titolo accedono al sistema informativo aziendale, collegato o meno alla rete o che custodiscono qualsiasi dato personale di competenza dell'azienda e non destinato alla diffusione dovranno attenersi a quanto riportato di seguito.

Utilizzo del personal computer: Il personal computer è assegnato ai dipendenti al momento dell'instaurazione del rapporto di lavoro ed è considerato uno strumento di lavoro.

Qualsiasi utilizzo che avvenga al di fuori di tali finalità, salvi i casi in cui sia stato consentito l'uso promiscuo anche per fini personali, può contribuire a creare disservizi, costi di manutenzione e soprattutto, minacce per la sicurezza informatica.

L'accesso al personal computer è protetto da password, che deve essere custodita dai dipendenti con la massima diligenza. La password, oltre a consentire l'avvio del personal computer, consente anche di accedere alla rete e a tutti i sistemi ed applicazioni aziendali che comportano il trattamento dei dati personali.

Non è consentita l'attivazione della password di accensione (bios) senza preventiva autorizzazione da parte dell'Amministratore di Sistema, cui deve essere data copia in busta chiusa della stessa.

L'Amministratore di Sistema potrà accedere ai dati presenti su ciascun PC esclusivamente al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività aziendale nei casi in cui si renda indispensabile ed indifferibile l'intervento.

Le modalità di accesso ai PC consentite all'Amministratore di Sistema sono le seguenti:

- su richiesta dell'utente: la richiesta di intervento viene effettuata dall'utilizzatore del PC e l'Amministratore di Sistema effettuerà l'intervento alla presenza dell'utente richiedente stesso;

- in assenza di richiesta: ad esempio in caso di prolungata assenza od impedimento dell'Autorizzato, informando tempestivamente l'utente dell'intervento di accesso realizzato.

Il personal computer deve essere spento tutti i giorni prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso deve essere attivato il blocco del personal computer in caso di allontanamento dalla propria postazione di lavoro, al fine di impedire a terzi l'utilizzo dello strumento a titolo indebito.

Gestione ed assegnazione delle credenziali di autenticazione: Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dal Servizio ICT, associato ad una parola chiave (password) riservata che dovrà venir 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 del Servizio ICT.

Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale del Servizio ICT, previa formale richiesta del Responsabile dell'ufficio/area nell'ambito del quale verrà inserito e andrà ad operare il nuovo utente.

È necessario procedere alla modifica della parola chiave a cura dell'utente, autorizzato del trattamento, al primo accesso. La parola chiave è personale e riservata, deve quindi essere mantenuta segreta e custodita.

Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso d'intesa con il personale del Servizio ICT.

Linee guida per la costruzione delle parole chiave: Per garantire il rispetto delle disposizioni di legge, l'Autorizzato dovrà scegliere con cura le parole chiave e, ove possibile, in conformità alle principali *best practices* esistenti. A mero titolo esemplificativo:

- presenza di caratteri appartenenti a 3 delle 4 categorie seguenti: caratteri maiuscoli (A – Z), caratteri minuscoli (a – z), cifre in base 10 (0 – 9), caratteri non alfabetici (ad esempio !, $, #, o %) ;
- non uguaglianza con il profilo utente;
- non facilmente riconducibili all'Autorizzato;
- note SOLO all'Autorizzato, scelte da quest'ultimo al primo accesso al sistema.

Si riportano alcune indicazioni per aiutare nella scelta di password che possono considerarsi sicure:

Parole chiave sicure

Sono da ritenere parole chiave di soddisfacente sicurezza quelle che hanno le seguenti caratteristiche:

- sono composte da caratteri maiuscoli e minuscoli;
- utilizzano anche caratteri di interpunzione, come; [,] , * " , ed una combinazione di numeri e lettere;

- non devono rappresentare una parola in una qualsiasi lingua o dialetto sufficientemente diffuso;

- non devono essere basate su informazioni personali, come nomi di membri della famiglia, date di nascita, anagrammi o combinazione di nomi e simili;

- un altro importante accorgimento riguarda la selezione di parole chiave, che possano essere facilmente digitate sulla tastiera, senza doverla guardare, per ridurre al minimo il tempo di digitazione ed evitare che la digitazione possa essere osservata surrettiziamente da terzi nelle vicinanze.

Parole chiave deboli

Si sottolinea che le parole chiave di facile individuazione hanno le seguenti caratteristiche:

- la parola chiave si può trovare in un comune dizionario italiano, in inglese od altra lingua comune.

- la parola chiave è una parola di uso comune, come ad esempio il nome di qualche membro della famiglia, di animali da salotto, di amici, di collaboratori o di caratteri di fantasia.

- la parola chiave legata a espressioni informatiche, hardware e software, come pure quelle legate a date di nascita od altre informazioni personali, come l'indirizzo, il numero telefonico e simili.

- le sequenze numeriche del tipo aaaaaaaa, bbbb, 121212, 123456, eccetera. Sono da scartare parole come sopra, digitate alla rovescia.

- una qualsiasi delle parole chiave precedentemente indicata come debole, preceduta o seguita da una cifra come ad esempio giovanni1, oppure 1giovanni.

Raccomandazioni per la protezione della parola chiave

- Non utilizzare la stessa parola chiave per sistemi di autenticazione interni all'azienda e per sistemi di autenticazione esterni, come ad esempio l'accesso al proprio conto corrente bancario ed altre attività, non legate all'attività aziendale.

- Non condividere la parola chiave con alcun soggetto, interno o esterno all'azienda, ivi inclusi i superiori, a qualsiasi livello.

Tutte le parole chiave che sono state generate da un Autorizzato devono essere trattate come informazione strettamente riservata.

In particolare, a titolo esemplificativo e non esaustivo, si fornisce un elenco di accorgimenti da adottare:

- non rivelare una parola chiave attraverso il telefono a chicchessia;
- non scrivere la parola chiave su un qualsiasi documento e non nascondetelo in alcuna parte del vostro ufficio;
- non archiviare la parola chiave in un qualsiasi tipo di sistema di elaborazione, incluso un telefono cellulare, un computer palmare e simile;
- non scrivere una parola chiave in un messaggio di posta elettronica;
- non parlare di parole chiave di fronte a terzi;
- non dare alcuna indicazione in merito al formato ed alla lunghezza della parola chiave, che utilizzate;
- non rivelare la parola chiave ad un vostro collega di lavoro, mentre si è assenti;
- non utilizzare mai la caratteristica, offerta da parecchie applicazioni, di memorizzare la parola chiave.

Nel caso di operazioni sistemistiche che richiedano la password (es: cambio del PC o installazione di programmi), i sistemisti o le persone incaricate dal Titolare la cambieranno temporaneamente, dandone comunicazione. Al primo utilizzo del PC è obbligatorio modificare subito la password.

Se qualcuno insiste per conoscere la parola chiave, dapprima fare riferimento a questo documento e successivamente informare immediatamente il Responsabile di riferimento.

Se si ha anche solo il minimo sospetto che la parola chiave sia stata in qualche modo compromessa o venuta a conoscenza di terzi, provvedere immediatamente alla sostituzione della parola chiave e riferire l'accaduto al Responsabile di riferimento.

Nel caso l'utente abbia qualsiasi dubbio afferente alle modalità sicure di generazione, utilizzo e conservazione delle parole chiave, deve rivolgersi quanto prima possibile all'Amministratore di Sistema per ottenere opportuni chiarimenti ed istruzioni.

Sessioni di trattamento incustodite: Si raccomanda di non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento di dati personali, in particolare qualora sia necessario allontanarsi temporaneamente dal posto di lavoro. Si ricorda che la pressione contemporanea dei tasti Ctrl + Alt + Canc attiva la finestra di "Protezione di Windows" dalla quale è possibile premere il pulsante "Blocca computer" per bloccare la stazione di lavoro senza la necessità di uscire dai programmi in uso. Una volta ritornati davanti alla propria postazione, per riprendere l'operatività è necessario seguire le istruzioni a video delle finestre di Windows premendo nuovamente i tasti Ctrl + Alt + Canc e inserendo la propria password.

Si ricorda che, per maggiore sicurezza, su ciascuna postazione di lavoro può essere configurato uno screen saver con password di sblocco che si attiva dopo n. minuti di inattività.

Raccomandazioni per il salvataggio dei dati in rete: È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parole chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

Le cartelle utenti presenti nei server della Società sono aree di condivisione di informazioni strettamente professionali 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 del Servizio ICT.

Il personale del Servizio ICT può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli Autorizzati sia sulle unità di rete.

Risulta opportuno che, con regolare periodicità, 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.

Utilizzo di notebook: i dipendenti possono ricevere in dotazione dall'azienda un notebook per garantire un adeguato svolgimento della propria attività lavorativa.

i dipendenti sono responsabili del notebook e devono custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo sul luogo di lavoro.

Ai notebook si applicano le regole previste per i personal computer connessi alla rete, con particolare riferimento agli accessi dell'amministratore di sistema ed alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

Il notebook utilizzati all'esterno del luogo di lavoro abituale devono essere custoditi in luogo protetto in caso di allontanamento temporaneo.

In caso di furto è necessario che i dipendenti informino tempestivamente l'amministratore di sistema, fornendo quanti più dettagli possibili e consegnando copia della denuncia presentata all'autorità di pubblica sicurezza, che costituisce documento necessario per ricevere un nuovo notebook in dotazione.

Riproduzione dei contenuti su supporti informatici: La riproduzione abusiva di contenuti, ove protetti da copyright, è sanzionata civilmente e penalmente, ed è pertanto fatto divieto a tutto il personale di effettuare la loro duplicazione in qualsiasi forma e su qualsiasi tipo di supporto.

E' ammessa, per motivi attinenti la propria attività lavorativa e con il consenso del responsabile competente, la riproduzione dei soli supporti informatici aziendali (floppy disc o CD), in quanto ciò non rappresenta una violazione di legge.

Raccomandazioni per l'utilizzo di hardware e software: Il software installato in ciascuna macchina nonché la relativa configurazione hardware, rispecchiano la condizione necessaria e sufficiente per il consueto lavoro da svolgersi.

Software e hardware, secondo le autorizzazioni rilasciate, possono essere installati solo dall'Amministratore di Sistema o suoi delegati in possesso di chiavi segrete conosciute solo dal medesimo Amministratore di Sistema.

Qualora si ritenga necessario disporre di un nuovo software o di un aggiornamento hardware per le consuete mansioni, è necessario inoltrare una specifica richiesta al Responsabile dei Sistemi informativi il quale valuterà la stessa in accordo con il Responsabile Privacy di riferimento.

È bene ricordare che ogni software, ad esclusione di quelli denominati freeware, ha una licenza e l'uso improprio di questa può portare a conseguenze civili e penali.

Utilizzo della posta elettronica: La casella di posta elettronica è uno strumento di lavoro configurato dall'Amministratore di Sistema ed assegnato ai dipendenti dell'Azienda al momento dell'assunzione. La stessa deve essere utilizzata esclusivamente per finalità connesse al rapporto di lavoro instaurato.

Non è, pertanto, consentito l'utilizzo della casella di posta elettronica aziendale per motivi non attinenti allo svolgimento della propria attività lavorativa (messaggi relativi a tematiche personali indirizzati a gruppi di persone ovvero a persone singole, partecipazione a dibattiti, etc.).

I dipendenti sono considerati responsabili dei messaggi che inviano, e le eventuali conseguenze negative o dannose derivanti dall'invio di messaggi ed allegati dal contenuto illecito, illegale o immorale, saranno a carico dei dipendenti, ivi comprese le azioni legali di qualsiasi tipo che ne possano derivare.

La casella di posta elettronica deve essere mantenuta in ordine, attraverso la cancellazione di documenti inutili ed allegati ingombranti, soprattutto in relazione alle attività di salvataggio e back up dei dati trattate nei paragrafi successivi.

L'utilizzo della casella di posta elettronica è consentito anche per lo scambio di informazioni e documenti interni.

È fatto obbligo al dipendente di controllare con attenzione i file attachements prima del loro utilizzo e, quindi, di non eseguire download di file eseguibili o di documenti da siti Web o Ftp non conosciuti e non ritenuti sicuri.

Tutti i file contenenti estensioni quali a titolo esemplificativo .exe e .bat non possono essere inviati per posta elettronica e, se ricevuti, devono essere immediatamente cancellati.

L'account di posta elettronica è generalmente definito da n.cognome@cinecitta.it. L'utilizzo all'interno della casella di posta elettronica aziendale dei riferimenti personali dei dipendenti è strumentale ad una più agevole ricostruzione dei diversi indirizzi e-mail dell'azienda; tuttavia la loro personalizzazione non comporta in alcun modo la privatezza degli stessi.

L'azienda, qualora vi siano delle specifiche motivazioni provenienti dai dipendenti, può concedere, attraverso un ragionevole utilizzo del collegamento ad Internet, l'attivazione di una casella di posta elettronica personale attraverso la quale inviare e ricevere comunicazioni di carattere privato, purché ciò avvenga con modalità tali da non influire sulla produttività e sull'efficienza dei dipendenti.

In caso di prolungata assenza o altro impedimento da parte dei dipendenti, l'Azienda si riserva la possibilità di accedere alla casella di posta aziendale dello stesso. L'accesso sarà effettuato solo qualora urgenti necessità operative o connesse alla sicurezza rendano di fatto indifferibile attendere il rientro in sede degli stessi.

L'accesso alla casella elettronica dei dipendenti sarà effettuato a cura dell'Amministratore di Sistema che, al termine delle operazioni, avrà cura di informare i dipendenti attraverso dettagliato rapporto informativo riportante tutte le operazioni svolte. Copia del rapporto sarà inoltre trasmessa all'Ufficio del personale.

Per garantire la disponibilità e l'integrità dei dati aziendali, tutti i messaggi di posta elettronica ricevuti ed inviati attraverso l'account aziendale sono oggetto di periodico back-up ed archiviazione su supporti magnetici. Ciascun dipendente è pertanto tenuto a rimuovere dalle cartelle di posta in entrata e posta in uscita eventuali messaggi e documenti ricevuti o inviati di carattere personale, al fine non occupare spazi di memoria aziendali adibiti al salvataggio di informazioni di carattere lavorativo.

Le caselle di posta elettronica aziendali potranno essere, infine, oggetto di monitoraggio periodico dello spazio occupato sui server di rete. Tale monitoraggio non comporterà in alcun modo l'accesso

alle informazioni archiviate, ma in caso di superamento dei limiti di spazi assegnati o ragionevoli, potrebbe prevedere la richiesta di cancellazione di parte dei messaggi archiviati.

Tali controlli saranno effettuati a cura dell'Amministratore di Sistema.

Navigazione in internet: I personal computer di Cinecittà S.p.A. in dotazione ai dipendenti sono abilitati alla navigazione Internet per finalità legate alle attività lavorative in carico a ciascuno di essi.

È da evitare la navigazione in Internet in modi diversi da quelli strettamente legati all'attività lavorativa, con particolare riferimento alle forme di fruizione di immagini e video previste dalla normativa per la prevenzione dei reati di tipo pedopornografico.

È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, di e-commerce o simili, salvo i casi direttamente autorizzati dalla Direzione per le esigenze dell'Azienda. In deroga a ciò, ed esclusivamente in ambiente Web protetto, è consentita l'effettuazione di operazioni di Home Banking durante la pausa pranzo.

È da evitare qualsiasi registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

È vietata la partecipazione a forum non legati all'attività lavorativa svolta dai dipendenti, l'utilizzo di chat on line, di bacheche elettroniche e le registrazioni a guest books, anche attraverso l'utilizzo di pseudonimi (nick name). È vietata, infine, la partecipazione a social networking (Facebook, MySpace, Orkut, Hi5, etc.), laddove non vi sia una connessione con l'attività lavorativa.

L'azienda dispone attualmente di un sistema, anche mediante antivirus, che prevede un filtro per l'accesso ad alcune categorie di siti Internet. Qualora un dipendente debba accedere per finalità lavorative ad un sito Internet bloccato, potrà richiedere l'assistenza dell'Amministratore di Sistema, i quali, dopo aver positivamente valutato la richiesta, provvederanno ad attivare la connessione alla pagina Web.

L'azienda si riserva la facoltà di monitorare l'utilizzo dello strumento Internet, attraverso l'analisi dei file di log del Proxy Server attualmente in uso e si riserva la facoltà di utilizzare tale strumento quando lo ritenga opportuno. I file di log del Proxy Server vengono cancellati con frequenza mensile (mensile o semestrale).

Raccomandazioni per l'utilizzo dello smartphone: Il telefono mobile viene assegnato dall'azienda al dipendente in relazione all'attività svolta e al ruolo ricoperto. Esso è, pertanto, uno strumento di lavoro in dotazione ai dipendenti.

Il telefono mobile può essere utilizzato dai dipendenti anche a fini "personali", attraverso la digitazione di un prefisso previsto dall'operatore, che dà diritto ad un profilo tariffario maggiormente conveniente. Tale profilo tariffario è attivato dall'Azienda a favore dei dipendenti che hanno in dotazione l'apparecchio di telefonia mobile. Resta inteso che, come per i personal computer e i notebook, per gli apparecchi di telefonica mobile può essere concesso *ad personam* l'uso promiscuo anche per fini personali.

L'azienda si riserva la facoltà di procedere al monitoraggio e alla verifica dell'utilizzo di tale strumento da parte dei dipendenti, attraverso l'acquisizione e la successiva analisi dei tabulati telefonici al fine di verificare i volumi di traffico generati dai dipendenti. I tabulati saranno raccolti, e i dati ivi contenuti saranno trattati, nel rispetto della vigente normativa in materia di dati personali adottando le dovute misure di oscuramento e limiti di durata di conservazione del dato nel rispetto dei principi di finalità e di minimizzazione del trattamento del dato personale per realizzare il legittimo interesse di verifica da parte dell'Ente, anche tenendo conto dei provvedimenti del Garante Privacy adottati in tale fattispecie.

TRATTAMENTI NON AUTOMATIZZATI | GESTIONE QUOTIDIANA PRATICHE

Istruzioni per i dati personali in genere

- Le pratiche contenenti dati personali devono essere di norma riposte in archivi chiusi. Si considera archivio chiuso anche il locale chiuso a chiave;

- le pratiche sono prelevate, a cura degli Autorizzati, solo nella misura e per il tempo strettamente necessari per lo svolgimento dei relativi compiti, al termine dei quali - ed in ogni caso al termine della giornata/settimana lavorativa - sono riposte negli archivi. Ciascun Autorizzato deve aver cura di verificare che le pratiche affidategli non restino incustodite, specie in contesti accessibili a soggetti non Autorizzati del trattamento (aree di passaggio, sale d'attesa, sale riunioni, e via dicendo);

- anche durante la giornata lavorativa, in caso di allontanamento dalla postazione di lavoro per un periodo di tempo significativo, le pratiche sono riposte negli archivi, salvo adeguata garanzia di controllo da parte di altri Autorizzati dei medesimi trattamenti. In ogni caso le pratiche non devono essere mai lasciate incustodite sul tavolo durante il giorno;

- lo smarrimento o il furto di informazioni deve essere comunicato immediatamente al proprio Responsabile di riferimento;

- è buona regola evitare la proliferazione eccessiva di stampe e fotocopie di documenti contenenti dati personali. Le stampe e le fotocopie malriuscite debbono essere distrutte nell' apposito distruggi-documenti, se disponibile, oppure devono essere strappate in pezzi piccoli.

Istruzioni per i dati personali sensibili e giudiziari

Oltre a quanto previsto per i dati personali in genere, le pratiche contenenti dati sensibili o giudiziari sono conservate in archivi ad accesso controllato, sono controllate e custodite dagli Autorizzati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione (ivi compresi altri Autorizzati del trattamento che non siano autorizzati ad accedere alle informazioni sensibili) e sono restituite al termine delle operazioni affidate.

Gestione chiavi: gli Autorizzati chiamati a gestire le chiavi "fisiche" degli archivi devono:

- all'atto della consegna delle chiavi, verificarne subito il corretto funzionamento;

- verificare che le chiavi non restino inserite negli armadi/archivi di riferimento;

- conservare le chiavi in un luogo e con modalità che ne garantiscano una sicurezza adeguata anche al tipo di archivio;

- non metterle a disposizione né, se possibile, mostrarle ad estranei;

- in caso di smarrimento o sottrazione, farne immediata segnalazione al referente e richiedere la sollecita sostituzione della serratura, spostando se del caso, per il tempo necessario, i documenti dall'archivio non protetto.

Scarti di archivio: Gli scarti di archivio, ossia il periodico smaltimento di materiale cartaceo contenente dati personali, deve essere effettuato evitando che le informazioni personali, specie se sensibili, possano essere utilizzate da soggetti non autorizzati.

In particolare, i dati sensibili devono essere smaltiti mediante utilizzo degli appositi strumenti per la distruzione dei documenti, ove disponibili oppure, in assenza di questi ultimi i fogli contenenti dati sensibili devono essere strappati in piccoli pezzi prima di essere cestinati.

fax: questo strumento appare utile a garantire efficienza, economicità e velocità di comunicazione; tuttavia, presenta rischi specifici riguardo all'identità (a volte sconosciuta) di colui che materialmente riceve il documento trasmesso. A tal proposito, prima di inviare documenti contenenti categorie particolari di dati o per i quali vi siano esigenze di riservatezza, assicurarsi preventivamente che l'effettivo destinatario sia sul posto o comunque che non vi siano rischi di conoscenza del contenuto da parte di soggetti non autorizzati. Si consiglia di anticipare telefonicamente la trasmissione e di inserire in calce alla copertina del fax, che viene utilizzata per la spedizione della documentazione allegata, la seguente formula: "Qualora il destinatario del presente fax non sia la persona indicata nella presente copertina, è pregato di dare immediata comunicazione al mittente, a mezzo telefono o per fax. Successivamente, si prega di distruggere la documentazione erroneamente ricevuta, con l'avvertimento che in caso di non ottemperanza a questo invito si potrà essere responsabili della mancanza di protezione o dell'uso non autorizzato delle informazioni erroneamente acquisite".

Istruzioni per l'utilizzo del fax:

- digitare correttamente il numero di telefono, cui inviare la comunicazione;

- controllare l'esattezza del numero digitato prima di inviare il documento;

- verificare che non vi siano inceppamenti della carta ovvero che non vengano

presi più fogli contemporaneamente;

- attendere la stampa del rapporto di trasmissione, verificando la corrispondenza tra il numero di pagine da inviare e quelle effettivamente inviate;

- qualora vengano trasmessi dati idonei a rivelare lo stato di salute, può essere opportuno anticipare l'invio del fax chiamando il destinatario della comunicazione al fine di assicurarsi che il ricevimento avverrà nelle mani del medesimo, evitando che soggetti estranei o non autorizzati, possano conoscere il contenuto della documentazione inviata;

- in alcuni casi, può essere opportuno richiedere una telefonata che confermi da parte del destinatario la circostanza della corretta ricezione e leggibilità del contenuto del fax;

- **telefono**: non fornire dati e informazioni di carattere personale o di natura comunque riservata per telefono, qualora non si conosca o non si abbia verosimilmente cognizione dell'identità o della legittimazione a conoscere del soggetto chiamante. In molti casi, si consiglia di richiedere l'identità del chiamante e la qualità, quindi di provvedere a richiamare, avendo così la certezza sull'identità del richiedente;

- scanner: i soggetti che provvedano all'acquisizione in formato digitale della documentazione cartacea (utilizzando ad esempio uno scanner) devono verificare che l'operazione avvenga correttamente e che il contenuto del documento oggetto di scansione sia correttamente leggibile; qualora vi siano errori di acquisizione ovvero si verifichino anomalie di processo, occorrerà procedere alla ripetizione delle operazioni;

- Pen-Drive: i supporti informatici, già utilizzati per il trattamento dei dati personali di qualunque tipologia, devono essere riutilizzati solo se le informazioni precedentemente contenute non sono più in alcun modo recuperabili, dovendo altrimenti essere distrutti. Tali dispositivi, qualora contengano dati personali, devono essere conservati in contenitori muniti di serratura;

- cd-rom: i supporti informatici, già utilizzati per il trattamento dei dati possono essere riutilizzati solo se le informazioni precedentemente contenute non sono più in alcun modo recuperabili, dovendo altrimenti essere distrutti. Tali dispositivi, qualora contengano dati personali, devono essere conservati in contenitori muniti di serratura;

- **spedizione di documenti contenenti dati personali a mezzo posta**: la documentazione contenente categorie particolari di dati ovvero dati relativi a condanne penali o reati, deve essere trasferita, anche all'interno delle Strutture aziendali, in busta chiusa, in modo da proteggere la riservatezza del

documento e dei dati contenuti. I lembi della busta devono essere sigillati e firmati per garantire l'integrità del contenuto;

ULTERIORI ISTRUZIONI PER I SOGGETTI AUTORIZZATI AL TRATTAMENTO:

Le persone autorizzate devono, altresì, rispettare le istruzioni seguenti in tema di protezione e di sicurezza dei dati e degli strumenti nello svolgimento delle operazioni affidate:

Rapporti di front-office e gestione documenti cartacei:

- identificazione dell'interessato: in alcuni casi può essere necessario dover identificare il soggetto interessato per esigenze di verifica dell'identità della persona e garanzia di correttezza del dato da raccogliere; può essere quindi necessario richiedere e ottenere un documento di identità o di riconoscimento;

- controllo dell'esattezza del dato: fare attenzione alla digitazione ed all'inserimento dei dati identificativi e personali degli interessati, evitando errori di battitura, che potrebbero creare problemi nella gestione dell'anagrafica e nel proseguo del processo;

- obbligo di riservatezza e segretezza: il soggetto autorizzato al trattamento ha l'obbligo della riservatezza e del segreto sulle informazioni, di cui venga a conoscenza nel corso delle operazioni del trattamento e deve evitare la comunicazione o la diffusione delle informazioni a soggetti non autorizzati o che non abbiano necessità di conoscere i dati trattati.

- tenuta cartelle e fascicoli: cartelle e fascicoli tenuti sulla propria scrivania, qualora si ricevano nella propria stanza utenti e cittadini, devono essere trattati in modo da garantire la riservatezza degli interessati. Si consiglia di rivoltare sotto sopra le cartelle ovvero di inserire (a seconda delle necessità operative e organizzativi) sul frontespizio dati e informazioni per cui non sia resa conoscibile a terzi estranei l'identità dei soggetti interessati;

- **data breach:** i dati personali conservati, trasmessi o trattati da aziende e pubbliche amministrazioni possono essere soggetti al rischio di perdita, distruzione o diffusione indebita, ad esempio a seguito di attacchi informatici, accessi abusivi, incidenti o 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.

Per tale ragione il soggetto autorizzato venuto a conoscenza di una violazione o di una perdita del dato personale, anche in occasione di catastrofi naturali, deve senza indugio comunicare al proprio responsabile, se presente, ovvero al titolare del trattamento del dato personale la circostanza ed accertarsi che la problematica venga presa in carico (anche chiedendo una risposta per iscritto da parte del soggetto responsabile del trattamento dei dati personali). In calce al presente documento è stata dettagliata una guida completa da seguire in caso di *Data – Breach.*

conservazione supporti rimovibili: i supporti utilizzati per la memorizzazione di copie di file di documenti di lavoro non devono essere lasciati in luoghi accessibili. Si consiglia di riporre cd-rom, DVD, dispositivi di memorizzazione in cassetti muniti di serratura ovvero di custodire gli stessi in modo da garantire un accesso controllato.

PROCEDURA DA SEGUIRE IN CASO DI DATA BREACH

DEFINIZIONE DATA BREACH

L'art. 33 del GDPR recita che: "*In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'Autorità di controllo competente a norma dell'art. 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'Autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo*".

Per "*Data Breach*" si intende un evento in conseguenza del quale si verifica una "violazione dei dati personali". Nello specifico, l'articolo 4 p.12 del GPDR definisce la violazione dei dati personali come violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Le Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) - WP250, definite in base alle previsioni del Regolamento (UE) 2016/679 precisano la nozione di violazione come di seguito riportata:

Nel parere 03/2014 sulla notifica delle violazioni, il Gruppo di lavoro ha spiegato che le violazioni possono essere classificate in base ai seguenti tre principi ben noti della sicurezza delle informazioni14:

• "*violazione della riservatezza*", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;

• "*violazione dell'integrità*", in caso di modifica non autorizzata o accidentale dei dati personali;

• "*violazione della disponibilità*", in caso di perdita, accesso distruzione accidentali o non autorizzati di dati personali. Va altresì osservato che, a seconda dei casi, una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse. Ci si potrebbe chiedere se una perdita temporanea della disponibilità dei dati personali costituisca una violazione e, in tal caso, se si tratti di una violazione che richiede la notifica.

L'articolo 32 del regolamento ("*Sicurezza del trattamento*") spiega che nell'attuare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, si dovrebbe prendere in considerazione, tra le altre cose, "*la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento*" e "*la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico*". Di conseguenza, un incidente di sicurezza che determina l'indisponibilità dei dati personali per un certo periodo di tempo costituisce una violazione, in quanto la mancanza di accesso ai dati può avere un impatto significativo sui diritti e sulle libertà delle persone fisiche. Va precisato che l'indisponibilità dei dati personali dovuta allo svolgimento di un intervento di manutenzione programmata del sistema non costituisce una "*violazione della sicurezza*" ai sensi dell'articolo 4, punto 12 del GDPR.

Si consiglia di consegnare questo documento a tutti gli operatori che, a qualunque titolo, siano stati autorizzati al trattamento dei dati personali. Per una più corretta diffusione della guida, si raccomanda di affiggere all'interno della bacheca della sede istituzionale e operativa della società.

PROCESSO DI NOTIFICAZIONE DATA BREACH

Prima che si verifichi un incidente di sicurezza occorre predisporre le procedure, gli strumenti e l'organizzazione per gestire l'evento fortuito al meglio.

GESTIONE DELL'EVENTO

In caso di accertamento di violazione che rientra nella definizione di *Data Breach*, sarà opportuno seguire i seguenti *step* del processo di notificazione:

- Acquisizione della notizia da parte dei soggetti preposti al ricevimento/raccolta della violazione (Titolare del Trattamento, Responsabile del Trattamento ovvero DPO) che provvederanno ad attivare i passi successivi;
- Analisi tecnica dell'evento;
- Contenimento del danno;
- Valutazione della gravità dell'evento;
- Notifica al Garante Privacy;
- Altre segnalazioni dovute;
- Comunicazione agli interessati, dove necessario;
- Inserimento dell'evento nel Registro delle Violazioni;
- Azioni correttive specifiche e per analogia.

ACQUISIZIONE DELLA NOTIZIA

La segnalazione di un *Data Breach* può essere interna o esterna all'Ente.

- **INTERNAMENTE:**

- Da personale dipendente;

- Da personale convenzionato/stagisti/tirocinanti, ecc.

● **ESTERNAMENTE**

- Da parte degli organi Pubblici (Agid, Polizia, altre Forze dell'Ordine, giornalisti, ecc.)
- Da parte del DPO
- Da parte dei Responsabili esterni del trattamento
- Da parte degli interessati
- Da parte di ulteriori soggetti.

La segnalazione deve essere inoltrata al DPO mediante:

- Posta elettronica;
- Avvertimento verbale/telefonico in ogni caso.

Dal momento in cui i soggetti preposti predetti, vengono a conoscenza dell'evento, decorre il termine delle 72 ore previsto dalla normativa per l'invio della notifica all'Autorità di controllo.

Tale termine è ridotto a 48 ore nel caso in cui i trattamenti oggetto dell'evento rientrino in quelli previsti dalle misure di sicurezza e modalità di scambio dei dati personali tra Amministrazioni Pubbliche.

ANALISI TECNICA DELL'EVENTO

I riceventi, dopo un'analisi preliminare, attivano il Gruppo di Gestione composto dal Titolare, dal Responsabile del Trattamento e dal *Data Protection Officer*, sotto la supervisione del Coordinatore del Gruppo Privacy.

Il Gruppo che gestisce gli incidenti è responsabile, sulla base delle rispettive competenze, in base alla tipologia della violazione, dell'analisi tecnica dell'evento, delle azioni da mettere in atto tempestivamente per il contenimento del danno.

In particolare, una volta verificato che l'evento segnalato si configuri effettivamente come un "*Data Breach*" (Analisi Preliminare), verranno svolte tutte le operazioni necessarie a raccogliere gli elementi per una valutazione dell'evento (Analisi Approfondita) ai fini della notifica al Garante della Privacy. È importante sottolineare che, anche nel caso in cui

dall'Analisi Preliminare emerga che la segnalazione non ha i caratteri del *Data Breach*, è necessario registrarla nel Registro delle Violazioni.

Durante l'Analisi Approfondita, dovranno essere accertate le circostanze della violazione, le conseguenze e i relativi rimedi. Si precisa che l'art. 33 paragrafo n. 4 del DGPR recita "*Qualora nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo*".

Pertanto, sarà fondamentale raccogliere il maggior numero di informazioni e, anche in caso queste non siano per il momento ritenute esaustive, effettuare la notificazione.

Nello specifico verrà effettuato, in un tempo consigliabile non superiore a 8 – 10 ore:

- Il riconoscimento della categoria della violazione (se di riservatezza, di integrità o di disponibilità) o altro evento (cfr. Linee Guida sulla notifica delle Violazioni dei dati personali ai sensi del Regolamento UE 2016/79 WP 250 Par. 1 . punto 2)
- L'identificazione dei dati violati/distrutti/compromessi e relativi trattamenti; - L'identificazione degli interessati;
- Il contenimento del danno come di seguito descritto:

• Limitazione degli effetti dell'incidente,
• Raccolta delle prove forensi nel caso sia ipotizzato un reato,
• Determinazione delle azioni possibili di ripristino,
• Valutazione delle eventuali vulnerabilità collegate con l'incidente,
• Individuazione delle azioni di mitigazione delle vulnerabilità individuate,
• Valutazione dei tempi di ripristino,
• Ripristino dei dati, dei sistemi, dell'infrastruttura e delle configurazioni,
• Verifica dei sistemi recuperati.

Tutte le operazioni effettuate devono essere tracciate e riconducibili al personale interno e/o collaboratore.

VALUTAZIONE DELLA GRAVITÀ DELL'EVENTO

Il Gruppo di loro sopra individuato dovrà appurare se l'evento merita di essere notificato al Garante della Privacy e con quali modalità (notifica unica o per fasi).

Insieme ai soggetti interni di ausilio alla fase di analisi tecnica, si dovrà:

- Accertare la probabilità o meno che l'evento abbia comportato dei rischi per i diritti e la libertà delle persone (cioè quando si è verificato una distruzione, perdita, modifica, divulgazione non autorizzata o accesso ai dati personali trasmessi, conservati o comunque trattati, sia che questi dati siano trattati all'interno che all'esterno);
- Effettuare la notifica al Garante, se necessaria;
- Verificare, successivamente, se sia necessaria una seconda notifica più approfondita, di conseguenza ad una analisi tecnica supplementare;
- Effettuare una comunicazione all'Autorità giudiziaria competente, se necessaria.

L'art. 33 paragrafo n. 1 chiarisce che non vi è obbligo di notifica della violazione quando è "**improbabile**" che questa comporti un rischio per i diritti e le libertà delle persone fisiche, ovviamente il giudizio che determina l'improbabilità del rischio deve essere riportato nel Registro delle Violazioni.

A questo proposito, i Garanti europei nelle loro linee guida, precisano che la mancata comunicazione può essere sanzionata ma che nessuna sanzione è prevista nel caso di comunicazione incompleta o di comunicazione non necessaria.

Nella fase di Valutazione, sulla base delle informazioni predisposte in fase di Pianificazione, occorre innanzitutto stabilire se nell'incidente sono coinvolti i dati personali.

In caso di risposta positiva occorre valutare l'impatto sugli interessati.

Se si tratta di una violazione di riservatezza occorre verificare che le misure di sicurezza (es.: cifratura dei dati) in vigore rendano improbabile l'identificazione degli interessati (non compromissione della chiave, algoritmo di cifratura o impronta senza vulnerabilità note).

In caso di perdita di integrità o disponibilità di dati occorre valutare se è possibile il recupero degli stessi in tempi compatibili con i diritti degli interessati.

Se in tale modo i rischi per gli interessati sono trascurabili, la procedura può terminare, dopo aver documentato il processo e le scelte operate: le misure messe in atto sono state adeguate alla minaccia.

La fase di Miglioramento può essere innescata per incrementare ulteriormente la protezione del dato, ma non è obbligatoria.

Nel caso che i rischi per l'interessato non siano trascurabili occorre procedere come di seguito:

1. Si ha il dovere di notificare al Garante, questo può presentarsi in 3 sottocasi:

a. L'organizzazione è Titolare del/i trattamenti dei dati coinvolti nell'incidente

b. L'organizzazione è contitolare del trattamento con delega alla notifica

c. L'organizzazione è Responsabile del trattamento con delega alla notifica.

2. L'organizzazione non ha nemmeno potenzialmente il dovere di notificare all'Autorità Garante: questo quando agisce come Responsabile del trattamento per conto di altro Titolare, senza delega alla notifica al Garante.

Nella seconda ipotesi l'ente deve comunicare al Titolare la sospetta violazione e/o l'incidente di sicurezza riguardante dati personali al Titolare stesso nei modi convenuti con la massima tempestività e mettersi a disposizione di quest'ultimo per approfondimenti e contenimento dei danni.

Nella prima ipotesi occorre valutare, seguendo le indicazioni dei documenti sopracitati, se il rischio per gli interessati è probabile.

In questa fase come prima indicazione occorre assumere come rischio il massimo risultante dall'analisi fatta in fase di Pianificazione.

Qualora i contorni della compromissione non siano chiari si può attendere fino ad un massimo di 72 ore prima di effettuare una notifica. Alla scadenza delle 72 ore è opportuno fare una comunicazione significando che questa è l'inizio di una notifica in fasi. Si può valutare di fare una notifica cumulativa se una stessa compromissione ha riguardato la stessa tipologia di dati con le stesse modalità. Per completare la comunicazione, se temporalmente fattibile, occorre individuare: • Le misure di contenimento adottate

- Il numero anche approssimativo di interessati
- Il periodo di violazione
- Se si ritiene di informare o meno gli interessati e le relative motivazioni
- Le misure di contenimento del danno da suggerire agli interessati
- Il carattere transfrontaliero e la nazionalità degli interessati o meno
- Le azioni di miglioramento intraprese.

NOTIFICA AL GARANTE DELLA PRIVACY

Come accennato, la notifica di una violazione al Garante è resa obbligatoria dall'art. 33 del GDPR nei casi in cui si verifichi una violazione dei dati personali, a meno che sia improbabile che tale violazione presenti un rischio per i diritti e le libertà delle persone fisiche. La notifica, effettuata dal Referente Ufficio Privacy, sulla base del Modello reso disponibile dal Garante della privacy (allegato C) dovrà contenere i seguenti elementi:

- La descrizione della violazione dei dati personali compresi, ove possibile le categorie e il numero approssimativo di interessati in questione nonché le categorie ed il numero approssimativo di registrazioni dei dati personali in questione;
- L'indicazione del nome ed i relativi dati di contatto del DPO;
- La descrizione delle probabili conseguenze della violazione;
- L'indicazione delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e che, se del caso, per attenuare i possibili effetti negativi;
- Nello specifico, la notifica al Garante sarà effettuata dal Titolare tramite PEC e per conoscenza al DPO, con indicazione del DPO come punto di contatto con il Garante.

Se l'estensione della compromissione è chiara e non si sono verificati episodi analoghi si deve procedere alla notifica all'Autorità. I contenuti della notifica sono specificati dal GDPR e dai documenti citati.

COMUNICAZIONE AGLI INTERESSATI

In caso di elevato rischio per la libertà e i diritti degli individui, si provvederà ad informare gli interessati sul fatto avvenuto, sui dati violati e sulle procedure necessarie a ridurre il rischio. La comunicazione agli interessati, secondo quanto previsto dal paragrafo n. 3 dell'art. 34 del GDPR, non è richiesta quando:

- il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

- il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1; - la comunicazione richiederebbe sforzi sproporzionati.

In tal caso, si procede invece ad una comunicazione pubblica o a una misurazione simile, tramite la quale gli interessati sono informati con analoga efficacia.

La comunicazione deve contenere, ai sensi dell'art. 34, le seguenti informazioni:

- il nome e i dati di contatto del RPD o di altro punto di contatto;

- la descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi. A valle della decisione di notificare l'Autorità Garante, occorre valutare se è il caso di notificare anche gli interessati.

A tale scopo va valutata la gravità del rischio per gli interessati e i loro diritti. Se il rischio è grave occorre individuare:

- La fattibilità di contattarli singolarmente oppure la necessità di procedere con pubblicazioni su diversi mezzi di comunicazione (sito web, quotidiani, radio, tv)
- le misure di contenimento che gli stessi interessati possano mettere in atto per minimizzare i rischi
- Le forme di comunicazione più comprensibili per gli interessati (mezzi, lingue, linguaggio) come indicato nelle Linee guida elaborate dal Gruppo Art. 29 in materia di trasparenza (WP 260), definite in base alle previsioni del Regolamento (UE) 2016/679. Anche di queste fasi deve essere prodotta e conservata appropriata documentazione.

INSERIMENTO DELL'EVENTO NEL REGISTRO DELLE VIOLAZIONI

L'art. 33 paragrafo n. 5 del DGPR, prescrive al Titolare di documentare qualsiasi violazione dei dati personali, al fine di consentire all'Autorità di controllo di verificare il rispetto della norma. Pertanto, il Gruppo Ricezione *Data Breach* è Responsabile dell'inserimento di tutte le attività indicate sopra nel registro delle violazioni, che devono essere documentate, tracciabili, e in grado di fornire evidenza nelle sedi competenti. Tale procedura deve essere

diffusa a tutti i soggetti deputati al trattamento dei dati personali che, a diverso titolo, potranno e dovranno essere di ausilio al Titolare del trattamento.

MIGLIORAMENTO

Le azioni previste in questa fase sono:

- Analisi della relazione dettagliata sull'incidente
- Reiterazione del processo di Gestione del rischio informativo
- Eventuale revisione di questo documento (se necessaria) e di eventuali altri documenti collegati (es. Analisi del rischio, Misure di sicurezza)
- Individuazione di controlli che diminuiscano la probabilità dell'incidente o i relativi impatti sul sistema colpito e su sistemi analoghi
- Revisione del Sistema di Gestione della Privacy
- Eventuale revisione annuale della procedura.

SEGNALAZIONE DATA BREACH

MODELLO DI NOTIFICA DATA BREACH AL GARANTE PRIVACY

1. Titolare che effettua la comunicazione:

a. Denominazione o ragione sociale

b. Sede del Titolare

c. Persona fisica addetta alla comunicazione

d. Funzione rivestita

e. Indirizzo e-mail per eventuali comunicazioni

f. Recapito telefonico pe eventuali comunicazioni

2. Natura della comunicazione:

a. Nuova comunicazione (inserire contatti per eventuali chiarimenti, se diversi da quelli sub 1.)

b. Seguito di precedente comunicazione (inserire numero di riferimento)

b1. Inserimento ulteriori informazioni sulla precedente comunicazione

b2. Ritiro precedente comunicazione (inserire le ragioni del ritiro)

3. Denominazione della/e banca/banche dati oggetto di Data Breach e breve descrizione della violazione di dati personali ivi trattati.

_____

_____

_____

_____

_____

4. Quando si è verificata la violazione di dati personali?

a. il……

b. tra il……..e il……..

c. in un tempo non ancora determinato

d. È possibile che sia ancora in corso

5. Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smaltimento di dispositivi o di supporti portatili).

_____

_____

_____

_____

_____

6. Modalità di esposizione al rischio:

a. tipo di violazione:

a.1. lettura (presumibilmente i dati non sono stati copiati)

a.2. copia (i dati sono ancora presenti sui sistemi del Titolare)

a.3. alterazione (i dati sono presenti sui sistemi ma sono stati alterati)

a.4. cancellazione (i dati non sono più sui sistemi del Titolare e non li ha neppure l'autore della violazione)

a.5. furto (i dati non sono più sul sistema del Titolare e li ha l'autore della violazione)

a.6. altro (specificare)

b. dispositivo oggetto della violazione:

b.1. computer

b.2. dispositivo mobile

b.3. documento cartaceo

b.4. file o parte di un file

b.5. strumento di backup

b.6. rete

b.7. altro (specificare)

7. Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione.

_____

_____

_____

_____

_____

8. Quante persone sono state colpite dalla violazione di dati personali?

a. (numero esatto) persone

b. circa (numero) persone

c. un numero (ancora) sconosciuto di persone

9. Che tipo di dati sono coinvolti nella violazione?

a. Dati anagrafici

b. Numeri di telefono

c. Indirizzi di posta elettronica

d. Dati di accesso e di identificazione (username, password, customer ID, altro)

f. Altri dati personali (sesso, data di nascita/età,…) dati sensibili e giudiziari

g. Ancora sconosciuto

h. Altro (specificare)

10. Livello di gravità della violazione di dati personali (secondo le valutazioni del Titolare):

a. Basso/trascurabile

b. Medio

c. Alto

d. Molto alto

11. Misure tecniche e organizzative applicate ai dati colpiti dalla violazione.

_____

_____

_____

_____

_____

12. La violazione è stata comunicata anche alle persone interessate?

a. Sì, e stata comunicate il…..

b. No, perché (specificare)

13. Qual è il contenuto della comunicazione alle persone interessate?(riportare il testo della comunicazione)

_____

_____

_____

_____

_____

14. Quale canale è utilizzato per la comunicazione alle altre persone interessate?

_____

_____

_____

_____

_____

15. Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?

_____

_____

_____

_____

_____

16. La violazione coinvolge contraenti (o altre persone interessate) che si trovano in altri Paesi EU?

_____

_____

_____

_____

_____

17. La comunicazione è stata effettuata alle competenti Autorità di altri Paesi EU?

a. No

b. Sì (specificare)

APPENDICE COVID-19

Con il "Protocollo condiviso di regolazione delle misure per il contrasto e il contenimento della diffusione del virus Covid-19 negli ambienti di lavoro" stipulato in data 14.03.2020 sottoscritto su invito del Presidente del Consiglio dei ministri, del Ministro dell'economia, del Ministro del lavoro e delle politiche sociali, del Ministro dello sviluppo economico e del Ministro della salute, di concerto con le parti sociali e le rappresentanze datoriali si è inteso formulare delle linee guida condivise tra le Parti per agevolare le imprese nell'adozione di protocolli di sicurezza anti-contagio, ovverosia Protocollo di regolamentazione per il contrasto e il contenimento della diffusione del virus COVID 19 negli ambienti di lavoro.
La prosecuzione delle attività produttive dovrà nei fatti avvenire solo in presenza di condizioni che assicurino alle persone che lavorano adeguati livelli di protezione.

Cinecittà S.p.A. in ottemperanza a tale protocollo ha inteso diffondere una corretta informazione, attraverso le modalità più idonee ed efficaci, informando tutti i lavoratori e chiunque entri in azienda circa le disposizioni delle Autorità, consegnando e/o affiggendo all'ingresso e nei luoghi maggiormente visibili dei locali aziendali, appositi depliants informativi al cui interno è rappresentato quanto segue:

- l'obbligo di rimanere al proprio domicilio in presenza di febbre (oltre 37.5°) o altri sintomi influenzali e di chiamare il proprio medico di famiglia e l'autorità sanitaria o la consapevolezza e l'accettazione del fatto di non poter fare ingresso o di poter permanere in azienda e di doverlo dichiarare tempestivamente laddove, anche successivamente all'ingresso, sussistano le condizioni di pericolo (sintomi di influenza, temperatura, provenienza da zone a rischio o contatto con persone positive al virus nei 14 giorni precedenti, etc) in cui i provvedimenti dell'Autorità impongono di informare il medico di famiglia e l'Autorità sanitaria e di rimanere al proprio domicilio;

- l'impegno a rispettare tutte le disposizioni delle Autorità e del datore di lavoro nel fare accesso in azienda (in particolare, mantenere la distanza di sicurezza, osservare le regole di igiene delle mani e tenere comportamenti corretti sul piano dell'igiene);
- l'impegno a informare tempestivamente e responsabilmente il datore di lavoro della presenza di qualsiasi sintomo influenzale durante l'espletamento della prestazione lavorativa, avendo cura di rimanere ad adeguata distanza dalle persone presenti.

In tal senso sino al termine dell'emergenza epidemiologica il personale, prima dell'accesso al luogo di lavoro potrà essere sottoposto al controllo della temperatura corporea. Se tale temperatura risulterà superiore ai 37,5°, non sarà consentito l'accesso ai luoghi di lavoro. Le persone in tale condizione – nel rispetto delle indicazioni riportate in nota – saranno momentaneamente isolate e fornite di mascherine non dovranno recarsi al Pronto Soccorso e/o nelle infermerie di sede, ma dovranno contattare nel più breve tempo possibile il proprio medico curante e seguire le sue indicazioni.

Cinecittà S.p.A. provvederà ad informare preventivamente il personale, e chi intende fare ingresso in azienda, della preclusione dell'accesso a chi, negli ultimi 14 giorni, abbia avuto contatti con soggetti risultati positivi al COVID-19 o provenga da zone a rischio secondo le indicazioni dell'OMS.

La rilevazione in tempo reale della temperatura corporea costituisce un trattamento di dati personali e, pertanto, deve avvenire ai sensi della disciplina privacy vigente. A tal fine non verrà registrato alcun dato in merito alla temperatura corporea se non in casi di sospetto contagio al fine di comunicare la circostanza all'interessato, per poter permettere allo stesso le comunicazioni al proprio medico curante.

Cinecittà S.p.A. ha predisposto l'informativa sul trattamento dei dati personali personali con riferimento alla finalità del trattamento di prevenzione dal contagio da COVID-19 avente quale base giuridica l'implementazione dei protocolli di sicurezza anti-contagio ai sensi dell'art. art. 1, n. 7, lett. d) del DPCM 11 marzo 2020 e quale termine dell'eventuale conservazione dei dati si intenderà quello di cessazione dell'emergenza.

Sotto il profilo organizzativo, all'interno dell'informativa sono stati individuati i soggetti preposti al trattamento e fornite loro le istruzioni necessarie. A tal fine, si ricorda che i dati possono essere trattati esclusivamente per finalità di prevenzione dal contagio da COVID-19 e non devono essere diffusi o comunicati a terzi al di fuori delle specifiche previsioni normative (es. in caso di richiesta da parte dell'Autorità sanitaria per la ricostruzione della filiera degli eventuali "*contatti stretti di un lavoratore risultato positivo al COVID-19*").

In caso di isolamento momentaneo dovuto al superamento della soglia di temperatura, verranno assicurate modalità tali da garantire la riservatezza e la dignità del lavoratore. Tali garanzie saranno assicurate anche nel caso in cui il lavoratore comunichi all'ufficio responsabile del personale di aver avuto, al di fuori del contesto aziendale, contatti con soggetti risultati positivi al COVID-19 e nel caso di allontanamento del lavoratore che durante l'attività lavorativa sviluppi febbre e sintomi di infezione respiratoria e dei suoi colleghi.

Qualora si richieda il rilascio di una dichiarazione attestante la non provenienza dalle zone a rischio epidemiologico e l'assenza di contatti, negli ultimi 14 giorni, con soggetti risultati positivi al COVID-19, si provvederà a raccogliere i soli dati necessari, adeguati e pertinenti rispetto alla prevenzione del contagio da COVID-19, astenendosi nell'indicare i nominativi dei contatti risultati positivi al virus risultate positive al COVID-19 ed astenendosi nello specificare i luoghi di provenienza.