POLICY GESTIONE STRUMENTI INFORMATICI

Il regolamento sull'uso degli strumenti informatici aziendali ha lo scopo di dettare la procedura per una corretta e adeguata gestione delle informazioni, e ciò in ossequio alle raccomandazioni del Garante per la protezione dei dati personali, nonché alle previsioni di cui al GDPR 2016/679.
In ogni caso, nell'utilizzare gli strumenti informatici messi a disposizione dall'azienda il dipendente e/o collaboratore è tenuto ad usare la massima diligenza, nel rispetto degli obblighi di cui agli articoli 2104 e 2105 c.c., utilizzandoli esclusivamente per ragioni di servizio e, comunque, limitatamente all'esecuzione dei compiti, delle mansioni e degli incarichi affidati.
Comportamenti difformi possono causare gravi rischi alla sicurezza ed all'integrità dei sistemi aziendali e possono essere oggetto di valutazione da un punto di vista disciplinare, anche ai sensi e per gli effetti dell'art. 7, L. 300/70 e della sezione disciplinare del CCNL categoriale, oltre che da un punto di vista penale.
A fronte di quanto sopra, Nova Group S.r.l. si impegna a fornire a tutti i soggetti autorizzati a trattare e, comunque, impegnati a qualsiasi tiolo nei processi aziendali, un'adeguata e continuativa formazione in merito ai rischi e alle problematiche relative alla sicurezza in materia di trattamento dei dati tramite l'utilizzo degli strumenti informatici.
Ogni dipendente e/o collaboratore è tenuto a rispettare il presente regolamento sull'uso degli strumenti informatici aziendali, senza che risultino installati e/o configurati sui sistemi informatici in uso agli utenti apparati hardware o strumenti software aventi come scopo il controllo a distanza dell'attività dei lavoratori.

1. Riferimenti normativi

a. Legge 300/70 (art. 4): secondo cui la regolamentazione dell'uso degli strumenti informatici non è finalizzata all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro ma solo a permettere a quest'ultimo di utilizzare sistemi informativi per fare fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali;
b. Regolamento Europeo 2016/679 (GDPR): garantisce al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli articoli 15-16-17-18-20-21-77;
c. "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007;
d. D.lgs. n. 151/2015 (art. 23, recante *"Modifiche all'articolo 4 della legge 20 maggio 1970, n. 300 e all'articolo 171 del decreto legislativo 30 giugno 2003, n. 196"*): rimodulazione della fattispecie integrante il divieto dei controlli a distanza, nella consapevolezza di dover tener conto, nell'attuale contesto produttivo, oltre agli impianti audiovisivi, anche degli altri strumenti «dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori» e di quelli «utilizzati dal lavoratore per rendere la prestazione lavorativa».

2. Definizione di strumenti informatici e di lavoro

Gli strumenti informatici affidati ai dipendenti, compreso il PC, sono strumenti di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Tutti gli strumenti informatici aziendali affidati ai dipendenti, compresi laptop/tablet/pc/smartphone sono di proprietà dell'ente e sono strumenti di lavoro che devono essere utilizzati esclusivamente per rendere la prestazione lavorativa e/o di collaborazione. Ogni utilizzo per fini privati o comunque estranei all'attività lavorativa, infatti, può minacciare la sicurezza dell'ente, provocare disservizi e generare costi (di manutenzione e ripristino o relativi a sanzioni amministrative laddove si verificasse un *data breach*).

3. Divieto di installazione

Non è consentito installare autonomamente programmi provenienti dall'esterno salva specifica autorizzazione esplicita dell'amministratore di sistema, in quanto sussiste il grave pericolo di portare virus e di creare rischi seri per la sicurezza informatica.

4. Divieto utilizzo programmi non autorizzati

Non è consentito l'utilizzo di programmi diversi da quelli distribuiti ed installati ufficialmente dal responsabile dei sistemi informatici. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'azienda a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software.

5. Divieto modifica impostazioni

Non è consentito modificare le caratteristiche impostate sul proprio PC, salva specifica autorizzazione dell'amministratore di sistema. Il personal computer, inoltre, deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio.

6. Divieto installazione dispositivi esterni

Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc…), se non con l'autorizzazione espressa dell'amministratore di sistema. Per quanto riguarda l'utilizzo dei PC e, comunque, degli strumenti aziendali di natura informatica è assolutamente vietato introdurre devices esterni, e ciò anche al fine di scongiurare l'intrusione di qualsivoglia virus/malware.

7. Accesso ai *devices*

L'accesso agli strumenti è protetto da password; per l'accesso devono essere utilizzati Username e password assegnate. L'utente è tenuto a conservarli nella massima segretezza. Una volta autenticati al sistema è vietato lasciare incustodita e accessibile la propria postazione, con assoluto divieto di utilizzare credenziali altrui.

8. Gestione delle password

Per quanto riguarda la gestione della Password di accesso alla postazione è necessario attenersi alle seguenti norme:

- deve essere custodita con la massima attenzione e riservatezza;
- non deve essere comunicata a terzi in alcuna circostanza;
- non deve essere scritta su supporti facilmente accessibili (post-it, blocco appunti, ecc.). Qualora si desideri mantenerne una traccia scritta, per propria memoria, essa deve essere conservata in luogo sicuro;
- deve essere cambiata almeno ogni 3 mesi per i dati sensibili, ogni 6 mesi per i dati comuni;
- deve avere una lunghezza minima di 8 caratteri;
- deve includere una combinazione di caratteri alfabetici e numerici e contenere almeno una lettera e un numero.;
- non deve contenere più di due caratteri consecutivi identici (es: aaaaa…);
- non deve includere sequenze numeriche consecutive (es: 12345…);
- non deve essere legata al nome dell'utente, oppure alla sua user-id, o in generale a parole a lui riconducibili (nome della moglie o dei figli, luogo e data di nascita);
- non deve includere parole di uso comune (nomi di luoghi, personaggi, mesi, giorni della settimana, ecc.);
- non deve essere uguale ad una delle ultime 5 già utilizzate.

9. Procedura di logout e account

Al fine di prevenire l'uso improprio della posta elettronica e, comunque, di ogni e qualsivoglia account aziendale sarà implementata l'adozione di sistemi di risposta automatica in caso di assenze programmate. Alla cessazione del rapporto di lavoro e/o di collaborazione, la casella di posta elettronica dell'ex dipendente e/o collaboratore sarà disattivata, con implementazione di sistema che generi un messaggio automatico informando che l'indirizzo mail non è più operativo.

In ogni caso, gli account aziendali, alla cessazione dei rapporti di lavoro e/o di collaborazione saranno cancellati, e ciò in proporzione alle finalità dei servizi di posta elettronica rispetto ai requisiti minimi di sicurezza.

Gli operatori tutti, alla fine del turno di lavoro e/o delle singole prestazioni, sono obbligati ad effettuare il log-out dai propri account, con cancellazione giornaliera dei dati tutti di navigazione; in mancanza sarà

valutata la condotta sotto il profilo disciplinare.

10. Utilizzo esclusivo delle postazioni e delle apparecchiature

Tutte le postazioni ed i devices affidati al personale diretto e/o indiretto per lo svolgimento delle attività lavorative e/o di collaborazione sono ad uso esclusivo. Ogni eventuale violazione dovrà essere segnalata alla direzione aziendale e, comunque, valutata in termini di natura disciplinare.

11. Limiti di navigazione

La navigazione su internet è limitata, mediante appositi filtri, con selezione di *white list*, ai soli scopi professionali, con espresso divieto di accedere a contenuti inopportuni, violenti, discriminatori.

12. Stampanti e fotocopiatrici

L'utilizzo di stampanti e fotocopiatrici può essere fonte di rischio; pertanto, fermo quanto previsto in tema di *paperless* e organizzazione *green*, il personale può stampare/fotocopiare documenti e atti solo se strettamente necessari per lo svolgimento delle proprie funzioni lavorative e monitorando l'apparecchio. Non si devono lasciare incustoditi documenti contenenti dati riservati o informazioni aziendali.

13. Posta elettronica

La casella di posta elettronica, al pari di tutti i *devices* forniti dall'ente, è strumento di lavoro e deve essere utilizzata esclusivamente per scopi lavorativi. Ogni utente è responsabile del corretto utilizzo e manutenzione della casella di posta a lui assegnata.

Le caselle di posta elettronica nominative, sono comunque di proprietà aziendale e messe a disposizione del personale al fine di rendere la prestazione lavorativa.

Non si devono aprire i messaggi che appaiono palesemente come spam e occorre cancellarli tempestivamente dalla inbox.

Tutti gli allegati devono essere controllati e scansionati prima di essere scaricati.

L'iscrizione, con l'indirizzo di posta assegnato, a newsletter estranee all'ente può essere esplicitamente consentito solo per scopi professionali; resta fermo che si deve evitare di diffondere il proprio indirizzo e-mail aziendale attraverso siti, social network, forum, chat, o quanto altro non attinente all'attività lavorativa.

È vietato l'inoltro automatico di e-mail ad un indirizzo e-mail privato, anche nei periodi di assenza del personale; all'uopo sarà impostata una risposta automatica con i recapiti alternativi da contattare in caso di necessità.

Nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali o dati personali particolari è obbligatorio che questi allegati vengano preventivamente resi illeggibili attraverso la criptografia con apposito software (archiviazione e compressione con password). La password di cifratura deve essere comunicata al destinatario attraverso un canale diverso dalla mail (ad esempio per lettera o per telefono) e mai assieme ai dati criptati. Tutte le informazioni, i dati personali e/o sensibili di competenza possono essere inviati soltanto a destinatari – persone o Enti – qualificati e competenti.

In caso di assenza improvvisa o prolungata di un dipendente e per improrogabili necessità legate all'attività lavorativa il titolare della casella di posta elettronica ha l'onere di designare un altro dipendente (fiduciario) per verificare il contenuto di messaggi e per inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.

Tuttavia, in caso di assenza improvvisa o prolungata del dipendente ovvero per imprescindibili esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale ovvero per motivi di sicurezza del sistema informatico, l'azienda per il tramite dell'amministratore di sistema potrà accedere all'account di posta elettronica, prendendo visione dei messaggi, salvando o cancellando file.

In caso di cessazione del rapporto lavorativo, la mail affidata all'incaricato verrà disattivata immediatamente. Potrà, quindi, essere previsto un meccanismo che genererà una risposta automatica al mittente, informando che la casella di posta elettronica è stata disattivata.

Tutte le informazioni eventualmente raccolte saranno utilizzate a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 2016/679.

Ai sensi di legge e della normativa fiscale, l'azienda è tenuta a conservare per dieci anni sui propri server

di posta elettronica tutti i messaggi e-mail a contenuto e rilevanza giuridica e commerciale provenienti da e diretti a domini della stessa.

14. Verifiche

I log relativi all'utilizzo di strumenti, reperibili nella memoria degli Strumenti stessi ovvero sui server o sui router, nonché i file con essi trattati sono registrati nei termini di cui alle relative piattaforme informatiche e possono essere oggetto di controllo da parte del titolare del trattamento, attraverso l'amministratore di sistema, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio.
I controlli potranno avvenire secondo le modalità previste dal regolamento ed andranno ben illustrati ai dipendenti/incaricati.
In ogni caso, Nova Group S.r.l. si impegna ad adottare tutte le misure tecnologiche volte a minimizzare l´uso di dati identificativi, e ciò in maniera adeguata e proporzionale alla tecnologia effettivamente impiegata.
Nova Group S.r.l. si impegna, altresì, ad eseguire i controlli nei limiti dei principi di pertinenza e non eccedenza – con esclusione di prolungati, costanti o indiscriminati - evitando interferenze ingiustificate sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

15. Conservazione

I sistemi software sono programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.
In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all'uso degli strumenti elettronici dovrà essere giustificata da finalità specifica e comprovata e limitata al tempo necessario –e predeterminato– a raggiungerla.
Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione: (i) ad esigenze tecniche o di sicurezza del tutto particolari; (ii) all´indispensabilità del dato rispetto all´esercizio o alla difesa di un diritto in sede giudiziaria; (iii) all´obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell´autorità giudiziaria o della polizia giudiziaria.
In questi casi, il trattamento dei dati personali sarà limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.