ALLEGATO 1

DISCIPLINARE RELATIVO ALL'UTILIZZO DEGLI STRUMENTI INFORMATICI E DEI DATI RACCOLTI MEDIANTE SUPPORTI CARTACEI

INDICE

1. Postazione di lavoro e personal computer
2. Password
3. Internet
4. Posta elettronica
5. Altri device
6. Dati raccolti mediante supporti cartacei - Clean desk policy
7. Sospette violazione dei dati (data breach)
8. Applicazione e controllo, provvedimenti disciplinari

PREMESSA

La Provincia di Cosenza, in qualità di titolare dei numerosi trattamenti di dati personali svolti nell'espletamento di compiti di interesse pubblico o per obblighi di legge, intende dare istruzioni specifiche ai propri dipendenti ("soggetti autorizzati" al trattamento dei dati) per l'utilizzo delle postazioni di lavoro e personal computer, della posta elettronica, di internet, nonché in merito alla raccolta di dati mediante supporti cartacei.
Un Ente pubblico gestisce una serie di documenti, atti, provvedimenti amministrativi, ecc. che riportano delle "informazioni" o dei dati.
Per **dato personale** si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile (l'«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.
Per **trattamento di dati personali** si intende, invece, qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
La progressiva diffusione delle tecnologie informatiche espone l'Ente a possibili rischi, pertanto, l'utilizzo delle risorse informatiche e telematiche dell'Ente deve sempre ispirarsi al principio di diligenza e correttezza.

Le attrezzature informatiche messe a disposizione dall'Ente nonché la posta elettronica sono strumenti di lavoro.

1.POSTAZIONE DI LAVORO E PERSONAL COMPUTER

Il sistema informativo dell'Ente è composto da un insieme di unità, server centrali e macchine client connessi ad una rete locale (LAN), che utilizzano diversi sistemi operativi e applicativi.
Il personal computer (pc) è uno strumento di lavoro e contiene tutti i software necessari a svolgere le attività affidate ed ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, rallentamenti del sistema, costi di manutenzione e, soprattutto, minacce alla sicurezza.
L'accesso all'elaboratore è protetto da password che deve essere custodita con la massima diligenza e non divulgata.
Gli Amministratori di sistema, utilizzando le proprie credenziali di accesso con privilegi di amministratore, potranno accedere sia alle memorie di massa locali di rete che ai server nonché, previa comunicazione, accedere al computer, anche in remoto.
Il "Login" è l'operazione con la quale ci si connette al sistema informativo dell'Ente o ad una parte di esso, dichiarando il proprio Username e Password (ossia l'Account) e aprendo una sessione di lavoro. In molti casi è necessario effettuare più login, tanti quanti sono gli ambienti di lavoro (ad es. applicativi web, rete, ecc.) che richiedono un username e una password.
In alcuni casi può essere assegnato un univoco username e password per gruppi di Autorizzati per l'accesso alla macchina fisica, mentre rimarranno separati ed univoci username e password per l'accesso agli applicativi che contengono dati.
Il "Logout" è l'operazione con cui viene chiusa la sessione di lavoro.
Al termine della giornata lavorativa, tutte le applicazioni devono essere chiuse secondo le regole previste dall'applicazione stessa in quanto la non corretta chiusura può provocare una perdita di dati o l'accesso agli stessi da parte di persone non autorizzate.
È obbligatorio eseguire le operazioni seguenti.

1. Se ci si allontana dalla propria postazione, mettere in protezione il pc affinché persone non autorizzate non abbiano accesso ai dati protetti.
2. Chiudere la sessione (Logout) a fine giornata.
3. Spegnere il PC dopo il Logout.
4. Controllare sempre che non vi siano persone non autorizzate alle spalle che possano prendere visione delle schermate del pc.
5. Non lasciare la postazione informatica incustodita lasciando accessibili i dati; tutti i supporti magnetici utilizzati devono essere riposti negli archivi.

Mediante lo scambio di file via internet, via mail, lo scambio di supporti removibili, il filesharing, le chat, ecc. possono essere trasmessi virus informatici in grado di danneggiare le attrezzature informatiche dell'Ente e sottrarre i dati ivi contenuti.
Per questo l'Ente impone su tutte le postazioni di lavoro l'utilizzo di un sistema antivirus, antimalware e firewall correttamente installato, attivato e aggiornato automaticamente con frequenza almeno quotidiana.
Alla luce di tutto ciò, è vietato eseguire le seguenti operazioni.

1. Gestire, memorizzare (anche temporaneamente) o trattare file, documenti e/o informazioni personali o comunque non afferenti alle attività lavorative nella rete locale, nel disco fisso o in altre memorie di massa dell'Ente e negli strumenti informatici in genere.
2. Modificare le configurazioni già impostate sul pc dell'Ente, se non con apposita autorizzazione.

3. Utilizzare programmi e/o sistemi di criptazione senza preventiva autorizzazione scritta.
4. Installare software senza licenza, né installare alcuna versione diversa, anche più recente, rispetto alle applicazioni o al sistema operativo presenti sul pc dell'Ente, senza espressa autorizzazione.
5. Fare copia del software installato sui pc dell'Ente al fine di farne un uso personale.
6. Caricare sul disco fisso del pc dell'Ente o nel server alcun documento, gioco, file musicale o audiovisivo o immagine diversi da quelli necessari allo svolgimento delle mansioni affidate.
7. Aggiungere o collegare dispositivi hardware (ad esempio hard disk, memorie USB, driver, PCMCIA, ecc.) o periferiche (telecamere, macchine fotografiche, smartphone, chiavi USB ecc.), senza apposita autorizzazione.
8. Creare o diffondere, intenzionalmente o per negligenza, programmi idonei a danneggiare il sistema informatico dell'Ente, quali per esempio virus, trojan horses ecc.
9. Effettuare in proprio attività manutentive o permettere attività manutentive da parte di soggetti non autorizzati.
10. Utilizzare aree di memoria diverse o creare altri files fuori dalle unità di rete locale dell'Ente.
11. Utilizzare i pc e accedere alla rete locale senza sistemi antivirus, antimalware e firewall attivi.
12. Utilizzare i pc senza periodicamente aggiornare i sistemi antivirus, antimalware e firewall.
13. Disattivare l'antivirus o il firewall, anche temporaneamente.
14. Cliccare su allegati di messaggi di posta elettronica, certificata e non, provenienti da mittenti sconosciuti o di dubbia provenienza.
15. Cliccare su allegati di messaggi di posta elettronica, certificata e non, provenienti da persone conosciute ma con testi inspiegabili o in qualche modo strani.
16. Omettere di comunicare ogni anomalia o malfunzionamento dei sistemi antivirus, antimalware e firewall, nonché la presenza di virus o file sospetti e di ogni altra attività sospetta.

I log relativi all'utilizzo di strumenti nonché i file con essi trattati sono registrati e possono essere oggetto di controllo da parte del titolare del trattamento, attraverso l'amministratore di sistema, per esigenze organizzative, per la sicurezza del lavoro e per la tutela del patrimonio.

2. PASSWORD

Le password costituiscono un metodo di autenticazione per garantire l'accesso protetto ad uno strumento hardware oppure ad un applicativo software.
È consigliata l'adozione dell'autenticazione a due fattori (2FA), che aumenta notevolmente la sicurezza dei nostri account, ed è ormai disponibile per la quasi totalità degli account dei servizi on line.
Per una corretta e sicura gestione delle proprie password, è obbligatorio attuare le seguenti pratiche.

1. Le password sono segrete e non devono essere svelate ad altri soggetti per evitare danni al proprio lavoro e a quello dei colleghi.
2. La password deve essere modificata al primo utilizzo ed ogni volta che viene richiesto dal sistema. Fino a qualche anno fa, vigeva l'obbligo di cambiare periodicamente le password, ma tale pratica non è più considerata consigliabile dal National Institute of Standards and Technology (NIST), poiché può portare l'utente ad utilizzare password banali per riuscire a ricordarle più facilmente (ogni volta che si è obbligati a cambiarle).

Addirittura, potrebbero indurre l'utente ad impostare password molto prevedibili e correlate tra loro: quindi la password successiva può essere dedotta sulla base della password precedente. Se la password è solida, può essere cambiata di tanto in tanto, ma deve essere certamente modificata, e immediatamente, qualora vi sia il dubbio che ne sia stata violata la segretezza.

3. Non memorizzare la password su supporti facilmente intercettabili da altre persone: il miglior luogo in cui conservare una password è la propria memoria.
4. Le password devono essere lunghe almeno 12 caratteri (meglio se è lunga 16 caratteri) e contenere anche lettere maiuscole, numeri e caratteri speciali quali { } [ ] , . <> ; : ! " £ $ % & / ( ) = ? ^ \ | ' * - + _..
5. Le password non devono essere memorizzate su alcun tipo di supporto, quali, ad esempio, Post-It (sul monitor o sotto la tastiera), agende, files, posta elettronica, cellulare.
6. È vietato digitare la propria password in presenza di altri soggetti che possano vedere la tastiera, anche se autorizzati.

La password ideale è complessa, senza alcun riferimento.

Di seguito, alcuni esempi di password poco sicure.

1. Nome, cognome e loro parti.
2. Username assegnato.
3. Indirizzo di posta elettronica (e-mail).
4. Parole comuni (in Inglese e in Italiano).
5. Date, mesi dell'anno e giorni della settimana, anche in lingua straniera.
6. Parole banali e/o di facile intuizione e palindromi.
7. Ripetizioni di sequenze di caratteri (es. abcdabcd).
8. Password già impiegate in precedenza.
9. Se Username = "marioverdi", password = "mario", o ancora peggio, password = "marioverdi".
10. Il nome della moglie/marito, fidanzato/a, figli, ecc. anche a rovescio.
11. La propria data di nascita, quella del coniuge, ecc.
12. Targa della propria auto.
13. Numero di telefono proprio, del coniuge, ecc.
14. Il nome di login (o codice di identificazione personale) in qualsiasi forma (ad esempio: invertito, in maiuscole, duplicato, ecc.).
15. Il nome del sistema operativo che si sta usando.
16. Il numero di telefono.
17. Altre informazioni facilmente ricavabili dall'indirizzo, o parti del codice fiscale.
18. Nomi di città, nomi propri.
19. Semplici composizioni quali ad esempio "qwerty".
20. Caratteri sequenziali ripetuti (ad esempio 1111, aaaa, ecc.).
21. Cifre in progressivo ordine crescente o decrescente.
22. Informazioni legate al lavoro quali nomi di software, hardware, nomi di prodotti o servizi.

3.INTERNET

La connessione alla rete internet dal pc è ammessa esclusivamente per motivi attinenti allo svolgimento dell'attività lavorativa.

L'utilizzo per scopi personali è permesso con moderazione e con gli accorgimenti di cui al presente documento.

In particolare, si vieta l'utilizzo dei social network, se non espressamente autorizzati.
L'Ente potrà adottare idonee misure tecniche preventive volte a ridurre navigazioni a siti non correlati all'attività lavorativa attraverso filtri e black list.
È altresì vietato:

1. Navigare nei siti che possono rivelare le opinioni politiche religiose, sindacali e di salute.
2. Avere accesso a siti internet che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, rilevante ai fini della realizzazione di una fattispecie di reato o che siano in qualche modo discriminatori sulla base della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.
3. Scaricare software (anche gratuito) prelevato da siti Internet;
4. Effettuare ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi autorizzati e con il rispetto delle normali procedure di acquisto.
5. Registrare account a siti i cui contenuti non siano legati all'attività lavorativa.
6. Partecipare a forum non professionali, utilizzare chat line e bacheche elettroniche, partecipare a gruppi di discussione o lasciare commenti ad articoli o iscriversi a mailing list spendendo il marchio o la denominazione dell'Ente, salvo specifica autorizzazione.
7. Memorizzare documenti informatici di natura oltraggiosa, diffamatoria e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
8. Promuovere utile o guadagno personale attraverso l'uso di Internet o della posta elettronica dell'Ente.
9. Accedere dall'esterno alla rete locale, salvo autorizzazione specifica.
10. Creare siti web personali sui sistemi dell'Ente.
11. Accedere ad alcuni siti internet mediante azioni inibenti dei filtri, sabotando o comunque superando o tentando di superare o disabilitando i sistemi adottati dall'Ente per bloccare accessi non conformi all'attività lavorativa.
12. Utilizzare l'accesso a internet in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore (es. legge 22 aprile 1941, n. 633 e successive modificazioni, d.lgs. 6 maggio 1999, n. 169 e legge 18 agosto 2000, n. 248) e, in particolare, scaricare materiale soggetto a copyright (testi, immagini, musica, filmati, file in genere) se non espressamente autorizzato.

Infine, si raccomanda di evitare di inviare username e password o altre informazioni personali su siti il cui indirizzo inizia con http://.
Http e https sono due protocolli.
Un protocollo è un set di regole che definiscono il modo in cui due elaboratori debbano effettuare lo scambio di un certo tipo di dati.
HTTP è acronimo di HyperText Transfer Protocol.
HTTPS è acronimo di HyperText Transfer Protocol over Secure Socket Layer (SSL).
Come è intuitivo osservare, in HTTPS la comunicazione tra client e server avviene secondo le stesse regole del protocollo HTTP, ma all'interno di una connessione criptata (over Secure Socket Layer).
Questo significa che i dati da e verso un sito web che utilizza il protocollo HTTPS non viaggiano "in chiaro" ma criptati, evitando così che malintenzionati li possano catturare e/o manomettere durante il tragitto.

4. POSTA ELETTRONICA

L'utilizzo della posta elettronica è connesso allo svolgimento dell'attività lavorativa e l'uso per motivi personali è vietato.
Di seguito alcune operazioni vietate.

1. Inviare, tramite la posta elettronica, anche all'interno della rete locale, materiale a contenuto violento, sessuale o comunque offensivo dei principî di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico.
2. Inviare messaggi di posta elettronica, anche all'interno della rete locale, che abbiano contenuti contrari a norme di legge ed a norme di tutela dell'ordine pubblico, rilevanti ai fini della realizzazione di una fattispecie di reato, o che siano in qualche modo discriminatori della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.
3. Usare un account di posta elettronica per iscriversi in qualsivoglia sito per motivi non attinenti all'attività lavorativa, senza espressa autorizzazione scritta, nonché utilizzare il dominio dell'organizzazione per scopi personali.
4. Creare, archiviare, spedire messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) non connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto, "catene di Sant'Antonio" o in genere a pubblici dibattiti.
5. Inviare messaggi di posta elettronica a gruppi numerosi di persone senza autorizzazione.
6. Sollecitare donazioni di beneficenza, propaganda elettorale o altre voci non legate alle finalità istituzionali.
7. Trasmettere a soggetti esterni informazioni riservate o comunque documenti su cui vige il segreto d'ufficio, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte.
8. Inviare messaggi contenenti allegati con dati personali senza che siano stati prima resi illeggibili attraverso la crittografia 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, e ancor di più i dati personali, possono essere inviati soltanto a destinatari – persone o Enti – qualificati e competenti.
9. Usare la posta elettronica per inviare messaggi con allegati di grandi dimensioni.

È altresì obbligatorio controllare i file allegati di posta elettronica prima del loro utilizzo. In particolare, si deve evitare, secondo le regole di buona diligenza, l'apertura e la lettura di messaggi di posta elettronica in arrivo provenienti da mittenti di cui non si conosce con certezza l'identità o che contengano allegati del tipo .exe, .com, .vbs, .htm, .scr, .bat, .js, .pif.
Infine, in caso di assenza improvvisa o prolungata di un dipendente il titolare della casella di posta dovrebbe designare un altro dipendente per verificare il contenuto di messaggi.

È opportuno, inoltre, inserire, in calce alla firma della e-mail, un disclaimer per i destinatari, quale quello che segue.
Disclaimer
Le informazioni contenute nel presente messaggio ed i relativi allegati sono riservate e confidenziali e comunque destinate esclusivamente alle persone o ai soggetti indicate come destinatari, pertanto ne è vietata la diffusione, la comunicazione, la distribuzione o la copia da parte di qualsiasi soggetto diverso dal destinatario sia ai sensi dell'art. 616 c.p., che ai sensi del Regolamento UE 2016/679. Qualora Lei non fosse la persona alla quale il presente messaggio è destinato La invitiamo gentilmente, dopo aver informato tempestivamente il mittente, ad eliminarlo e a non utilizzarne in alcun caso il contenuto. Qualsiasi utilizzo non autorizzato di questo

messaggio e dei suoi eventuali allegati espone a conseguenze civili e penali. L'invio di e-mail al nostro indirizzo potrebbe non assicurare la riservatezza, potendo essere viste da altri soggetti appartenenti all'organizzazione oltre al sottoscritto, per finalità di sicurezza informatica, amministrative e allo scopo del continuo svolgimento dell'attività istituzionale.

Attenzione al phishing.

Il "phishing" è una frode finalizzata all'acquisizione via e-mail, per scopi illegali, di dati personali e riservati: molto spesso arrivano nella casella di posta elettronica dei messaggi in cui si richiede di inserire le proprie credenziali o di cliccare su un link.

Il furto dei dati avviene attraverso l'invio di e-mail contraffatte, anche con grafica, nomi e loghi ufficiali di Società ed Enti, in molti casi anche Banche, Istituti di Credito, Avvocati, ecc. che invitano a fornire informazioni personali, quali ad esempio i dati della carta di credito, o contenenti la richiesta di credenziali per accedere alle vostre aree riservate, oppure a pagare per riavere informazioni, ecc.

Per accedere ad un sito, però, non bisogna mai inserire i propri dati di login cliccando direttamente sui link proposti all'interno di un'e-mail, ma digitare manualmente (nella barra degli indirizzi del browser) l'indirizzo del sito per essere certi di non incorrere in siti contraffatti.

Nel caso in cui si dovesse ricevere una mail sospetta con oggetto simile a "...notifica sentenza..." oppure "avviso di spazio esaurito sulla casella postale" oppure "fattura n. ... del..." oppure "spedizione n. ... del ...", deve evitare di aprirla e soprattutto deve evitare di "cliccare" sui link in essa presenti e su eventuali allegati.

In caso di sospetti, è comunque obbligatorio modificare la password.

Attenzione al Ransomware (cryptor, blocker).

Sovente arrivano dei messaggi di posta elettronica con oggetto del tipo "...notifica sentenza..." oppure "avviso di spazio esaurito sulla casella" oppure "fattura n. ... del..." oppure "spedizione n. ... del ...".

È severamente vietato cliccare sui link presenti in tali messaggi e sugli allegati senza essersi accertati dell'identità del mittente e dell'autenticità del sito.

È necessario fare molta attenzione ai messaggi ricevuti nelle caselle di posta elettronica, sia quella normale sia quella certificata, perché cliccando sugli allegati potrebbe avviarsi il download di un virus. Nei casi più gravi il pc viene infettato da un *malware* detto "***Cryptolocker***", ossia quella tipologia di codice malevolo che cripta i dati di un hard disk rendendoli praticamente inutilizzabili e prevedendo un riscatto per il ripristino della situazione "ex ante".

Si tenga conto che spesso il virus si nasconde dietro messaggi di posta elettronica con mittente apparentemente noto, ma a ben vedere associato ad un indirizzo e-mail diverso.

Se però l'indirizzo e-mail del mittente è stato hackerato, mediante una modalità di falsificazione nota come spoofing, il virus potrebbe nascondersi in e-mail provenienti da indirizzi noti.

È opportuno dunque evitare:

a) di cliccare sui link contenuti in tali messaggi;

b) di cliccare su eventuali file allegati a tali messaggi;

c) di salvare gli allegati.

Nel dubbio, è consigliabile chiedere telefonicamente al mittente se quella e-mail è autentica.

Ecco altre semplici regole pratiche che ci possono aiutare a non cadere nella trappola dei ransomware:

- abilitare l'opzione Mostra estensioni nomi file nelle impostazioni di Windows: i file più pericolosi hanno l'estensione EXE, ZIP, JS, JAR, SCR ecc. Se questa opzione è disabilitata non riusciremo a vedere la reale estensione del file;

- disabilitare la riproduzione automatica ("autorun") di chiavette USB, CD/DVD e altri supporti esterni e, più in generale, evitare di inserire questi oggetti nel nostro computer se non siamo certi della provenienza;
- disabilitare l'esecuzione di macro da parte di componenti Office (Word, Excel, PowerPoint). Una macro malevola potrebbe essere contenuta in un allegato in formato Office e attivarsi automaticamente a seguito di un nostro clic;
- aggiornare sempre i sistemi operativi e i browser. In generale è buona regola installare sempre e subito le "patch" (gli aggiornamenti) di sicurezza che ci vengono proposti dai produttori dei software che abbiamo installati;
- utilizzare – quando possibile – account senza diritti da amministratore: se viene violato un account con privilegi ed accessi di amministratore, l'attaccante potrà utilizzare gli stessi privilegi per compiere più azioni e fare maggiori danni;
- installare servizi antispam efficaci ed evoluti, i quali non riusciranno a bloccare tutte le e-mail di phishing, ma i migliori riescono a raggiungere un'efficienza superiore al 95%.

In caso di sospetti, è comunque obbligatorio avvisare il Referente privacy e il Responsabile della Protezione Dati dell'Ente ed è opportuno modificare la password.

Cosa fare in caso di sospetta infezione da virus, malware, ecc.

1. Non spegnere il pc/device, perché ciò renderebbe più difficile il recupero dei dati.
2. Disattivare immediatamente la connessione ad internet (sul pc basterà cliccare, nella barra delle applicazioni, sull'icona del collegamento wi-fi o ethernet e poi su "Apri impostazioni Rete e Internet" oppure estrarre il cavo ethernet oppure spegnere il modem).
3. Avvertire immediatamente il Responsabile IT o CED oppure la società informatica esterna che si occupa della sicurezza dei pc.
4. Qualora sussista la possibilità che siano in pericolo i dati personali presenti sul pc/device e sulle memorie ad esso collegate, avvertire immediatamente il Titolare e il Responsabile Protezione Dati (DPO) per la valutazione dell'attivazione della procedura di data breach.

5. ALTRI DEVICE

Qualora ai soggetti Designati e Autorizzati dovesse essere affidato un computer portatile, un tablet o uno smartphone dall'Ente, gli stessi sono responsabili di tali device, ai quali si applicano le regole di utilizzo previste per i pc.

I files creati o modificati su tali device devono essere trasferiti sulle memorie di massa dell'Ente al primo rientro in ufficio e cancellati in modo definitivo da tali device, che comunque devono essere custoditi in un luogo protetto.

In caso di perdita o furto dei device mobili deve far seguito la denuncia alle autorità competenti.

Anche di giorno, durante l'orario di lavoro, non è consentito lasciare incustoditi i device mobili né a vista dentro l'auto o in una stanza d'albergo o nell'atrio dell'albergo o nelle sale d'attesa delle stazioni ferroviarie e aeroportuali.

Le stesse regole valgono per il caso in cui ai soggetti Designati e Autorizzati venga affidata una memoria esterna (quale una chiave USB, un hard disk esterno, una memory card, ...) su cui copiare temporaneamente dei dati per un facile trasporto, o altri usi (es. macchine fotografiche con memory card, videocamere con dvd, ecc.).

Ogni Device ed ogni memoria esterna affidati ai soggetti Designati e Autorizzati (computer, notebook, tablet, smartphone, memory card, chiavi usb, hard disk, dvd, cd-rom, ecc.), al termine del loro utilizzo dovranno essere restituiti all'Ente, che è esclusivo titolare e proprietario dei device.

I device non devono essere utilizzati per finalità private e diverse da quelle istituzionali.

È fatto divieto assoluto di formattare o alterare o manomettere o distruggere i device assegnati o rendere inintelligibili i dati in essi contenuti tramite qualsiasi processo.
A seguito di una cessazione del rapporto lavorativo con l'organizzazione, Designati e Autorizzati devono immediatamente restituire i device in uso.

6.DATI RACCOLTI MEDIANTE SUPPORTI CARTACEI - CLEAN DESK POLICY

È obbligatorio adottare una "politica della scrivania pulita" ovvero trattare dati raccolti mediante supporti cartacei solo se necessario, privilegiando, ove possibile, l'utilizzo degli strumenti digitali.
In particolare, si invita a non lasciare in vista sulla propria scrivania dati raccolti mediante supporti cartacei quando ci si allontana dalla stessa oppure quando è previsto un incontro con un soggetto non abilitato alla conoscenza dei dati in essi contenuti.
Prima di lasciare la propria postazione (per esempio per la pausa pranzo o per una riunione) è obbligatorio riporre in luogo sicuro (armadio, cassettiera, archivio, ecc.) i dati raccolti mediante supporti cartacei, affinché gli stessi non possano essere visti da terzi (es. addetti alle pulizie, visitatori, ecc.).
A fine giornata deve essere previsto il riordino della scrivania e la corretta archiviazione di tutte le pratiche d'ufficio, in modo da lasciare la scrivania completamente sgombra, e, ove possibile, bisogna evitare la stampa di documenti digitali, anche ai fini di ridurre l'inquinamento ed il consumo delle risorse in ottica ecologica.
È altresì necessario rimuovere immediatamente ogni foglio stampato da una stampante o da un'apparecchiatura fax, per evitare che siano prelevati o visionati da soggetti non autorizzati.
È necessario eliminare i documenti attraverso apparecchiature trita documenti.
A seguito di una cessazione del rapporto lavorativo è necessario restituire immediatamente i dati raccolti mediante supporti cartacei in possesso.
L'eventuale accesso fuori dall'orario di lavoro impone la registrazione e identificazione delle persone ammesse ai locali e i documenti (o loro copia) non possono, senza autorizzazione, essere portati fuori dai luoghi di lavoro, salvo i casi di comunicazione dei dati a terzi, previa autorizzazione.
Se del caso, bisogna conservare in armadi ben custoditi gli archivi relativi alle banche dati di tipo cartaceo assicurandosi che gli uffici siano adeguatamente chiusi.
Qualora venga raccolto il consenso dell'interessato, il relativo documento deve essere custodito con la massima cura ed adeguate misure di sicurezza al fine di evitare che altri soggetti prendano visione dei dati riportati nel documento.

7. PROCEDURA IN CASO DI SOSPETTA VIOLAZIONE DEI DATI (DATA BREACH)

Con il termine data breach si intende la violazione dei dati personali dell'interessato, persona fisica, che può consistere, a titolo esemplificativo e non esaustivo, in:

- perdita del controllo dei dati personali che riguardano gli interessati o limitazione dei loro diritti;
- discriminazione, furto o usurpazione d'identità;
- perdite finanziarie, decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale;
- qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.
- divulgazione di dati confidenziali a persone non autorizzate;
- perdita o furto di dati o di strumenti (es. un pc portatile) nei quali i dati sono memorizzati;

- perdita o furto di documenti;
- infedeltà (ad esempio: data breach causato da un autorizzato, il quale, dopo aver avuto accesso ai dati, ne produca una copia distribuita in ambiente pubblico);
- accesso abusivo (ad esempio: data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);
- casi di pirateria informatica;
- banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo proprietario;
- virus o altri attacchi al sistema informatico o alla rete locale;
- violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o archivi, contenenti informazioni riservate);
- smarrimento di pc portatili, devices o attrezzature informatiche al cui interno sono contenuti dati personali "in chiaro" e non cifrati;
- invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario.

In linea con la definizione di violazione di dati personali, possiamo distinguere tre tipi di violazione dei dati personali, che possono tuttavia combinarsi tra loro:
1) violazione di riservatezza, quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;
2) violazione di integrità, quando si verifica un'alterazione di dati personali non autorizzata o accidentale;
3) violazione di disponibilità, quando si verifica perdita, inaccessibilità, o distruzione, accidentali o non autorizzate, di dati personali.
La rilevazione di un evento di data breach può avvenire:
- in maniera automatica (da sistemi di segnalazione automatica come, ad esempio, violazioni conseguenti al superamento del firewall);
- dall'interno (segnalazione ad opera di autorizzati, e/o amministratori di sistema, intrusioni fisiche di soggetti non autorizzati nei locali, furti, smarrimenti di fascicoli cartacei e/o di devices contenenti dati personali, blocco dei sistemi e/o malfunzionamenti degli stessi);
- dall'esterno (segnalazione da parte di fornitori).

In caso di sospetto data breach viene attivata una procedura ad hoc, nella quale il Referente privacy dell'Ente assume il ruolo di responsabile del processo.
Lo scopo della procedura è di disegnare un flusso per la gestione delle violazioni dei dati personali.
Ogni volta che vengono rilevate attività sospette per quanto riguarda la protezione dei dati, è obbligatorio avvertire il Titolare del trattamento e il DPO dell'Ente.

8.APPLICAZIONE E CONTROLLO, PROVVEDIMENTI DISCIPLINARI

L'Ente, in qualità di Titolare degli strumenti informatici, dei dati ivi contenuti e/o trattati, si riserva la facoltà di effettuare i controlli che ritiene opportuni per tutelare la sicurezza e preservare l'integrità degli strumenti e dei dati, evitare la commissione di illeciti o per esigenze di carattere difensivo, anche preventivo, verificare la funzionalità del sistema e degli strumenti informatici. In ogni caso l'organizzazione non adotta "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori" (ex art. 4, primo comma, l. n. 300/1970), tra cui sono comprese le strumentazioni hardware e software mirate al controllo dell'utente né adotta sistemi che determinano interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.
Le infrazioni disciplinari alle norme del presente Disciplinare potranno essere punite, a seconda della gravità delle mancanze, in conformità alle disposizioni di legge e/o del Contratto Collettivo Nazionale del Lavoro applicato.