ALLEGATO 2

MANUALE OPERATIVO PER LA PROTEZIONE DATI E LA SICUREZZA INFORMATICA

Il presente documento programmatico definisce le linee guida e le misure organizzative e tecniche adottate dalla Procura di Terni per la protezione dei dati personali, al fine di garantire la conformità alla normativa vigente e tutelare i diritti degli interessati.

Gli incaricati devono trattare i dati personali garantendo la massima riservatezza delle informazioni emanate vengono in possesso, considerare tutti i dati personali come riservati e osservare le norme vigenti e le disposizioni dall'Ufficio in materia di sicurezza e riservatezza.
Gli incaricati accedono ai soli dati personali la cui conoscenza sia strettamente necessaria per il trattamento dei compiti loro assegnati. I documenti, atti, fascicoli sono trattenuti dagli incaricati solo per il tempo strettamente necessario alle operazioni di trattamento.
Curano il corretto utilizzo degli applicativi informatici e degli archivi cartacei nell'ambito dei rispettivi uffici; svolgono il trattamento secondo correttezza con raccolta e registrazione di dati esclusivamente per gli scopi inerenti alla attività svolta; provvedono alla conservazione in conformità alle misure di sicurezza, garantendo in ogni operazione di trattamento, sia cartaceo che automatizzato, la massima riservatezza evitando l'accesso da parte di terzi.
Mantengono l'assoluto riserbo sui dati cui vengono a conoscenza nell'esercizio della propria funzione. In caso si debba procedere alla distruzione devono adottarsi tutte le misure volte ad evitare che i dati possano essere individuati e recuperati e che si possa conoscere il contenuto e la provenienza dei dati.
Gli incaricati sono invitati a segnalare al titolare:

- le violazioni dei dati personali;
- ogni eventuale situazione da valutarsi al fine dell'eventuale adozione di specifiche e ulteriori misure di sicurezza rispetto a quelle in essere.

Per quanto non su indicato si richiamano le disposizioni impartite in sede ministeriale e contenute nel "Piano strategico di sicurezza" (PSS).

PRESCRIZIONI PER TRATTAMENTI CON L'AUSILIO DI STRUMENTI ELETTRONICI

Di seguito i principali suggerimenti e le istruzioni per aumentare la sicurezza informatica e nel trattamento dei dati.

SPEGNERE IL COMPUTER IN CASO DI ASSENZA PER UN PERIODO DI

TEMPO LUNGO

Un computer acceso è in linea di principio maggiormente attaccabile perché raggiungibile tramite la rete o direttamente sulla postazione di lavoro. Inoltre, più lungo è il periodo di assenza, maggiore è la probabilità che un'interruzione dell'energia elettrica possa portare un danno.

NON LASCIARE LAVORI INCOMPIUTI SULLO SCHERMO

Occorre sempre chiudere le applicazioni con le quali sta lavorando quando ci si allontana dal posto di lavoro per più di pochi minuti: un documento presente sullo schermo è vulnerabile a trattamenti non autorizzati.

SALVASCHERMO

Ogni postazione di lavoro deve avere il salvaschermo attivato, con richiesta di password per poter riprendere il controllo della postazione.

PROTEGGERE ATTENTAMENTE I DATI

Bisogna prestare particolare attenzione ai dati importanti di cui si è personalmente responsabili. Poiché può risultare difficile distinguere tra dati normali e dati importanti, è buona norma trattare tutti i dati come se fossero importanti. Come minimo posizionarli in un'area protetta da password e non dare di default a nessun altro utente il permesso di lettura o modifica. Ai dati da condividere applicare i permessi opportuni solo per il tempo strettamente necessario all'interazione con gli altri utenti.

UTILIZZO SUPPORTI DI MEMORIA

Alla conservazione dei supporti di memoria (CD, dischetti) si applicano gli stessi criteri di protezione dei documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può anche essere dovuto a un furto) può passare più facilmente inosservato. Occorre riporli in luogo sicuro non appena finito di usarli.

ABILITAZIONE OVE POSSIBILE DELL'ACCESSO TRAMITE PASSWORD PROTEGGERE IL COMPUTER CON UNA PASSWORD

La maggior parte dei computer offre la possibilità di impostare una password all'accensione. Anche alcuni applicativi permettono di proteggere i propri dati tramite password. E' buona norma utilizzare queste caratteristiche che offrono un buon livello di riservatezza.

NON CONSENTIRE L'USO DEL COMPUTER O DELL' ACCOUNT A PERSONALE ESTERNO

Nel caso in cui personale esterno ha necessità di installare nuovi software/hardware nel vostro computer occorre assicurarsi dell'identità della persona e delle autorizzazioni ad operare sul vostro PC.

NON UTILIZZARE APPARECCHIATURE NON AUTORIZZATE O PER CUI NON SI E' AUTORIZZATI

L'utilizzo di modem su postazioni di lavoro collegate alla rete di ufficio offre una porta d'accesso dall'esterno non solo al computer del dipendente ma a tutta la rete di cui fa parte. E' quindi vietato l'uso di modem all'interno della rete locale. Nel caso che ciò sia strettamente necessario, disconnettere fisicamente la postazione di lavoro dalla rete locale prima di effettuare il collegamento via modem. Per l'uso di altre apparecchiature, chiedere consiglio all'amministratore di sistema.

NON INSTALLARE PROGRAMMI NON AUTORIZZATI

Oltre alla possibilità di trasferire involontariamente un virus o di introdurre un cosiddetto "cavallo di troia", va ricordato che la maggior parte dei programmi sono protetti da copyright, per cui la loro installazione può essere illegale.

DIFFIDARE DEI DATI O DEI PROGRAMMI LA CUI PROVENIENZA NON È CERTA

Per proteggersi da virus ed altri agenti attivi di attacco, occorre diffidare di tutti i dati e programmi che vi vengono inviati o consegnati, anche se la fonte appare affidabile o il contenuto molto interessante. Infatti, molti sistemi di attacco inviano dati che sembrano provenire da un utente noto al destinatario per vincerne la naturale diffidenza nei confronti degli estranei.

AMMINISTRARE CORRETTAMENTE LE PASSWORD

La scelta della password è estremamente importante per la sicurezza dei propri dati e dell'intera rete del Ministero della Giustizia. Le password debbono essere cambiate con frequenza:

- quadrimestrale, per gli account a rischio, di sistema o con elevati privilegi (inclusi amministratori, manutentori. ecc.);

- semestrale per gli account utenti;

- annuale per le password di accensione delle postazioni di lavoro. Per la composizione della password si indica il link del GPDP dove è possibile trovare consigli per impostare password sicure e gestirle in modo accorto https://www.garanteprivacy.it/temi/cybersecurity/password .

Tutti gli utenti, infine, debbono attenersi scrupolosamente alle seguenti prescrizioni:

• non rivelare le password a nessuno, inclusi amici e familiari;
• non condividere le password con altri colleghi o assistenti;
• non inviare le password tramite e-mail o altri metodi di comunicazione elettronica, né tramite telefono;
• non scrivere le password su carta o biglietti e non memorizzare le password su file o altri sistemi (palmari o agende elettroniche) senza cifratura;
• non scrivere la propria password su questionari o presunti moduli di sicurezza;
non utilizzare sistemi informatici che permettono di memorizzare le password o gestire un database di password;
• non riutilizzare in nessun caso le password.

VIRUS E MISURE ANTIVIRUS

Gli utenti devono:

• usare soltanto programmi provenienti da fonti fidate perché copie sospette di programmi possono contenere virus o altro software dannoso;
• installare (o farsi istallare dagli amministratori di sistema) l'ultima versione dell'antivirus e tenere aggiornati i file con gli identificativi dei virus.
Gli utenti non devono:
• visitare siti illegali (ad esempio depositi di software pirata) che sono spesso usati come specchietto per le allodole per attirare visitatori su cui condurre attacchi.

UTILIZZO POSTA ELETTRONICA

Gli utenti devono:
• usare solo il software di posta approvato dal Ministero della Giustizia;
• impedire ad altre persone di utilizzare il proprio account per inviare posta elettronica;
• trasmettere di preferenza messaggi con firma digitale

Gli utenti non devono:
• utilizzare la posta elettronica per scopi in conflitto con il piano di sicurezza ed in ogni caso non utilizzarla per scopi personali;
• partecipare alle cosiddette "Catene di Sant'Antonio" o, in generale, utilizzare la posta elettronica per spamming;
• inviare mai informazioni confidenziali tramite posta elettronica non cifrata;
• aprire posta elettronica di provenienza dubbia e, in generale, non aprire nessun allegato senza una preventiva scansione anti-virus.

PRESCRIZIONI PER TRATTAMENTO DATI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI (ATTI, DOCUMENTI E FASCICOLI CARTACEI)

Ciascun operatore si atterrà alle seguenti ulteriori prescrizioni:

a) occorre chiudere a chiave il proprio ufficio alla fine della giornata ed in ogni caso di assenza. I documenti devono essere conservati in armadi o cassetti chiusi quando possibile;
b) i fascicoli e gli altri atti cartacei, nelle fasi di trasporto all'interno dell'ufficio, devono permanere nei corridoi il tempo strettamente necessario alla loro consegna.
c) nessuno può accedere all'archivio se non autorizzato;
d) i fascicoli e gli atti affidati agli incaricati del trattamento, devono essere da questi ultimi conservati e restituiti al termine delle operazioni da svolgere;
e) i fascicoli ubicati su scrivanie e/o piani di appoggio in genere devono essere posizionati in modo da non rendere visibili i dati (per es.: capovolti). Lo stesso accorgimento deve essere tenuto se fascicoli ed atti sono posizionati su carrelli per il loro trasporto o all'interno di autovetture;
f) le stampe di materiale riservato devono essere maneggiate e custodite con cura evitando la possibilità di accesso alle stampe alle persone non autorizzate. Se la stampante non si trova sulla scrivania occorre ritirare le stampe nel più breve tempo possibile. Occorre distruggere personalmente le stampe quando non servono più. Evitare di gettare nel cestino le stampe di documenti che possono contenere informazioni confidenziali se si trattano dati di particolare riservatezza e in ogni caso non gettare mai documenti cartacei senza averli prima fatti a pezzi.