Disposizioni in materia di trattamento dei dati personali

Visto il d.lgs. 30 giugno 2003, n. 196, “Codice in materia di protezione dei dati personali”;

visto il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 “relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE” (GDPR - General Data Protection Regulation);

vista la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016, “relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio”;

visto il d.lgs. 10 agosto 2018, n. 101 “Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)”;

visto il D.M. 27 aprile 2009 “Nuove regole procedurali relative alla tenuta dei registri informatizzati dell'amministrazione della giustizia”;

premesso che, sensi dell’art. 4 punto 1) del Regolamento (UE) 2016/679, per **dato personale** s’intende “*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 on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*”;

premesso che, ai sensi dell’art. 4 punto 2) del Regolamento (UE) 2016/679, per **trattamento** s’intende “*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";

premesso che, ai sensi dell'art. 4 punto 22) del Regolamento (UE) 2016/679, per **violazione dei dati personali** s'intende *"la 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",*

il trattamento di dati personali deve avvenire nel rispetto dei seguenti principi fissati all'art. 5 del Regolamento (UE) 2016/679:

- liceità, correttezza e trasparenza del trattamento, nei confronti dell'interessato;
- limitazione della finalità del trattamento, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati;
- minimizzazione dei dati: ossia, i dati devono essere adeguati pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento;
- esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;
- limitazione della conservazione: ossia, è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
- integrità e riservatezza: occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento.

I soggetti interessati dal trattamento dei dati sono:

1. il **titolare del trattamento** è [art. 4 - 7) del Regolamento (UE) 2016/679] la persona fisica, la persona giuridica, la P.A. e qualsiasi altro organismo cui competono le decisioni in ordine alle finalità e alla modalità del trattamento dei dati. Il titolare vigila sulla correttezza delle operazioni di trattamento dei dati e sull'osservanza, da parte dei responsabìli ed incaricati, delle istruzioni impartite al fine che interessa, nonché sull'attuazione del presente documento. **Titolari del trattamento sono**

nel rispetto delle relative competenze il Ministero della giustizia e la Corte di Appello di Venezia in persona del Presidente pro-tempore;

2. il **responsabile del trattamento** è [art. dell'art. 4 - 8) del Regolamento (UE) 2016/679] Ia persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento. È il soggetto preposto a vigilare, nell'ambito del proprio settore e sfera di **intervento**, a che il trattamento medesimo avvenga in maniera corretta. **Responsabili del trattamento sono il Ministero della Giustizia e il dirigente amministrativo, che può ricorrere ad altro responsabile, previa autorizzazione scritta, specifica o generale, del titolare del trattamento;**

3. il **responsabile della protezione dei dati personali** [art. 37 del Regolamento (UE) 2016/679] individuabile nella **persona fisica pro tempore nominata per tutti gli uffici dal Ministero della Giustizia;**

4. gli **incaricati del trattamento:** tutte le persone fisiche autorizzate, in relazione alle attività svolte in conformità all'ambito di competenza e nei limiti delle proprie attribuzioni, a compiere operazioni di trattamento. In via esemplificativa i magistrati, il personale amministrativo, i collaboratori a qualsiasi titolo, i tirocinanti e il personale esterno all'amministrazione autorizzato a operare nell'ufficio.

Nell'ufficio giudiziario sono trattati i dati relativi a tutti i soggetti giuridici identificati o identificabili, anche indirettamente mediante riferimento a qualsiasi altra informazione, che vengono comunicati per motivi istituzionali o di servizio al personale dell'ufficio e i dati del personale dipendente.

Gli incaricati devono trattare i dati personali garantendo la massima riservatezza delle informazioni di cui vengono in possesso, considerare tutti i dati personali come riservati e osservare le disposizioni emanate dall'Ufficio in materia di sicurezza e riservatezza.

Gli incaricati accedono ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati.

Nel corso dell'intero ciclo necessario alle operazioni di trattamento gli incaricati devono attenersi alle seguenti disposizioni:

- i documenti, atti, fascicoli contenenti i dati personali non possono essere consultati da persone diverse da quelle incaricate del trattamento;
- i documenti, atti, fascicoli sono trattenuti dagli incaricati solo per il tempo strettamente necessario alle operazioni di trattamento;
- tutt gli archivi devono essere provvisti di dispositivi volti a impedire accessi non autorizzati.

I responsabili e 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.

A. Criteri tecnici e organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza, nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi.

1. Protezione delle aree e dei locali interessati

1.1 Le macchine *server* vanno collocate in un apposito locale (sala *server*).
1.2 La sala *server* deve essere dotata di:
a) impianto antincendio adeguato a locali contenenti apparati informatici;
b) impianto di condizionamento ambientale, opportunamente dimensionato;
c) impianto elettrico a norma;
d) gruppo di continuità.
1.3 L'accesso alla sala *server* è consentito solo al responsabile del trattamento e alle persone espressamente autorizzate.
1.4 In assenza del personale autorizzato, la sala deve essere tenuta chiusa a chiave.
1.5 I supporti di *backup* vanno tenuti in armadi blindati, posti in locali distanti dalla sala *server*, non trasportabili e dotati di impianto antifurto.
1.6 Tutte le chiavi vanno custodite dalla vigilanza o dal personale delegato dal Capo dell'ufficio.
1.7 Tutte le risorse necessarie per l'attuazione di quanto previsto in questa sezione sono individuate dal capo dell'ufficio, con l'intervento, ove necessario, del Procuratore Generale, nel suo ruolo di responsabile della sicurezza delle infrastrutture.

2. Gestione degli apparati di rete

2.1 Gli armadi che contengono gli apparati di rete vanno tenuti chiusi a chiave. Le chiavi devono essere custodite secondo le stesse procedure previste al punto 1.6

2.2 Le porte telematiche degli apparati di rete che non siano utilizzate devono essere disabilitate tramite *il software* di gestione.

2.3 Laddove gli apparati di rete vengano gestiti attraverso la rete locale dell'edificio, il loro indirizzamento deve avvenire su una rete IP distinta.

B. Criteri per il trattamento di dati con strumenti elettronici

Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che permettano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

C. Criteri e procedure per assicurare l'integrità dei dati

3. Integrità dei dati

3.1 L'economo - consegnatario con la collaborazione degli amministratori di sistema, mantiene un elenco, da aggiornare con cadenza almeno semestrale, di tutte le attrezzature informatiche dell'ufficio, dello scopo cui sono destinate, della loro collocazione fisica, delle misure di sicurezza su di esse adottate e delle eventuali misure di adeguamento pianificate.

3.2 Il responsabile del trattamento individua i volumi logici o le aree di disco da sottoporre a *backup*, sui vari *server.*

3.3 Compatibilmente con le risorse informatiche dell'ufficio, a ciascun utente viene assegnata una *directory*, in un'area disco di un s*erver* che sia sottoposta a *backup*, dove conservare i dati che debbono essere

mantenuti in maniera sicura. L'accesso a queste *directory* è consentita esclusivamente all'utente proprietario, nonché agli incaricati del *backup*.

3.4 Il responsabile del trattamento individua, tra gli amministratori di sistema, uno o più incaricati del *backup.*

3.5 Laddove il *backup* venga effettuato localmente nell'ambito dell'ufficio, gli incaricati effettuano le seguenti operazioni:

a) esecuzione quotidiana del *backup*, eventualmente attraverso procedure automatiche;

b) verifica almeno settimanale della corretta esecuzione dei backup;

c) mantenimento di un elenco dei *backup* effettuati;

d) archiviazione dei supporti secondo le disposizioni della sezione a)1.5;

e) verifica, con cadenza almeno mensile, della procedura di *recovery* dai supporti di *backup;*

f) effettivo ripristino dei dati in caso di necessità.

4. Sistema di monitoraggio

4.1 Deve essere messo in atto un processo di controllo e verifica della sicurezza del sistema informatico, attraverso l'utilizzo di appositi strumenti a livello di sistema, di gestione delle basi e di applicazioni.

4.2 Il sistema di controllo deve registrare:

a) gli accessi, riusciti e falliti, a livello di sistema, di base e di applicativo;

b) gli accessi in lettera e scrittura attraverso il sistema di gestione delle basi dati;

c) tutti gli accessi in lettura e scrittura ai singoli archivi.

4.3 Il responsabile del trattamento individua, tra gli amministratori di sistema, uno o più incaricati della verifica delle registrazioni di cui al punto 4.2.

4.4 Le operazioni di verifica delle registrazioni debbono essere effettuate almeno settimanalmente. I problemi riscontrati vanno riportati al responsabile del trattamento che, di concerto con il Presidente della Corte, individuerà le opportune contromisure.

4.5 L'individuazione delle responsabilità connesse a modifiche o letture non autorizzate viene effettuata, sulla registrazione di cui alla lettera 4.2c), su richiesta del responsabile del trattamento o del Presidente della Corte.

4.6 Con cadenza annuale, il responsabile del trattamento conferisce a uno o più degli amministratori di sistema l'incarico di stilare un

rapporto relativo all'applicazione delle norme contenute nel Documento programmatico sulla sicurezza dei dati.

D. Criteri e procedure per la sicurezza delle trasmissioni dei dati, ivi compresi quelli per le restrizioni di accesso per via telematica

Sul collegamento dell'ufficio verso la Rete Giustizia è installato un apparato di controllo (*firewall*).
Al firewall spetta il compito d'individuare cosa può passare all'interno della rete Giustizia e cosa deve essere bloccato. Per ampliare i parametri di sicurezza della RUG, tutti i Palazzi di Giustizia sono dotati di un proprio *firewall*. Il *firewall è* configurato in maniera da permettere alle postazioni di lavoro interne all'ufficio di accedere solo ai servizi disponibili sulla rete di interesse dell'utente, bloccando gli eventuali tentativi di accesso non autorizzati provenienti dall'esterno verso l'ufficio.
Qualora un ufficio voglia rendere disponibili o accedere ai servizi di altri uffici dell'Amministrazione della Giustizia (tipicamente l'accesso ad applicativi ministeriali), deve richiedere all'ufficio preposto della Direzione Generale per i Sistemi Informativi Automatizzati (il Centro *Firewall* di Napoli) l'apertura dei canali di comunicazione necessari.

E. Criteri per la conservazione dei fascicoli cartacei negli uffici di segreteria e cancelleria e per l'accesso ad esse da parte di terzi

5. Conservazione e trasporto dei fascicoli processuali

5.1 I fascicoli processuali devono rimanere in armadi chiusi e, quando ciò non è possibile, devono essere custoditi con le copertine rovesciate, per non rendere leggibili i dati ad eccezione del numero di RG.

5.2 La consegna dei fascicoli in visione, o per il rilascio di copia, deve avvenire solo nei confronti delle parti o dei difensori aventi diritto e sotto il controllo del personale addetto.

5.3 Gli armadi contenenti fascicoli o documenti processuali, eventualmente collocati nei corridoi e/o in aree cui è consentito il libero accesso del pubblico, devono essere chiusi a chiave; se con ante a vetri, deve essere predisposta la schermatura al fine di evitare la visione dei dati oppure le copertine devono essere rovesciate, per non rendere leggibili i dati, lasciando sulla copertina stessa solo il numero di RG.

5.4 I fascicoli cartacei, nelle fasi di trasporto all'interno dell'ufficio, devono permanere nei corridoi il tempo strettamente necessario alla loro consegna.

6. Richiesta e rilascio di copie

Nei casi in cui la richiesta di copia sia rivolta in cancelleria, le copie vengono rilasciate su istanza presentata attraverso la compilazione di un apposito modulo e sono estratte dal personale di cancelleria, previa escussione dei diritti di copia previsti dal testo unico sulle spese di giustizia.

7. Accesso alle cancellerie

Le cancellerie e gli uffici maggiormente frequentati dal pubblico devono dotarsi di sportelli front-office; in difetto, l'ingresso va limitato a una persona per volta bloccando l'accesso diretto alle scrivanie degli impiegati in modo da evitare la visione occasionale degli atti d'ufficio da parte di soggetti non legittimati. Massima cautela deve esser utilizzata nella custodia di tutti i fascicoli relativi a procedimenti riguardanti minori.

8. Fascicoli personali dei magistrati

8.1 I fascicoli personali dei magistrati ordinari, anche in tirocinio, e onorari sono custoditi in armadi chiusi a chiave e con ante non trasparenti; i dati personali devono essere conservati separatamente rispetto alle altre informazioni negli stessi contenute, in apposita stanza chiusa a chiave.

8.2 Le cartelle sanitarie e di rischio previste dall'art. 41 d.lgs. 9 aprile 2008 n. 81 e la documentazione relativa alla fissazione delle visite mediche deve essere conservata in armadi chiusi a chiave. L'accesso alle cartelle e alla restante documentazione è consentito esclusivamente agli organi di vigilanza ed al medico competente.

8.3 I fascicoli relativi ad esposti, congedi ordinari e straordinari, procedimenti disciplinari e pre-disciplinari dei magistrati sono custoditi in armadi chiusi a chiave e con ante non trasparenti in apposita stanza chiusa a chiave.

8.4 I responsabili/coordinatori di settore verificano che gli incaricati del trattamento, durante le relative operazioni di gestione dei dati, compresa la fase di archiviazione, utilizzino tutte le misure idonee a mantenere la riservatezza dei dati personali.

8.5 I responsabili e gli incaricati del trattamento dei dati relativi all'attività del Consiglio giudiziario adottano le necessarie misure per assicurare la

riservatezza dei dati personali sia nella fase di gestione che di archiviazione informatica e cartacea dei dati stessi.

8.6 I dati riguardanti l'attribuzione dei buoni pasto sono custoditi in luogo riservato ed accessibile solo agli incaricati del trattamento dei dati ed utilizzati esclusivamente per le richieste di fornitura e per eventuali adempimenti statistici.

9. Fascicoli personali dei dipendenti amministrativi

9.1 I fascicoli personali dei dipendenti sono custoditi in armadi chiusi a chiave e con ante non trasparenti; i dati personali devono essere conservati separatamente rispetto alle altre informazioni negli stessi contenute.

9.2 Le cartelle sanitarie e di rischio previste dall'art. 41 d.lgs. 9 aprile 2008 n. 81 e la documentazione relativa alla fissazione delle visite mediche deve essere conservata in armadi chiusi a chiave. L'accesso alle cartelle e alla restante documentazione è consentito esclusivamente agli organi di vigilanza ed al medico competente.

9.3 Ulteriori indicazioni per la tutela dei dati personali riguardanti il personale:

- i responsabili/coordinatori di settore verificano che gli incaricati del trattamento, durante le relative operazioni di gestione dei dati, compresa la fase di archiviazione, utilizzino tutte le misure idonee a mantenere la riservatezza dei dati personali;
- le medesime misure sono adottate per i procedimenti riguardanti la gestione delle visite mediche, da qualunque disposizione previste (visite fiscali, collegiali, visite periodiche ai sensi del d.lgs. 81/2008, visite per esiti infortuni sul lavoro, ecc.), per la formazione obbligatoria e per l'attività di recupero somme nei confronti di terzi a seguito di incidenti che vedano coinvolti dipendenti dell'Amministrazione;
- i fascicoli personali dei dipendenti e quelli comunque contenenti dati personali, quali la corresponsione di emolumenti accessori, sono conservati in spazi accessibili solo agli addetti, in armadi chiusi a chiave e la chiave è custodita dal responsabile del servizio;
- eventuali elenchi contenenti la tipologia delle assenze dei dipendenti e relativa documentazione sono analogamente conservati in spazi riservati ed i relativi dati possono essere diffusi solo in forma anonima/aggregata, per adempimenti statistici;
- i dati riguardanti l'attribuzione dei buoni pasto sono custoditi in luogo riservato ed accessibile solo agli incaricati del trattamento dei dati ed utilizzati esclusivamente per le richieste di fornitura e per eventuali adempimenti statistici;

- i "fogli-firma" devono essere mantenuti in cartelle chiuse che non ne consentano la visione agli utenti, così come la cartella nella quale i dipendenti depositano le loro istanze, in attesa che vengano acquisite dal dipendente che gestisce il sistema di rilevazione delle presenze;
- i dati relativi alla gestione delle presenze del personale vengono trattati esclusivamente dagli addetti, sotto la vigilanza del responsabile, compreso l'accesso al sistema informatizzato di gestione, dal quale ciascun dipendente deve poter ricavare esclusivamente le informazioni che lo riguardano.

F. Criteri per la protezione dei dati personali nelle udienze e nella diffusione dei provvedimenti

10. Ruoli di udienza e citazione dei testi

10.1 L'affissione dei ruoli d'udienza deve avvenire con i dati personali oscurati o comunque senza nomi delle parti.

10.2 Nei casi di decreti di citazione cumulativi dei testi deve provvedersi all'oscuramento delle generalità e degli altri dati identificativi dei testi non destinatari della comunicazione in modo da pervenire, in fatto, al confezionamento di un provvedimento individuale.

11. Trattamento dei dati nei provvedimenti e loro diffusione

11.1 L'accessibilità alle decisioni dell'autorità giudiziaria deve avvenire nel rispetto degli artt. 51[1] e 52[2] D.lgs. 30 giugno 2003, n. 196.

---

[1] Art. 51 D.lgs 196/2003: *"1. Fermo restando quanto previsto dalle disposizioni processuali concernenti la visione e il rilascio di estratti e di copie di atti documenti, i dati identificativi delle questioni pendenti dinanzi all'autorità giudiziaria di ogni ordine e grado sono resi accessibili a chi vi abbia interesse anche mediante reti di comunicazione elettronica, ivi compreso il sito istituzionale della medesima autorità nella rete Internet. 2. Le sentenze e le altre decisioni dell'autorità giudiziaria di ogni ordine e grado depositate in cancelleria o segreteria sono rese accessibili anche attraverso il sistema informativo e il sito istituzionale della medesima autorità nella rete Internet, osservando le cautele previste dal presente capo".*

[2] Art 52 D.lgs. 196/2003: *"1.Fermo restando quanto previsto dalle disposizioni concernenti la redazione e il contenuto di sentenze e di altri provvedimenti giurisdizionali dell'autorità giudiziaria di ogni ordine e grado, l'interessato può chiedere per motivi legittimi, con richiesta depositata nella cancelleria o segreteria dell'ufficio che procede prima che sia definito il relativo grado di giudizio, che sia apposta a cura della medesima cancelleria o segreteria, sull'originale della sentenza o del provvedimento, un'annotazione volta a precludere, in caso di riproduzione della sentenza o provvedimento in qualsiasi forma, per finalità di informazione giuridica su riviste giuridiche, supporti elettronici o mediante reti di comunicazione elettronica, l'indicazione delle generalità e di altri dati identificativi del medesimo interessato riportati*

11.2 Al di fuori dei casi di anonimizzazione obbligatoria previsti dall'art. 52 comma 5 D.lgs. 196/2003[3], ogni interessato può chiedere per motivi legittimi, prima della definizione del relativo grado di giudizio, che sull'originale della sentenza o del provvedimento sia apposta un'annotazione sull'anonimizzazione. I magistrati sono invitati in ogni caso a valutare l'opportunità di disporre d'ufficio l'anonimizzazione a tutela dei diritti o della dignità degli interessati. Nei casi di oscuramento su istanza di parte o su ordine del giudice nel provvedimento deve essere inserita l'annotazione: "Ai sensi dell'art. 52 comma 3 D.lgs.

sulla sentenza o provvedimento. 2. Sulla richiesta di cui al comma 1 provvede in calce con decreto, senza ulteriori formalità, l'autorità che pronuncia la sentenza o adotta il provvedimento. La medesima autorità può disporre d'ufficio che sia apposta l'annotazione di cui al comma 1, a tutela dei diritti o della dignità degli interessati. 3. Nei casi di cui ai commi 1 e 2, all'atto del deposito della sentenza o provvedimento, la cancelleria o segreteria vi appone e sottoscrive anche con timbro la seguente annotazione, recante l'indicazione degli estremi del presente articolo: "In caso di diffusione omettere le generalità e gli altri dati identificativi di....". 4. In caso di diffusione anche da parte di terzi di sentenze o di altri provvedimenti recanti l'annotazione di cui al comma 2, o delle relative massime giuridiche, è omessa l'indicazione delle generalità e degli altri dati identificativi dell'interessato. 5. Fermo restando quanto previsto dall'articolo 734 bis del codice penale relativamente alle persone offese da atti di violenza sessuale, chiunque diffonde sentenze o altri provvedimenti giurisdizionali dell'autorità giudiziaria di ogni ordine e grado è tenuto ad omettere in ogni caso, anche in mancanza dell'annotazione di cui al comma 2, le generalità, altri dati identificativi o altri dati anche relativi a terzi dai quali può desumersi anche indirettamente l'identità di minori, oppure delle parti nei procedimenti in materia di rapporti di famiglia e di stato delle persone. 6. Le disposizioni di cui al presente articolo si applicano anche in caso di deposito di lodo ai sensi dell'articolo 825 del codice di procedura civile. La parte può formulare agli arbitri la richiesta di cui al comma 1 prima della pronuncia del lodo e gli arbitri appongono sul lodo l'annotazione di cui al comma 3, anche ai sensi del comma 2. Il collegio arbitrale costituito presso la camera arbitrale per i lavori pubblici ai sensi dell'articolo 209 del codice dei contratti pubblici di cui al decreto legislativo 18 aprile 2016, n. 50, provvede in modo analogo in caso di richiesta di una parte. 7. Fuori dei casi indicati nel presente articolo è ammessa la diffusione in ogni forma del contenuto anche integrale di sentenze e di altri provvedimenti giurisdizionali".

[3] E' opportuno richiamare l'interpretazione fornita dal Primo Presidente della Corte di Cassazione nel proprio decreto n. 178/2016, laddove ha evidenziato la necessità di anonimizzare, nel settore penale, tutti i provvedimenti resi nei procedimenti concernenti reati contro la famiglia (artt. da 556 a 574-*bis* c.p.), reati di cui agli artt . 414-*bis* e 416, settimo comma, c.p., reati di cui all'art. 591 c.p., reati di cui agli artt. da 600-*bis* a 600-*octies* e da 609-*bis* a 609-*undecies* c.p., reati di cui all'art . 643 c.p., reati di cui all'art. 734-*bis* c.p., reati in tema di prostituzione, reati in materia di interruzione volontaria della gravidanza, reati in materia di procreazione medicalmente assistita e reati commessi da o in danno di minorenni. In queste ipotesi, secondo quanto previsto dal decreto in questione, l'oscuramento «deve riguardare non solo i dati identificativi dell'interessato, ma ogni altro dato, anche relativo a terzi, tramite il quale si possa risalire anche direttamente alla sua identità». Nel settore civile, secondo il richiamato provvedimento, l'anonimizzazione deve riguardare i provvedimenti resi nei procedimenti riguardanti le materie dell'adozione, dell'assistenza ai minori, della capacità della persona fisica, della delibazione di sentenze straniere, della famiglia, dell'interruzione di gravidanza, della responsabilità civile, del lavoro privato, dello stato civile: cfr. A. Centonze, "La protezione dei dati personali nei provvedimenti della Corte di Cassazione", in "Il trattamento dei dati personali in ambito giudiziario", Quaderno n. 5/2021 della Scuola Superiore della Magistratura, pagg. 98-100

196/2003 in caso di diffusione omettere le generalità e gli altri dati identificativi di …".

11.3 Per interessato deve intendersi qualsiasi persona identificata o identificabile dalla decisione dell'autorità giudiziaria[4].

11.4 I magistrati sono invitati a richiamare, nel caso di conferimento di incarichi a c.t.u./periti, l'osservanza delle Linee guida in materia di trattamento di dati personali da parte dei consulenti tecnici, periti e ausiliari del giudice e del pubblico ministero (Deliberazione n. 46 del 26 giugno 2008 - Gazzetta Ufficiale n. 178 del 31 luglio 2008), vigilando sull'osservanza degli obblighi relativamente al reperimento ed utilizzo di dati personali, limitato all'incarico conferito e al tempo di svolgimento dello stesso, ed alla necessità di assicurare idonee modalità di conservazione, con divieto di divulgazione esteso anche agli eventuali collaboratori e ausiliari del perito o consulente.

G. Criteri per assicurare l'osservanza degli obblighi in materia di trattamento dei dati personali da parte del personale esterno

Tutto il personale esterno all'amministrazione che, a vario titolo, svolge attività negli uffici deve sottoscrivere una dichiarazione di responsabilità, con la quale si impegna al mantenimento del segreto di ufficio e al rispetto delle previsioni del codice in materia di protezione dei dati personali e del presente documento, con l'allegato manuale operativo.

Il presente documento e l'allegato manuale operativo generale dei dati personali vengono pubblicati sul sito della Corte.

[4] Lo si desume dalla definizione di dato personale dell'art. 4 n. 1) Regolamento (UE) 2016/679. Si evidenzia che il 14° considerando del Regolamento (UE) 2016/679 stabilisce: *"È opportuno che la protezione prevista dal presente regolamento si applichi alle persone fisiche, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al trattamento dei loro dati personali. Il presente regolamento non disciplina il trattamento dei dati personali relativi a persone giuridiche, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto".*

Sicurezza significa anche integrità, esattezza e aggiornamento dei dati, nonché trattamenti leciti e conformi alle finalità della raccolta.

1. Uso degli strumenti del trattamento

a) **Telefono**: nel caso di richieste d'informazioni da parte di terzi può essere necessario, a seconda della natura dei dati richiesti, procedere nel seguente modo:
- chiedere l'identità del chiamante e la motivazione della richiesta;
- richiedere il numero di telefono da cui l'interlocutore sta effettuando la chiamata;
- verificare che il numero di telefono dichiarato corrisponda effettivamente a quello del chiamante;
- procedere immediatamente a richiamare la persona che ha richiesto le informazioni, con ciò accertandosi della identità dichiarata in precedenza;

b) **Fax**: nell'utilizzare questo strumento residuale, vietato nella comunicazione di documenti tra pubbliche amministrazioni dall'artt. 47 d.lgs. 7 marzo 2005, n. 82, occorre prestare attenzione, in particolar modo, nel caso in cui vengano inviati documenti contenenti dati personali:
- digitare correttamente il numero di telefono, cui inviare la comunicazione;
- controllare l'esattezza del numero digitato prima di premere il tasto invio;
- verificare che non vi siano inceppamenti della carta o che non vengano presi più fogli;
- attendere la stampa del rapporto di trasmissione, verificando la corrispondenza del numero di pagine da inviare con quelle effettivamente inviate;
- qualora vengano trasmessi dati idonei a rivelare lo stato di salute, può essere opportuno anticipare l'invio chiamando il destinatario

della comunicazione al fine di assicurare il ricevimento nelle mani del medesimo, evitando che terzi estranei o non autorizzati conoscano il contenuto della documentazione inviata;

- tenuto conto della della natura dei dati trasmessi, può essere opportuno richiedere una telefonata di conferma della corretta ricezione e leggibilità del contenuto del fax;

c) **Scanner**: gli incaricati preposti all'acquisizione ottica della documentazione contenente dati personali devono verificare che l'operazione avvenga correttamente e il contenuto sia leggibile; qualora vi siano errori di acquisizione ovvero si verifichino anomalie, procedere alla ripetizione delle operazioni;

d) **Distruzione delle copie cartacee e delle stampe**: tutti coloro che provvedono alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche), in caso di copia erronea o non correttamente leggibile, qualora possano essere desunti dati personali riferiti ad un interessato determinato, sono tenuti a procedere alla distruzione del supporto, in modo da escludere la possibilità, da parte di estranei, di venire a conoscenza dei dati medesimi, anche utilizzando un apparato elettrico distruggi-documenti (shredder). In ogni caso non devono gettarsi documenti cartacei senza averli prima fatti a pezzi (sminuzzati in modo da non essere ricomponibili e che non sia possibile riconoscere contenuto e/o provenienza);

e) **Riutilizzo dei supporti di memorizzazione dei dati**: per poter riutilizzare i supporti di memorizzazione di dati (ad esempio chiavette USB, floppy-disk, CD-ROM, dvd-rom) si deve procedere alla cancellazione dei dati precedentemente registrati, in modo da evitare che soggetti terzi possano conoscere o comunque risalire alle informazioni memorizzate in precedenza;

2. Istruzioni in tema di sicurezza

a) Sicurezza del software

Presso ciascun Ufficio è consentita l'installazione delle seguenti tre categorie di software sempreché autorizzata dal DGSIA: a) Software

commerciale, dotato di licenza d'uso; b) Software realizzato specificamente per l'Amministrazione a livello nazionale; c) Software eventualmente realizzato per l'Ufficio a livello locale.

L'installazione di software diversi da quelli indicati va autorizzato dal responsabile del trattamento.

La conformità dei software di cui alle lettere b) e c) viene di norma certificata dall'Ufficio del Responsabile per i Sistemi Informativi Autorizzati.

Il software deve essere installato solo da supporti fisici originali o dei quali sia nota la provenienza da parte del personale tecnico.

Tramite l'Ufficio del Responsabile per i Sistemi Informativi Autorizzati si provvede alla distribuzione di un software antivirus aggiornato su tutto il territorio.

In mancanza di procedure d'installazione automatiche, il responsabile del trattamento garantisce l'effettuazione delle installazioni del software antivirus su tutte le posizioni di lavoro, con cadenza almeno semestrale.

Non è consentito l'utilizzo di dispositivi rimovibili (chiavette USB, ecc.) di proprietà di persone estranee all'amministrazione (avvocati e parti private).

b) Spegnere il PC in caso di assenza dall'ufficio per un periodo di tempo lungo

Lasciare un computer acceso non crea problemi al suo funzionamento e al contrario velocizza il successivo accesso. Tuttavia, 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. Può essere utilizzato il comando sospendi (tasti win + L oppure selezionare "start", "arresta" e " sospendi") in caso di assenza prolungata dalla postazione.

c) Password

L'accesso ad internet avviene dall'Ufficio tramite intranet ovvero la rete del DOMINIO Giustizia. Grazie a intranet è possibile accedere alla quasi totalità dei servizi ministeriali. Per motivi di sicurezza l'accesso è filtrato da un "proxy server" ovvero un intermediario, che funge da guardiano del dominio rispetto ad attacchi che possono venire da internet e regola anche il tipo di utilizzo che gli utenti del DOMINIO possono fare delle risorse

internet. Il proxy consente di presentare il DOMINIO Giustizia a Internet, mettendo a disposizione degli utenti attestati alla rete geografica del ministero (RUG) l'accesso al World Wide Web.

Gli utenti del DOMINIO Giustizia sono individuati tramite le credenziali ADN, acronimo di Active Directory Nazionale ovverosia il sistema che riconosce l'identificativo univoco, costituito dal nome utente (nome.cognome) e da una password, unica per tutti gli accessi, posta elettronica, internet e pc migrati in ADN. Tutto il personale del Ministero della Giustizia ha una propria utenza ADN. Esiste la possibilità di assegnare le credenziali ADN anche a personale esterno all'Amministrazione (in via esemplificativa, al personale della polizia giudiziaria e ai tecnici dell'assistenza esterna).

Il processo di autenticazione consente di ottenere uno specifico insieme di privilegi di accesso ed utilizzo, denominato profilo, rispetto alle risorse del sistema informatico. A ciascun profilo è associato un gruppo di utenti, che condividono gli stessi privilegi di accesso e utilizzo.

La creazione della password di accesso al dominio deve rispettare le regole previste a livello nazionale e diffuse dalla DGSIA. Di tali regole occorre prendere visione all'atto dell'invio della mail dalla casella supportosistemico.dgsia@giustizia.it e in occasione del periodico cambio password tramite il sito https://pst.giustizia.it/

Se la password è scaduta e non è reperita la mail di avviso, la modifica della password va effettuata presso il seguente sito, seguendo le istruzioni per la scelta della nuova password: https://pst.giustizia.it/

Al momento della redazione del presente documento, per la formulazione di una nuova password, la DGISIA prescrive le seguenti regole:

- lunghezza minima 8 (otto) caratteri (massima a piacere);
- presenza obbligatoria di maiuscole, minuscole, numeri;
- impossibilità di inserire parti consistenti del nome o del cognome;
- impossibilità di riutilizzare le 8 password precedentemente utilizzate.

La password ha una durata di 180 gg. Se l'utente inserisce erroneamente per tre volte consecutive le proprie credenziali l'account viene bloccato per un certo lasso di tempo.

Vengono forniti i seguenti ulteriori suggerimenti e raccomandazioni con riferimento alla formulazione di una parola chiave:

- deve essere abbastanza lunga (almeno 8 caratteri) perché più aumenta il numero dei caratteri più la password diventa "robusta" (è suggerito l'utilizzo di 15 caratteri);
- deve contenere caratteri di almeno 4 diverse tipologie, da scegliere tra: lettere maiuscole, lettere minuscole, numeri, caratteri speciali (cioè punti, trattino, underscore, ecc.);
- non deve contenere riferimenti personali facili da indovinare (nome, cognome, data di nascita, ecc.). Non deve nemmeno contenere riferimenti al nome utente (detto anche user account, alias, user id, user name);
- non deve corrispondere a password già utilizzate in passato;
- non deve essere divulgata o comunicata a terzi;
- deve essere conservata in luogo segreto e non deve essere trascritta in foglietti appesi al monitor ovvero conservati nel cassetto della propria scrivania. Non scrivere mai le password su biglietti conservati nel portafoglio oppure in file non protetti su dispositivi personali (computer, smartphone o tablet);
- non deve contenere parole "da dizionario", cioè parole intere di uso comune: è meglio usare parole di fantasia oppure parole "camuffate" per renderle meno comuni, magari interrompendole con caratteri speciali (ad esempio: caffè può diventare caf-f3). Esistono software programmati per tentare di indovinare e rubare le password provando sistematicamente tutte le parole di uso comune nelle varie lingue, e con questa accortezza si può rendere il loro funzionamento più complicato;
- deve essere periodicamente cambiata, soprattutto per i profili più importanti o quelli che usi più spesso (e-mail, e-banking, social network, ecc.). È preferibile password diverse per account diversi (e-mail, social network servizi digitali di varia natura, ecc.). In caso di «furto» di una

password si evita così il rischio che anche gli altri profili che ti appartengono possano essere facilmente violati.

Occorre ricordare che le eventuali password temporanee rilasciate da un sistema o da un servizio informatico vanno sempre immediatamente cambiate, scegliendone una personale.

Evitare di condividere le password via e-mail, sms, social network, instant messaging, etc. Anche se le comunicate a persone conosciute, le credenziali potrebbero essere diffuse involontariamente a terzi o sottratte da malintenzionati.

Se usate pc, smartphone o altri dispositivi di terzi, evitate sempre che possano conservare in memoria le password da voi utilizzate.

Qualora sia necessario accedere ai dati di un utente per lungo tempo assente dall'ufficio, l'intervento del tecnico richiede la password di amministratore del PC e con essa è possibile avere accesso a tutti i dati archiviati sull'hard disk e ai messaggi di posta elettronica ricevuti e inviati alla data di spegnimento del PC. Non è però possibile agire per conto dell'utente oppure collegarsi alle relative risorse di rete o violare la privacy dell'utente medesimo.

d) **Antivirus**

La DGSIA provvede alla distribuzione di software antivirus aggiornati su tutto il territorio attraverso la piattaforma di ADN in modo che tutte le postazioni siano protette da attacchi informatici esterni.

Esiste la possibilità di verificare i messaggi sospetti in entrata nella propria casella di posta elettronica, trattenuti nella c.d. quarantena (fra questi risulteranno i messaggi con allegati protetti da password, con allegati contenenti file office con macro,…) con la possibilità, laddove attendibili, di consentirne la consegna al proprio indirizzo di posta. Il sistema invia periodicamente un report con l'elenco delle mail sospette bloccate in ingresso, ma l'accesso all'area di quarantena per il rilascio delle mail attendibili può avvenire, da parte dell'utente, in ogni momento.

In mancanza di procedure automatiche, ad esempio dovute alla non attestazione del PC sull'Active Directory Nazionale, l'aggiornamento viene

scaricato tramite la RUG dai tecnici informatici con cadenza almeno mensile.

Non è sufficiente scaricare l'aggiornamento dell'antivirus. Occorre, ogni volta che viene scaricata una versione aggiornata, provvedere alla scansione dell'intero sistema al fine di verificare la presenza di virus.

e) Utilizzo di screen-saver

In caso di assenza, anche momentanea, dalla propria postazione di lavoro, devono essere adottate misure atte a escludere che soggetti non autorizzati possano acquisire informazioni o accedere ai dati trattati con strumenti elettronici. A tal proposito, a titolo meramente esemplificativo, si consiglia di adottare un sistema di oscuramento (cd. *screen-saver*) dotato di password, ovvero di uscire dal programma che si sta utilizzando, ove sia protetto da parola chiave, ovvero, in alternativa, spegnere l'elaboratore che si sta utilizzando.

f) Salvataggi automatici

Molti programmi applicativi, come quelli di videoscrittura, salvano automaticamente il lavoro a intervalli fissi, in modo da minimizzare il rischio di perdita accidentale dei dati. Imparate comunque a salvare manualmente il lavoro con una certa frequenza, in modo da prendere l'abitudine di gestire voi stessi i dati e non fare esclusivo affidamento sul sistema. La regola generale è quella di procedere al backup periodico dei dati su supporti esterni (ottico o di altro tipo) o su cartelle ospitate sui server, misure di sicurezza che devono essere eseguite da ogni utente, anche per evitare che la rottura o il malfunzionamento dell'hard disk comprometta il lavoro e causi la perdita dei dati.

g) Custodia supporti rimovibili

I supporti rimovibili (chiavette USB, CD-ROM, dvd-rom, ecc.) devono essere custoditi in modo da evitare l'utilizzo da parte di soggetti non autorizzati. È consigliato riporli in un contenitore munito di serratura ovvero nel cassetto della scrivania di lavoro, avendo cura di chiudere il cassetto a fine giornata.

h) **Non riutilizzate supporti rimovibili (CD, pen-drive, etc.) per affidare a terzi i vostri dati**

Quando un file viene cancellato da un disco magnetico, i dati non vengono effettivamente eliminati dal disco ma soltanto marcati come non utilizzati e sono facilmente recuperabili. Neanche la formattazione assicura l'eliminazione dei dati dai dischi. Solo l'uso di appositi programmi garantisce che sul dischetto non resti traccia dei dati precedenti. Se ciò non è possibile, essi devono essere distrutti e comunque è sempre meglio usare un dischetto nuovo.

i) **Sostituzione, assegnazione ad altro utente o dismissione del personal computer**

È necessario provvedere alla rimozione irreversibile di tutti i dati dall'apparecchiatura oggetto dell'operazione. La rimozione va effettuata dopo l'avvenuta copia dei dati su un opportuno supporto di memorizzazione (hard disk di un nuovo PC, se si tratta di una sostituzione di PC oppure su CD, DVD, etc.) da consegnare all'utente.

j) **Assistenza hardware per riparazione del personal computer**

Qualora l'impresa incaricata della riparazione ritenesse opportuno, per i necessari controlli, trasferire il personal computer presso i propri laboratori, nel rispetto delle politiche di sicurezza deve essere adottata una delle seguenti precauzioni:

• l'estrazione dal PC del supporto di memorizzazione magnetica (hard disk) contenente i dati dell'utente; custodia del supporto da parte dell'utente; successiva reinstallazione sul PC nel momento della restituzione;

• operare come se si trattasse di una sostituzione o riassegnazione nel caso in cui fosse necessario consegnare anche l'hard disk contenente dati personali.

k) **Gestione dello spam**

Sono da considerare spam (messaggio pubblicitario non richiesto) le e-mail inviate a un numero molto elevato di utenti di Internet tramite posta elettronica, nonché i messaggi contenenti link personali (il c.d. *phishing*) atti a carpire informazioni riservate dell'utente o che possono infettare con

virus le postazioni dì lavoro. Quasi tutti gli incidenti più importanti sono causati da pratiche errate o semplici errori degli utenti, come apertura di allegati e-mail sospetti o installazione di software non autorizzato. Una non attenta navigazione sul web può portare a selezionare banner pubblicitari ingannevoli e quindi a eseguire codici malevoli. Da non sottovalutare la pratica dello *spear phishing* che, a differenza del *phishing* generico, è concepito per risultare più rilevante per il contesto sociale-lavorativo di una specifica vittima, la quale riceve tipicamente una sollecitazione verso un link o un file attraverso e-mail apparentemente provenienti da persone conosciute o via messaggi istantanei, strumenti la cui popolarità è in forte aumento.

Eventuali messaggi di *phishing* possono essere inoltrati alla casella della D.G.S.I.A. (antispam.dgsia@giustizia.it), dove i tecnici preposti provvederanno a inserire l'indirizzo da cui proviene la mail in una lista d'indirizzi che non possono superare i controlli del *firewall*.

l) Collegamento dei portatili alla rete giustizia

Al personale in possesso di personal computer portatili è richiesto, con cadenza periodica, di collegare le apparecchiature alla rete di giustizia per permettere la scansione con l'antivirus aggiornato dell'Amministrazione.

3. Linee guida per la sicurezza

Utilizzate le chiavi

Il primo livello di protezione di qualunque sistema è quello fisico e pertanto, ove possibile, ricordarsi di chiudere a chiave l'ufficio alla fine della giornata e chiudere i documenti a chiave nei cassetti ogni volta che potete.

Utilizzate le password

Vi sono diverse categorie di password, ognuna con diversa funzione:

a) la **password di accesso al computer** impedisce l'utilizzo improprio della vostra postazione, quando per un motivo o per l'altro non vi trovate in ufficio;

b) la **password di accesso alla rete** impedisce che l'eventuale accesso non autorizzato a una postazione renda disponibili tutte le risorse presenti nella rete dell'ufficio;
c) la **password dei programmi specifici** permette di restringere l'accesso ai dati al solo personale autorizzato;
d) la **password del salvaschermo**, infine, impedisce che una vostra assenza momentanea permetta a una persona non autorizzata di visualizzare il vostro lavoro. Imparate a utilizzare questi quattro tipi fondamentali di password, e mantenete distinta almeno quella di tipo *a)*, che può dover essere resa nota, almeno temporaneamente, ai tecnici incaricati dell'assistenza.

Attenzione alle stampe di documenti riservati

Non lasciate accedere alle stampe persone non autorizzate. Se la stampante non si trova sulla vostra scrivania, recatevi quanto prima a ritirare le stampe. Distruggete personalmente le stampe quando non servono più.

Non lasciate traccia dei documenti riservati

Quando rimuovete un *file*, i dati non vengono effettivamente cancellati ma soltanto marcati come non utilizzati, e sono facilmente recuperabili. Neanche la formattazione assicura l'eliminazione dei dati; solo l'utilizzo di un programma apposito garantisce che sul dischetto non resti traccia dei dati precedenti. Nel dubbio, è sempre meglio usare un supporto nuovo.

Prestate attenzione nell'utilizzo di PC portatili

I PC portatili possono essere facilmente sottratti al legittimo proprietario. Se avete necessità di gestire dati riservati su un portatile, fatevi installare un buon programma di cifratura del disco rigido, e utilizzate una procedura di backup giornaliero.

Prestate attenzione quando digitate le password

Nonostante molti programmi non ripetano in chiaro la password sullo schermo, la password digitata potrebbe essere letta guardando i tasti che state battendo, anche se avete buone capacità di dattiloscrittura.

Non utilizzate apparecchi non autorizzati

L'utilizzo di modem o di chiavette con la medesima funzionalità su postazioni di lavoro collegate alla rete di edificio offre una porta d'accesso dall'esterno non solo al vostro computer, ma a tutta la rete dell'ufficio. È pertanto fatto divieto agli utenti di effettuare collegamenti telematici distinti da quelli previsti salvo autorizzazione del titolare del trattamento dei dati, sentito il parere dell'organo tecnico che dovrà essere informato sull'eventuale autorizzazione rilasciata.

Applicate con cura le linee guida per la prevenzione da infezioni di virus

La prevenzione dalle infezioni da virus sul computer è molto più facile e comporta uno spreco di tempo minore della correzione degli effetti di un virus. Tra l'altro sussiste il rischio d'incorrere in una perdita irreparabile di dati.

4. Linee guida per la prevenzione dei virus

Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi. Alcuni virus si limitano a riprodursi senza ulteriori effetti; altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido.

Come si trasmette un virus:

1. attraverso programmi provenienti da fonti non ufficiali;
2. attraverso le macro dei programmi di automazione d'ufficio.

Quando il rischio da virus aumenta:

1. quando s'installano programmi;
2. quando si copiano dati da dischetti;
3. quando si scaricano dati o programmi da Internet.

Quali effetti ha un virus:

1. effetti sonori e messaggi sconosciuti appaiono sul video;
2. nei menù appaiono funzioni extra finora non disponibili;
3. lo spazio disco residuo si riduce inspiegabilmente.

COME PREVENIRE I VIRUS

Usate soltanto programmi provenienti da fonti fidate

Copie sospette di programmi possono contenere virus o altro *software* dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato. Non utilizzate programmi non autorizzati, con particolare riferimento ai videogiochi spesso utilizzati per veicolare virus.

Assicuratevi di non far partire il vostro computer da cd rom, pen drive, etc.

Se il dischetto fosse infettato, facendo partire il computer da cd rom, chiavette etc. il virus si trasferirebbe nella memoria RAM e potrebbe espandersi ad altri files.

Assicuratevi che il vostro software antivirus sia aggiornato

La tempestività nell'azione di bonifica è essenziale per limitare i danni che un virus può causare; È fondamentale che il programma antivirus conosca gli ultimi aggiornamenti sulle "impronte digitali" dei nuovi virus. Questi file sono rilasciati, di solito, con maggiore frequenza rispetto alle nuove versioni dei motori di ricerca dei virus.

Non diffondete messaggi di dubbia provenienza

Se ricevete messaggi che avvisano di un nuovo virus pericoloso, ignorateli. Mail di questo tipo sono definite con terminologia anglosassone *hoax* (termine spesso tradotto con "bufala"). Il mittente può anche essere

un amico, un famigliare o un tecnico informatico. La falsa informazione potrebbe essere riportata come proveniente da Microsoft o altro noto produttore di software.

Non partecipate a "Catene di S. Antonio" e simili

Analogamente, tutti i messaggi che invitano a "diffondere la notizia quanto più possibile" sono *hoax*, anche se parlano della fame nel mondo, di un minore in fin di vita, di guadagni miracolosi o grande fortuna. Si tratta di *hoax* aventi spesso lo scopo di utilizzare indebitamente risorse informatiche. Si tratta di attività vietate dagli *standard* di Internet e potreste involontariamente collaborare alla loro diffusione. Quando si ricevono informazioni tramite posta elettronica o per altra via di nuovi virus, con richiesta di dare massima diffusione al messaggio, prima di effettuare qualunque operazione, occorre controllare che non si tratti di *hoax* con il Presidio CISIA o su un sito web specializzato, per evitare di diffondere informazioni che possano generare timori ingiustificati. È anche opportuno informare il Presidio CISIA affinché possa essere messo in allerta, fornire informazioni più corrette agli utenti ed eventualmente attivare una ricerca e/o blocco del mittente nel caso il fenomeno si ripeta.

Scelta delle password

Il più semplice metodo per l'accesso illecito a un sistema consiste nell'indovinare la password dell'utente legittimo. In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso protetto da password "deboli". La scelta di password "forti" è, quindi, parte essenziale della sicurezza informatica.

Cosa non fare

- **NON comunicate a nessuno la password**. Ricordate che lo scopo principale per cui usate una password è assicurare che nessun altro possa utilizzare vostre risorse o possa farlo a vostro nome;
- **NON annotate la password** in alcun luogo dove possa essere letta facilmente, soprattutto vicino al computer;
- **NON consentite a terzi** di osservare la password che inserite sulla tastiera;

- **NON scegliete password che si possano trovare in un dizionario**. Su alcuni sistemi è possibile "provare" tutte le password contenute in un dizionario per vedere quale sia quella giusta;
- **NON crediate che l'uso di parole straniere renda più difficile il lavoro di scoperta**. Chi vuole scoprire una password è dotato di molti dizionari delle più svariate lingue;
- **NON usate il vostro nome utente** perché è la password più semplice da indovinare;
- **NON usate password che possano in qualche modo essere legate a voi** come, in via esemplificativa, il vostro nome, quello di vostra moglie/marito, dei figli, del cane, date di nascita, numeri di telefono etc.

Cosa fare

- **modificate la password a intervalli regolari**, almeno una volta ogni 6 mesi. A seconda del tipo di sistema l'intervallo raccomandato per il cambio può andare da tre mesi fino a due anni;
- **usate password lunghe** e con le caratteristiche indicate al punto 2 c) del presente manuale;
- **utilizzate password distinte per sistemi con diverso grado di sensibilità**. In alcuni casi la password viaggia in chiaro sulla rete e possono essere quindi intercettate, per cui, oltre a cambiarla spesso, è importante che sia diversa per quella usata da sistemi "sicuri". Il tipo di password in assoluto più sicura è quella associata a un supporto di identificazione come un dischetto o una carta a microprocessore; la password utilizzata su un sistema di questo tipo non deve essere usata in nessun altro sistema.