Tribunale di Bergamo

MISURE MINIME DI SICUREZZA

(Codice in materia di protezione dei dati personali - D.Lgs 30/9/2003 n. 196: artt. 33 e 34)

Il Presidente del Tribunale

Visto il decreto legislativo 30 giugno 2003, n. 196, denominato **"Codice in materia di protezione dei dati personali";**
Visto l'art. 34 del Codice relativo ai trattamenti dei dati con strumenti elettronici e l'art. 35 relativo ai trattamenti senza l'ausilio di strumenti elettronici;
Ritenuto che negli archivi informatici e in quelli cartacei di questo Tribunale sono contenuti, per assolvere a compiti istituzionali, dati personali, sensibili e giudiziari, il cui trattamento deve essere sottoposto alle misure minime di sicurezza di cui agli artt. 34 e 35 del **Codice**;

DISPONE

Il trattamento dei dati effettuato con strumenti elettronici e il trattamento dei dati senza l'ausilio di strumenti elettronici è sottoposto alle seguenti misure minime di sicurezza per la protezione dei dati di cui ***al Documento*** *Programmatico sulla Sicurezza* in pari data.

TRATTAMENTI CON STRUMENTI ELETTRONICI

Vengono adottate le seguenti misure minime di sicurezza, nei modi previsti dall'ALLEGATO B del Codice

(Disciplinare Tecnico in materia di misure di sicurezza)

a) Autenticazione informatica:

L'autenticazione informatica per l'accesso alla workstation e/o al dominio di rete avviene solo ed esclusivamente mediante l'impostazione univoca di *Username* e correlata *Password* a sola conoscenza dell'utente che accede al sistema.
Nel caso di eventuale blocco dell'accesso alla workstation o ai servizi implementati nel dominio, sarà cura dell'Amministratore di sistema o dell'addetto all'assistenza sistemistica di provvedere alla assegnazione della nuova password ed all'eventuale sblocco dell'account.

b) Adozione di procedure di gestione delle credenziali di autenticazione:

L'autorizzazione alla creazione di nuovi utenti è rilasciata dal Responsabile del trattamento dei dati o da un suo delegato.
Gli utenti accedono alle workstations collegate alla rete locale solo se autenticati dal server di competenza.
Gli account di autenticazione alla rete con password avranno le seguenti caratteristiche:

- scadenza trimestrale della password;
- blocco dell'account nel caso di perdita del diritto di accesso;
- lunghezza minima di otto caratteri della password;
- utilizzo di almeno un carattere non alfabetico oppure di un misto di lettere minuscole e maiuscole;
- storicizzazione delle 3 ultime password inserite;
- alla scadenza della password saranno gli utenti stessi a poterla modificare;
- blocco dell'account dopo tre tentativi di accesso non riusciti: successiva richiesta di sblocco all'amministratore di sistema o al Presidio Sistemistica presso la Sala Server;
- connessione alla rete dalle ore 7,30 alle ore 20,00;

c) Utilizzazione di un sistema di autorizzazione:

L'autorizzazione all'accesso avviene tramite una procedura di autenticazione a più livelli che riconosce l'utente e lo abilita all'utilizzo delle risorse assegnate garantendo la giusta attribuzione ai diritti di accesso alle cartelle condivise per tutti gli utenti sui server, agli applicativi ed all'eventuali risorse del sistema messe a disposizione escludendo la possibilità d'accesso ad "everyone" ma solo a "domain user", tranne per casi particolari.

d) Aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici

Con cadenza almeno annuale devono essere aggiornati gli elenchi degli incaricati del trattamento (allegato A e allegato B del DPS).

e) Protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati ad accessi non consentiti e a determinati programmi informatici:

I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615 quinquies del codice penale sia mediante le procedure di autenticazione dell'utente sui servizi a disposizione sulla rete, sia mediante l'attivazione del programma antivirus in dotazione costantemente aggiornato.

Pertanto:

a) tutti i computers devono essere dotati di programmi antivirus residenti ed aggiornati periodicamente;

b) ogni PC viene automaticamente sottoposto a scansione antivirus all'accensione

ed ogni qual volta viene utilizzato un supporto informatico esterno;

d) all'atto della individuazione di un virus, questo viene immediatamente rimosso o posto in quarantena;

e) il personale è messo a conoscenza che la diffusione dei virus è punita dall'art. 615 quinquies del Codice Penale;

Al fine di non consentire l'accesso alle woorkstations ad estranei l'utente è tenuto:

1) ove sia possibile, a chiudere a chiave la porta del proprio ufficio e a tenere sotto chiave i propri documenti, indipendentemente dal supporto fisico utilizzato;
2) allontanandosi momentaneamente dalla postazione di lavoro, a chiudere le applicazioni attive ed a bloccare l'accesso alla stazione di lavoro;
3) al termine della giornata di lavoro, a spegnere la postazione;
4) ad assicurarsi dell'identità e delle autorizzazioni del personale che debba installare un nuovo software e che deve lavorare sulla propria postazione di lavoro;
5) a non utilizzare, su postazioni di lavoro collegate alla rete locale dell'ufficio, modem o altri strumenti di connessione con l'esterno;
6) a non installare sulla propria postazione di lavoro alcun programma non preventivamente autorizzato dal Responsabile del trattamento;
7) l'utente è tenuto a non diffondere messaggi di posta elettronica di provenienza dubbia.

f) Adozione di procedure per la custodia di copie di sicurezza e ripristino della disponibilità dei dati e dei sistemi:

Le procedure di salvataggio devono rispettare le regole seguenti:

- il backup viene effettuato con una frequenza giornaliera;
- per l'archiviazione devono essere utilizzati supporti per i quali l'operazione di scrittura non comporta una modifica permanente ed irreversibile delle caratteristiche del supporto stesso;
- le procedure di backup devono consentire, con frequenza almeno **annuale** una copia storica dei dati.

–Per le basi dati degli applicativi disponibili sui server si provvederà al backup giornaliero su **cassette Dat o altro.**

–Periodicamente viene effettuato su un server dedicato allo scopo, il ripristino e la verifica dell'ultimo backup della base dati.

–I supporti d'uso più frequenti, per motivi di maggiore funzionalità possono essere conservati in prossimità del luogo dove si effettua il salvataggio, ma in locali diversi.

–Per le basi dati di applicativi che non sono presenti sui server, ma su stazioni di lavoro dedicate, verranno predisposte all'occorrenza le più idonee procedure di backup che gli utenti dell'ufficio stesso dovranno eseguire periodicamente.

- In apposito locale, distante dalla sala server, in un armadio blindato ignifugo, sono conservati i supporti di archivio, nonché i backup a cadenza maggiore di una settimana.

–L'Amministratore di Sistema ha la responsabilità del controllo del corretto svolgimento delle procedure di salvataggio (backup) e del recupero dei dati (recovery), anche quando eseguite dall'assistenza sistemistica.

In particolare:

– garantisce l'effettiva messa in opera delle procedure di backup;

– verifica l'avvenuta esecuzione dei backup;
– mantiene un elenco delle operazioni di backup effettuate;
– archivia i supporti fisici;
- effettua, in caso di malfunzionamento, le procedure di recovery;
- effettua verifiche periodiche delle procedure di recovery;

Il ripristino dei dati di backup sui server è effettuato su apposita cartella, creata sul server di ***recovery disaster*** e verificata a cura dell'amministratore di sistema.

g) ***Documento Programmatico sulla Sicurezza***

Contestualmente al presente provvedimento è emanato il ***"Documento Programmatico sulla Sicurezza"***

TRATTAMENTI SENZA L'AUSILIO DISTRUMENTI ELETTRONICI

Vengono adottate le seguenti misure minime di sicurezza, nei modi previsti dall'ALLEGATO B del Codice *(Disciplinare Tecnico in materia di misure di sicurezza).*

Vengono adottate le seguenti modalità tecniche.

- ❑ Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.

- ❑ Nell'ambito dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati è redatta per settore e per ufficio, in relazione al tipo di incarico e del relativo profilo di autorizzazione.

- ❑ Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione, in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

- ❑ L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate.

In particolare vengono adottate le seguenti misure.

- ❑ I locali dei vari uffici e cancellerie devono essere sempre chiusi a chiave al termine della giornata di lavoro e ogni volta che ci si assenta dalla stanza.
- ❑ Possono accedere ai fascicoli, atti e documenti di ciascun ufficio o cancelleria solamente gli incaricati addetti rispettivamente allo stesso ufficio, secondo i rispettivi incarichi e competenze.
- ❑ Il registro cartaceo "PROTOCOLLO RISERVATO" della Presidenza deve essere custodito nell'armadio blindato presso la Segreteria della Presidenza, debitamente chiuso a chiave.
- ❑ I fascicoli personali dei magistrati togati e dei magistrati onorari devono essere conservati nei locali della Segreteria della Presidenza del Tribunale, all'interno di armadi metallici debitamente chiusi a chiave.
- ❑ I fascicoli personali del personale amministrativo devono essere conservati in locali in cui possano accedere solamente gli incaricati addetti all'Ufficio del Personale, all'interno di armadi metallici debitamente chiusi a chiave.
- ❑ Nel caso di spedizione ad altri uffici di documentazione sanitaria o comunque contenente dati sensibili, sulla busta chiusa deve essere apposta, mediante apposito timbro, la seguente dicitura: *"LA BUSTA CONTIENE DATI SENSIBILI AI SENSI DEL D. LGS 135/1999 E DEL D LGS 196/2003. "*
- ❑ Le cartelle sanitarie devono essere conservate in appositi armadi debitamente chiusi a chiave, presso la Segreteria della Presidenza per quanto riguarda i magistrati, in locali adibiti ad archivio presso l'Ufficio del Personale per quanto riguarda il personale amministrativo.
- ❑ Per quanto riguarda il diritto all'accesso ai documenti amministrativi, l'Ufficio si deve attenere rigorosamente a quanto disposto dalla Legge 7/8/1990 n. 241, dal DPR 27/6/1992 n. 352, dal DM 25/1/1996 n. 115 e, in particolare, alla *circolare contenente misure organizzative sul diritto d'accesso* in data 8/3/2006 del Ministero della Giustizia - Gabinetto del Ministro.
- ❑ Per quanto riguarda i fascicoli, atti e documenti delle cancellerie e archivi, civili e penali, l'accesso deve essere consentito solamente al diretto interessato (parte costituita nei procedimenti civili, imputato in quelli penali, difensori ecc.), previa identificazione e, per i difensori, verifica della delega.
- ❑ La movimentazione della documentazione cartacea deve essere effettuata in maniera tale da non consentire che possa essere visionata, durante il tragitto, da persone non autorizzate; pertanto deve avvenire, di norma, in orario di chiusura degli uffici al pubblico, con l'accorgimento di coprire i dati, per esempio con il registro di passaggio.

Il personale incaricato del trattamento ed i responsabili delle strutture sono tenuti ad uniformarsi alle suesposte misure di sicurezza ed al Manuale per la Sicurezza dei dati allegato, contenente le linee guida per gli incaricati.

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI

UFFICIO DEL RESPONSABILE DEL TRATTAMENTO DATI

TRIBUNALE DI BERGAMO

Il Presidente del Tribunale

Visto il decreto leg.vo n 196 del 30 giugno 2003, denominato Codice in materia di protezione dei dati personali,
Visto l'art 4,comma 1 lettera d del Codice che individua i dati sensibili;
Visto l'art 34 del Codice,relativo al trattamento dati con strumenti elettronici;
visto il decreto del Ministero della Giustizia del 24/5/2001,riguardante le regole procedurali sulla tenuta dei registri informatizzati;
Visto il decreto del Ministro della Giustizia n. 306 del 12/12/2006;
Considerato che negli archivi informatici di questo Tribunale sono contenuti,per compiti istituzionali,dati personali giudiziari e sensibili il cui trattamento è soggetto alle misure minime di sicurezza;
Considerato che ai sensi dell'art 34 lett.g del Codice deve redigersi il Documento Programmatico sulla sicurezza;
Considerato che il Documento deve contenere e analizzare
-l' elenco dei trattamenti dei dati personali effettuati
-la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte,delle persone incaricate del trattamento dei dati
-i irischi che incombono sui dati
-le misure adottate per garantire integrità e disponibilità dei dati,la protezione delle aree e dei locali inn cui dati sono custoditi
-i criteri da adottare per ripristinare i dati in caso di danneggiamento
-la previsione di interventi formativi degli incaricati del trattamento relativi ai rischi e alle misure per prevenire eventi dannosi,alla disciplina sulla protezione dati personali più rilevanti in rapporto alle relative attività,delle responsabilità derivanti e delle modalità di aggiornamento
-i criteri da adottare per la cifratura o per la separazione degli altri dati personali riguardanti stato di salute,vita sessuale,situazione economica,applicazione di sanzioni disciplinari e penali .
Tali dati sono trattati con strumenti elettronici o manuali mediante utilizzo di codici identificativi che li rendano intellegibili e comprensibili solo a chi è autorizzato all'accesso,consentendo l'identificazione degli interessati solo in caso di effettiva necessità ed esclusivamente per fini legittimati dalla normativa succitata;

DISPONE

che il presente Documento Programmatico nonché gli allegati Misure minime di sicurezza e Manuale di sicurezza degli utenti, siano posti alla base dell'accesso, della gestione del trattamento dati informatico e del trattamento dati non elettronici del Tribunale di Bergamo.
Il personale di magistratura e amministrativo,compresi ~~compresi~~ i dipendenti di aziende esterne addetti alla manutenzione e all'assistenza sistemistica sono tenuti ad osservare il presente documento.

NOMINA

-responsabili del trattamento la dott.ssa Simona Serrani,Direttore amministrativo,per il settore penale e la dott.ssa Francesca Corciulo per il settore civile e assegna loro il compito di rappresentare al titolare del trattamento le problematiche che eventualmente dovessero sopravvenire e provvedere all'effettiva realizzazione di quanto indicato nel Documento Programmatico,impartendo le opportune direttive agli incaricati del trattamento.
-addetto ai servizi informatici il funzionario Sig Antonio Cecere;
-amministratore di sistema l'esperto informatico Sig Luca Gilioli del CISIA di Brescia
-incaricati del trattamento:di norma tutti i dipendenti dell'ufficio devono accedere ai dati per l'esecuzione materiale delle operazioni di trattamento in base ad autorizzazioni circoscritte agli ambiti di rispettiva competenza,nel rispetto del presente Documento Programmatico della sicurezza,delle misure minime di sicurezza e del manuale per la sicurezza.

Criteri tecnici e organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza e procedure di controllo dell'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) Porte e finestre blindate;
d) Impianto elettrico a norma;
e) Gruppo di continuità.

1.3. L'accesso alla sala server è consentito solo al responsabile del trattamento o alle persone espressamente autorizzate.

1.4. In assenza del personale autorizzato, la sala server 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.

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 vanno 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 e le procedure per assicurare l'integrità dei dati.

3. **Sicurezza del software**

3.1. Presso ciascun Ufficio è consentita l'installazione esclusiva delle seguenti tre categorie di software:

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

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

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

3.4. Il software deve essere installato solo da supporti fisici originali o dei quali sia nota la , provenienza

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

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

4. **Integrità dei dati**

4.1. Il responsabile, 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 locazione fisica, delle misure di sicurezza su

esse adottate e delle eventuali misure di adeguamento pianificate.

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

4.3. A ciascun utente viene assegnata una directory, in un'area disco di un server che sia sottoposta a backup, dove mantenere 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.

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

4.5. 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 disposizione 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.

5. Sistema di monitoraggio

5.1. 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 dati e di applicazioni.

5.2. Il sistema di controllo deve registrare:
a) Gli accessi, riusciti e falliti, a livello di sistema, di base dati e di applicativo;
b) Gli accessi in lettura e scrittura effettuati attraverso il sistema di gestione delle basi dati;
c) Tutti gli accessi in lettura e scrittura ai singoli archivi.
d)

5.3. Il responsabile del trattamento individua, tra gli amministratori di sistema, uno o più incaricati della verifica delle registrazioni di cui al precedente comma.

5.4. 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 Capo dell'ufficio, individuerà le opportune contromisure.

5.5. L'individuazione delle responsabilità connesse a modifiche o letture non autorizzate viene effettuata sulla registrazione di cui alla lettera 5.2.c), su richiesta del responsabile del trattamento o del Capo dell'ufficio.

5.6. 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.***

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

6. Controllo degli accessi

6.1. Tutte le stazioni di lavoro debbono essere protette da una password di accensione.

6.2. L'inserimento della password di accensione va effettuato a cura dell'utente, affidandone una copia, in busta chiusa, al responsabile del trattamento, che le custodirà sotto chiave.

6.3. Ai fini dell'assistenza sistemistica, la password di accensione può venire comunicata agli incaricati, e sostituita al termine dell'intervento.

6.4. La password di accensione va modificata con cadenza annuale,

6.5. L'accesso alla rete di sistema va protetto tramite un nome utente e una password.

6.6. 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.

6.7. Il responsabile del trattamento fornisce ai preposti alla custodia delle parole chiave i nominativi e la qualifica degli utenti autorizzati, nonché i loro privilegi di utilizzo del sistema informatico. I preposti provvedono:
a) A definire, per ciascun utente, il nome utente e la password per il primo accesso;
b) A definire i gruppi necessari per rispettare i privilegi di utilizzo;
c) A consegnare agli interessati il nome utente e la password, unitamente a una copia del Manuale per la sicurezza.
d)

6.8. Dove questo è tecnicamente possibile, i preposti alla custodia delle parole chiave impostano il sistema in modo da forzare l'utente:
a) A cambiare la propria password al momento del primo accesso;
b) A cambiare la password periodicamente, con una frequenza non superiore a dodici mesi;
c) A non poter riutilizzare la stessa password prima di otto modifiche;
d) A non poter utilizzare lo stesso nome utente per accedere contemporaneamente al sistema da due postazioni di lavoro distinte.

6.9. La password di accesso alla rete:

a) Non deve derivare dal nome utente o dai dati personali dell'utente;
b) Deve avere una lunghezza di almeno sei caratteri;
e) Non deve essere una semplice parola rintracciabile in un dizionario;
d) Deve contenere almeno un carattere non alfabetico, oppure un misto di lettere minuscole e maiuscole.

6.10. Gli applicativi utilizzati per il trattamento possono sfruttare l'autenticazione di cui al punto

6.5, oppure richiedere a loro volta un nome utente e una password.

6.11. Alle eventuali password di accesso agli applicativi si applicano le indicazioni di cui ai punti 6.7, 6.8 e 6.9. Per gli applicativi che non consentano di automatizzare i controlli di cui al punto 6.8 va previsto un adeguamento, i cui tempi vanno indicati nel documento di cui al punto 4.1.

6,12. I preposti alla custodia delle parole chiave provvedono, con cadenza almeno trimestrale, alla verifica degli elenchi degli utenti, e provvedono, previa verifica con il responsabile del trattamento, alla disattivazione delle utenze su cui risultasse qualche problema mancato utilizzo da più di sei mesi, un elevato numero di tentativi di accesso non riusciti, o simili).

6.13. Nome utente e password sono strettamente personali. L'utente è tenuto
a) a non comunicare a terzi le password;
b) a non annotare le password su supporti posti in vicinanza della propria postazione di lavoro, o comunque incustoditi;
c) a scegliere la password di accensione diversa dalle altre due password;
d) ad attenersi a tutte le indicazioni contenute nel manuale per la sicurezza.

7. Trasmissione *dei dati*

7.1. Le connessioni telematiche verso le banche dati degli uffici, provenienti dall'esterno dello stesso ufficio, sono distinti in tre categorie:
a) Connessioni provenienti da altri uffici dell'Amministrazione della Giustizia;
b) Connessioni provenienti dall'interno dell'ufficio, su postazioni di lavoro pubblicamente disponibili;
c) Connessioni provenienti da utenti e postazioni di lavoro non appartenenti all'Amministrazione della Giustizia.
d)

7.2. Le connessioni di tipo a vengono controllate attraverso il Sistema Informatica di Sicurezza della Rete Giustizia, secondo le regole seguenti:

7.3. Sul collegamento dell'ufficio verso la Rete Giustizia è installato un apparato di controllo *(firewall);*

7.4. In maniera predefinita, il firewall è configurato in maniera da permettere alle postazioni di lavoro interne all'ufficio di accedere ai servizi disponibili sulla rete, bloccando i tentativi di accesso provenienti dall'esterno verso l'ufficio;

7.5. Qualora un ufficio voglia rendere disponibili dei servizi ad altri uffici dell'Amministrazione della Giustizia, dovrà richiedere all'Ufficio' del Responsabile per i Sistemi Informativi Automatizzati l'apertura dei canali di comunicazione necessari sul firewall.

7.6. Le procedure per la sicurezza delle connessioni di tipo *7.1.b)* sono stabilite dal responsabile del trattamento. Qualora le postazioni pubbliche consentano l'accesso ai dati sensibili di cui all'art. 22 della legge 675/99, o ai dati riservati di cui all'art. 24 della medesima legge, occorrerà stabilire rigorose procedure per l'autenticazione degli utenti (firma digitale, personale di presidio alla postazione, o simili).

7.7. Le procedure per la sicurezza delle connessioni di tipo 71.c) sono stabilite dall'Ufficio del Responsabile per i Sistemi Informativi Automatizzati (URSIA), di concerto con il Centro Tecnico per la Rete Unitaria della Pubblica Amministrazione. Gli uffici che abbiano necessità di connessioni di questo tipo debbono effettuarne richiesta all'URSIA.

7.8. Non sono autorizzati collegamenti telematici distinti da quelli previsti ai punti precedenti. In particolare, non sono autorizzate:
a) Connessioni dirette dalla rete dell'ufficio verso reti esterne diverse dalla Rete Giustizia;
b) Connessioni effettuate tramite modem da postazioni collegate alla rete dell'ufficio.

7.9. Qualora siano necessarie connessioni del tipo descritto al precedente punto 7.8, queste andranno effettuate da locali dedicati, le cui postazioni non siano connesse alla rete dell'ufficio. Per questi locali andranno previste adeguate misure di controllo degli 'accessi.

D) Piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire danni.

8. Manuale per la sicurezza

I responsabili di trattamento provvedono all'eventuale personalizzazione del manuale per la sicurezza, con la collaborazione degli amministratori di sistema,

. 11 manuale per la sicurezza viene aggiornato almeno ogni due anni.

Il manuale per la sicurezza viene consegnato agli utenti contestualmente ai codici (nome utente e password) per l'accesso al sistema.

9. Piano di intervento e formazione

Gli amministratori di sistema provvedono a informare tempestivamente i responsabili del trattamento di ogni eventuale problema di sicurezza di cui dovessero venire a conoscenza.

. I soggetti responsabili del trattamento provvederanno, anche per tramite degli amministratori di sistema, a informare tempestivamente gli incaricati;
a) della presenza di virus negli elaboratori dell'ufficio;
b) di prassi da parte del personale non conformi alle disposizioni di sicurezza;
c) della periodica necessità di variazione delle parole chiave da parte degli incaricati;
d) della disponibilità di programmi di aggiornamento relativi all'antivirus.

I responsabili,- ove richiesto o ove se ne ravvisi la necessità, provvederanno ad organizzare riunioni per l'illustrazione e la diffusione degli accorgimenti da adottare in tema di sicurezza.

10. Informatica giuridica
11. Fermo restando quanto previsto dalle disposizioni processuali circa visura e rilascio estratti e copie di atti e documenti,i dati identificativi delle questioni pendenti dinanzi all'autorità giudiziaria sono resi

accessibili a chi vi abbia interesse anche mediante comunicazione elettronica secondo le seguenti regole: l'interessato può chiedere al giudice per motivi legittimi, con richiesta depositata in cancelleria che sull'originale della sentenza o del provvedimento venga apposta un'annotazione volta a precludere l'indicazione delle generalità e di altri dati identificativi,in caso di riproduzione della sentenza o del provvedimento per finalità di informazione su riviste giuridiche o reti di comunicazione.

Fermo restando quanto previsto dall'art 734 bis del Codice penale,relativamente alle persone offese da atti di violenza sessuale,chiunque diffonde sentenze o altri provvedimenti giurisdizionali è in ogni caso tenuto ad omettere le generalità, dati identificativi e tutti quei dati dai quali può desumersi anche indirettamente l'identità dei minori o delle parti in procedimenti in materia di rapporti di famiglia e di stato delle persone.

Tutte le richieste provenienti da terzi docenti,studenti,giornalisti , enti vari,devono essere vagliate dal Presidente del Tribunale o da un suo delegato circa il presupposto di legittimità e ammissibilità.

Trattamento dati nei servizi civili

Il Responsabile del trattamento dati,con la collaborazione del coordinatore del reparto civile organizza il trattamento dati a cui i responsabili delle varie cancellerie e tutti gli impiegati assegnati a tale area,indicati in prospetto allegato devono attenersi .L'ambito del trattamento di ciascun operatore deve tenere conto della necessaria flessibilità e interscambiabilità dei compiti,per poter coprire tutti i servizi anche in assenza del singolo incaricato.

Trattamenti effettuati dalla struttura.

I dati trattati sono relativi agli affari contenziosi,alle cause di lavoro e previdenza,alle procedure concorsuali,agli affari con contenziosi, tutele,curatele, successioni alle procedure esecutive ,alle notifiche civili.

Il livello di accesso dell'utenza ad atti e fascicoli deve essere differenziato secondo le norme procedurali.

L'accesso ai registri informatici può avvenire attraverso richiesta al personale di cancelleria o,solo per gli Avvocati e i loro delegati,tramite consultazione diretta del p.c. situati esternamente dalla cancelleria.,previo inserimento di password e username e solo per la visione delle procedure in cui il richiedente è parte.

Protezione e accessibilità delle aree e dei locali riservati alla custodia dati:in ogni cancelleria viene prevista un'apposita area non accessibile agli utenti.

I dati inerenti il servizio civile vengono trattati su base cartacea e su base informatica attraverso i programmi ministeriali. Ogni postazione informatica ha una password e l'utente,per accedere al programma,deve utilizzare una propria password segreta.

Per la componente cartacea,i fascicoli durante la fase di movimentazione,devono permanere nei corridoi i tempi strettamente necessari alla loro consegna;sono conservati in locali inaccessibili all'utenza o in locali aperti al pubblico purchè collocati in armadi muniti di serratura e visionati con l'intervento del personale di cancelleria.

In particolare,per le esecuzioni mobiliari,ex art. 490 terzo comma cpc,nella pubblicità degli avvisi di vendita viene omessa l'indicazione del debitore .Inoltre,in base al provvedimento 7 febbraio 2008 del Garante per la privacy,l'ufficio e i professionisti delegati alla vendita non devono riportare le generalità del debitore e di ogni altro dato personale suscettibile di rivelare l'identità di quest'ultimo, nelle copie delle ordinanze e delle relazioni di stima pubblicate nè nell'avviso di vendita.

Per quanto riguarda le procedure concorsuali,gli atti vengono distinti tra quelli consultabili dal pubblico e quelli consultabili solo dal Curatore.Le perizie di stima sono consultabili dagli utenti solo successivamente alla pubblicazione dell'ordinanza di vendita.

I ruoli di udienza devono indicare il numero di registro generale ma non i nominativi delle parti.

Per le notifiche civili si applica l'art 137 terzo comma del cpc e in genere sono indicate le informazioni strettamente necessarie.

Trattamento dati nei servizi penali

Il Responsabile del trattamento,con la collaborazione del coordinatore dell'area penale e Gip,organizza il trattamento dati a cui gli incaricati,indicati nell'allegato prospetto devono attenersi nello svolgimento delle attività di istituto. L'ambito del trattamento consentito a ciascuna unità è individuato dal profilo di appartenenza e dall'assegnazione dei servizi in base agli ordini di servizio anche verbali..

Per coprire tutti i servizi anche in assenza del singolo incaricato è necessario prevedere flessibilità e interscambiabilità dei compiti.

I dati del settore penale sono trattati con strumenti elettronici e cartacei. Ogni postazione informatica ha una password e l'utente,per accedere al sistema deve usare una sua propria password segreta..I tecnici dell'assistenza sistemistica garantiscono la protezione dei dati contro il rischio di intrusione o danneggiamento ad opera di terzi.

I fascicoli penali vanno tenuti in armadi all'interno delle cancellerie o in armadi chiusi a chiave se posti all'esterno.:La consultabilità dei fascicoli è limitata alle parti e ai loro difensori a seguito di elezione del domicilio. I registri informatici vengono consultati solo dal personale dell'ufficio.

Al termine dell'otario di servizio le cancellerie sono chiuse a chiave.
Le richieste di copie presentate da soggetti diversi dalle parti o dai loro procuratori vanno sottoposte al magistrato per il vaglio circa la legittimità.Le parti che chiedono copie devono essere identificate .
I ruoli delle udienze dibattimentali aperte al pubblico contengono l'indicazione del nome dell'imputato.

Per tutte le aree,la designazione di incaricato del trattamento è implicita e deriva dall'assegnazione/preposizione della persona fisica a un ufficio o cancelleria.

Trattamento dati nei servizi amministrativi del personale.
I dati sono trattati con strumenti elettronici e cartacei.
I fascicoli personali sono tenuti in armadi chiusi a chiave e sono consultabili dall'interessato, dal personale addetto all'ufficio del personale,dal Capo dell'Ufficio o da un suo delegato e dal dirigente amministrativo.
Vanno tenuti conservati anche tutti quei documenti relativi allo stato di salute proprio e dei familiari e i fascicoli contenenti le visite mediche espletate dal medico del lavoro.
Le informazioni su straordinario e assenze di ciascuna unità sono consultabili dall'interessato e dal coordinatore della cancelleria nella cui area è collocato funzionalmente l'addetto. Eventuali richieste di informazioni su dati sensibili avanzate dalle organizzazioni sindacali o dalle RSU o di consultare atti del protocollo contenenti dati sensibili vengono trasmesse al titolare del trattamento per l'eventuale autorizzazione.

Bergamo 26.XI.2015

Firma

IL PRESIDENTE DEL TRIBUNALE
(Dr. Ezio Siniscalchi)