PROCURA GENERALE DELLA REPUBBLICA DI PERUGIA

Ordine di servizio n. 11 | 2021

MISURE DI SICUREZZA RELATIVE ALLA PROTEZIONE DEI DATI PERSONALI

(Art. 30 , par. 1, lett. g), Regolamento (UE) n. 2016/679)

Distribuzione dei compiti e delle responsabilità

Titolare del trattamento dei dati di natura amministrativa è il Ministero della Giustizia nella persona del Ministro pro tempore e **Titolare del trattamento** dei dati trattati per ragioni di giustizia e dei dati afferenti a condanne penali e reati è la **Procura Generale della Repubblica di Perugia,** nella persona del Procuratore Generale, dott. Sergio Sottani o sostituto pro tempore, quale legale rappresentante. E' stata designata **Responsabile della protezione** dei dati, la dott.ssa Doris Lo Moro (D.M. del 7/8/2018). È designato **Responsabile del trattamento,** il Dirigente Amministrativo dott.ssa Luisa Lucia Marsella o sostituto pro tempore. Il trattamento comprende anche i dati contenuti nel sito internet istituzionale. È designato ***webmaster***, quale responsabile della gestione del servizio del sito internet, il funzionario informatico Massimiliano Fiumicelli e , limitatamente alla parte relativa a questo Ufficio, il funzionario giudiziario Mauro Cristarella Orestano.

Incaricati del trattamento dei dati inseriti nelle banche informatiche e negli archivi cartacei sono i magistrati e il personale amministrativo nei limiti delle funzioni e delle mansioni indicate nel progetto organizzativo e negli ordini di servizio vigenti. Sono altresì incaricati del trattamento i tirocinanti nei limiti delle attività indicate nel progetto formativo e ogni altro soggetto incaricato espressamente dal Titolare.

Sono stati nominati in qualità di **Amministratore dei servizi informatici e preposti alla custodia della parola chiave** gli informatici assegnati al Presidio Cisia di Perugia:

1. Massimiliano Fiumicelli
2. Iolanda Laviosa
3. Alessandro Colangeli
4. Nicola Maggi
5. Francesco Polizzi

M_DG.Procura Generale della Repubblica di PERUGIA - Prot. 09/07/2021.0000112.I

I predetti , funzionari e assistenti informatici, sono coadiuvati nei propri compiti dai seguenti tecnici del Raggruppamento Temporaneo di Imprese (R.T.I.) che svolge assistenza sistemistica presso questo ufficio: Maurizio Pammolli, Michele Neri, Francesco De Santis.

Analisi dei rischi- Misure di protezione

I rischi cui sono sottoposti i dati sono i rischi tipici di ogni sistema informatico e si distinguono in rischi legati ad eventi "fisici" quali guasti, sabotaggi, furti, intercettazioni, allagamenti o incendi, ed eventi legati a codice programma maliziosi, comunemente classificati come *virus, malaware, trojan horse, backdoor* o ancora da attività generata per rendere inutilizzabili i servizi di rete, tecnicamente nota come *"Denial of Service". L'analisi dei rischi*, unitamente alle misure di protezione, sono riportate nell'allegata tabella A .

L'integrità fisica dei dati è affidata alle misure di sicurezza della sala server distrettuale, il cui accesso, protetto da porta blindata, è consentito al personale del Presidio Cisia, ai tecnici informatici della ditta aggiudicataria della gara di assistenza sistemistica distrettuale, i quali si occupano anche della gestione delle copie automatiche giornaliere dei dati, che vengono prodotte ogni sera della settimana, ad eccezione dei giorni festivi e prefestivi.

La sala server è dotata di porta tagliafuoco, impianto antintrusione, condizionatore, che rendono lo stesso ambiente abbastanza sicuro da eventi "fisici" accidentali.

Tutti i server, nonché le singole postazioni di lavoro, sono protetti da antivirus attivo, indicato e fornito dal superiore Ministero, il cui compito è quello di proteggere i dati dai codice-programma "maliziosi", sopra indicati, e il cui aggiornamento viene effettuato in maniera automatica con frequenza giornaliera. Anche il sistema operativo di ogni singolo *pc* viene aggiornato in tempo quasi reale al rilascio da parte di Microsoft.

Inoltre ogni *Server* è alimentato tramite un gruppo di continuità che filtra eventuali sbalzi di corrente e permette, in caso di assenza di elettricità, il corretto spegnimento del server, evitando quindi tutti i danni che possono verificarsi per gli sbalzi di tensione elettrica.

I server per la gestione della posta elettronica sono attualmente centralizzati presso enti indicati dal superiore Ministero, cui spetta l'onere di filtrare i messaggi contenenti codice "maligno".

Per quanto riguarda la protezione da eventuali attacchi *"Denial of Service"*, cioè mirati a rendere indisponibili i servizi di rete, si precisa che la rete di comunicazione dati è protetta da apposita apparecchiatura *Firewall*, configurata in remoto dall'apposito Centro di Sicurezza del Ministero, sito a Napoli, il cui compito è quello di evitare che utenti esterni alla rete possano accedere alle risorse interne al Palazzo di Giustizia di Perugia.

Pertanto si ritiene che la rete sia protetta da attacchi esterni che possano portare al blocco di servizi di rete. L'attuale organizzazione dei sistemi informatici del ministero prevede che le basi dati e gli SW siano fisicamente dislocati in luoghi anche molto distanti dalla sede giudiziaria. In

particolare le basi dati e i sistemi del civile si trovano presso la sala CED di Roma mentre le basi dati e i sistemi del penale si trovano presso la sala CED distrettuale di Perugia; per cui saranno tali strutture a garantire le politiche di sicurezza e di backup.

Criteri e modalità di ripristino in seguito a danneggiamento o distruzione Infrastruttura di Backup

La gestione del backup nella sede di Perugia si sviluppa su due livelli:

Primo livello	locale	ogni 24h o meno
Secondo livello	Secondo server locale	ogni 24h

Il primo livello copia i dati in oggetto sullo stesso server, tipicamente rappresenta il dump di un RDBMS. Il secondo livello copia i dati su altro server locale. In seguito alle recenti forniture di dispositivi NAS, gli stessi back up vengono replicati su tali apparecchiature.

Tipologia dei dati:

Le tipologie di dati sottoposti a *backup* sono:

cartelle utenti/uffici (files di Office, cartelle generiche di scambio dati), dati relativi alla rilevazione automatica delle presenze.	

Frequenza: Giornaliera.

Scheduling

Tutte le procedure di *backup*, assieme alle procedure pianificate sono gestite via procedure batch. Ciascun server ha pianificata quotidianamente una propria procedura unica, la quale esegue tutte le attività per quel *server.* Alcuni server hanno programmato più procedure, ma solo se queste hanno frequenza differente (per esempio una quotidiana e una settimanale).

Tutte le procedure *batch* sono localizzate in una unica cartella (sul *server backup*) e sono molto semplici da mantenere. Le operazioni comuni, come la copia dati, il *logging*, gli indici *Re.Ge.*, i *dump*, sono contenute in altre sotto-procedure *batch* modulari e parametrizzate.

MISURE RIGUARDANTI IL TRATTAMENTO DEI DATI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

1. I fascicoli cartacei contenenti dati personali sono conservati all'interno degli uffici. Nella fasi di trasporto, i fascicoli devono sempre essere presidiati dal personale della Procura Generale e comunque solo per il tempo strettamente necessario alla loro consegna.
2. Gli incaricati hanno accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati.
3. I locali utilizzati come archivi non sono accessibili al pubblico. L'accesso agli archivi è controllato. Il personale che vi accede è preventivamente autorizzato dal funzionario responsabile del settore.
4. Gli atti e i documenti contenenti categorie particolari di dati personali che godono di protezione rafforzata (es. dati relativi alla salute oppure dati che rivelino l'appartenenza sindacale) e i dati relativi a condanne penali e reati sono conservati in appositi armadi chiusi dal personale incaricato.
5. Ai soggetti esterni, che comunicano dati personali per lo svolgimento di un'attività amministrativa dell'Ufficio, è fornita l'informativa prevista dagli artt. 13 e 14 del Regolamento.

Per quanto riguarda l'uso delle *password*, si richiama il manuale per la sicurezza dei dati, allegato.

Si comunichi ai magistrati, al dirigente e al personale amministrativo, agli altri incaricati del trattamento e al presidio CISIA di Perugia.

Perugia, 7 luglio 2021

Il Procuratore Generale

Sergio Sottani

Allegati:

1. Documento incaricati;
2. Linee guida per la sicurezza dati.