

Prot. 62/2023 INT.
Prot. 707/2023 U.



Procura della Repubblica

presso il Tribunale

TRANI

Piazza Duomo, 10 – 76125 TRANI – Cod. Fisc. 83002280721
tel. 0883-505111 – fax 0883-583471 – e-mail: procura.trani@giustizia.it
PEC: prot.procura.trani@giustiziacert.it

MISURE DI SICUREZZA RELATIVE ALLA PROTEZIONE DEI DATI PERSONALI ai sensi di quanto disposto dal D. Lgs. n. 51/2018, dal Regolamento Europeo 2016/679 in materia di protezione dei dati personali – cd. Gdpr – nonché dalla Direttiva (UE) 2016/680.

Il Procuratore della Repubblica

- visto il Regolamento (EU) 2016/679 del Parlamento europeo e del Consiglio 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GDPR), compresi gli artt. 13, par. 1, e 14 par.1, relativi alla informativa prevista con la quale sono portate a conoscenza del cittadino, anche prima che diventi interessato, le finalità e le modalità dei trattamenti operati dal titolare del trattamento; informativa che ben può essere fornita attraverso il sito web (Considerando 58 del Reg. 679/16);
- visto il d.lgs. 18 maggio 2018, n.51, recante Attuazione della 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 esecuzioni di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio;
- visti i decreti ministeriali in materia di protezione e trattamento dei dati, nonché in materia di registri di cancelleria;
- vista la nota prot. n. 21611 del 27 giugno 2018 a firma del Capo di Gabinetto del Ministro che comunica che il Ministero della Giustizia ricopre la funzione di titolare del trattamento dei dati oggetto di lavorazione nei diversi uffici centrali e periferici;
- richiamato quanto disposto con provvedimento n. 184/2022 int. avente ad oggetto "MISURE DI SICUREZZA RELATIVE ALLA PROTEZIONE DEI DATI PERSONALI ai



sensi di quanto disposto dal D. Lgs. n. 51/2018, dal Regolamento Europeo 2016/679 in materia di protezione dei dati personali – cd. Gdpr –nonché dalla Direttiva (UE) 2016/680”;

- richiamato quanto previsto nel progetto organizzativo – paragrafo 5.2.8 – intitolato La protezione dei dati personali – pagg. 254 e seguenti;

- richiamato quanto previsto nel progetto organizzativo – paragrafo 5.2.7 – intitolato La disciplina dell’accesso agli uffici giudiziari – pagg. 251 e seguenti;

- richiamato quanto previsto nel progetto organizzativo – paragrafo 5.2.6 – intitolato Il protocollo riservato – pag. 251;

PRECISATO

- che per dato personale deve intendersi qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»);

PRESO ATTO

- dei rischi cui sono sottoposti i dati di ogni sistema informatico, ed in particolare i rischi legati ad eventi “fisici” quali guasti, sabotaggi, furti, intercettazioni, allagamenti o incendi, ed i rischi legati a programmi malware, trojan horse, e/o all’utilizzo di backdoor o ancora attività generata per rendere inutilizzabili i servizi di rete;

- dei rischi cui sono sottoposti i dati trattati senza l’ausilio di strumenti informatici;

RICHIAMATO

- l’ordine di servizio n. 184/2022 int. in materia di sicurezza relative alla protezione dei dati personali;

RICHIAMATE

- le iniziative assunte in materia di tutela della segretezza, sulle quali ci si è soffermati nel progetto organizzativo:

- a) l’accesso ordinato, programmato e tracciabile della utenza mediante sportello telematico;
- b) la realizzazione di Front office;
- c) l’acquisto di distruggi documenti sia per singolo magistrato sia di tipo massivo;
- d) l’avvio della vigilanza al piano;

DISPONE

1) La distribuzione dei compiti e delle responsabilità nel seguente modo:

Titolare del trattamento dei dati è il Ministero della Giustizia

Responsabile del trattamento è il Procuratore della Repubblica Dott. Renato NITTI – essendo vacante il posto di Dirigente Amministrativo -, che opera anche in qualità di Responsabile della Tenuta dei Registri Informatizzati e responsabile dell'Ufficio Re.Ge e Archivio;

Sub Responsabili del trattamento dei dati, per i servizi e le parti di rispettiva competenza, il direttore e i funzionari individuati quali responsabili dei vari uffici e segreterie, come da ordine di servizio; attualmente

Direttore Michela Di Fonzo per l'Ufficio Gestione Risorse Umane, VPO, Casellario Giudiziale e Certificazioni, Ufficio Dibattimento, Ufficio TIAP;

Funzionario Giovanna Bufo per la Segreteria particolare del Procuratore, Organizzazione amministrativa e Gestione Risorse Umane esterne;

Funzionario Francesco Paolo Laurora per l'Ufficio Spese, Liquidazioni ed Intercettazioni;

Funzionario Apollonia Zagaria per le segreterie dei P.M.;

Funzionario Angelina Zingarelli per la segreteria D.A.S. e G.d.P.;

Funzionario Michele Cellamaro per l'Ufficio Esecuzioni penali detentive;

Funzionario Mariagrazia Capozza per l'Ufficio Esecuzioni penali non detentive;

Funzionario Giuseppina Paracampo per l'Ufficio del Consegnatario;

Sig. Antonio Tarricone per l'Ufficio Conducenti automezzi;

Incaricati al trattamento sono i magistrati ed il personale amministrativo nei limiti delle funzioni e mansioni indicate nel progetto organizzativo e negli ordini di servizio vigenti. Sono altresì autorizzati al trattamento i tirocinanti nei limiti delle attività indicate nel progetto formativo e ogni altro soggetto autorizzato espressamente.

Tutti i soggetti autorizzati sono tenuti a rispettare l'obbligo di riservatezza e segretezza e conseguentemente il divieto di comunicazione e diffusione dei dati trattati nel corso dell'espletamento delle mansioni.

Il Procuratore della Repubblica, quale Responsabile del trattamento, provvede a garantire l'effettiva realizzazione di quanto indicato nel presente provvedimento; sovrintende e vigila sul rigoroso rispetto della normativa in materia di trattamento dei dati personali, sensibili e giudiziari; impartisce istruzioni dettagliate ai sub-responsabili e agli incaricati.

È compito degli incaricati del trattamento rispettare le norme vigenti in materia e tutte le disposizioni di sicurezza.

RICHIAMATE

le prescrizioni in tema di tutela della segretezza e protezione dei dati ed in particolare le misure di protezione adottate, che qui si confermano - accesso agli uffici della procura, custodia dei fascicoli dei procedimenti, chiusura degli uffici, consultazione dei fascicoli, divieto di fotocopiatura o scannerizzazione e di esportazione, distruzione dei documenti, protocollo riservato.

2) Le prescrizioni dettate nel progetto organizzativo

Nel fare integrale rinvio al lgs. 51/2018, ci si sofferma, ancora una volta, sulle disposizioni e misure organizzative già attuate nell'Ufficio di Procura, volte ad assicurare la protezione dei dati personali.

2.1) Accesso negli uffici

In particolare, si richiamano le disposizioni – poste a tutela della riservatezza dei dati personali - in ordine all'accesso negli uffici evidenziando che gli stessi sono distinti a seconda che siano

- a) Aperti al pubblico anche senza un appuntamento – I Front Office dell'ufficio per le Relazioni con il Pubblico nelle sue articolazioni;
- b) Aperti al pubblico soltanto previo appuntamento – Segreteria Amministrativa, Ufficio Predibattimento; Ufficio Dibattimento; stanze del Procuratore della Repubblica, del Procuratore Aggiunto e di tutti i sostituti procuratori, con le rispettive segreterie, l'Ufficio della Segreteria Centrale; l'Ufficio Affari Civili;
- c) Mai aperti al pubblico – Ufficio Registro Generale, Ufficio della Esecuzione, C.I.T. con esclusione della zona Avvocati (per la quale occorre comunque fissare appuntamento), Archivi, Protocollo.

L'ufficio del Registro Generale, dove vengono iscritti i procedimenti e dove, pertanto, è massima l'esigenza di tutela della segretezza dei dati, è zona assolutamente riservata: l'accesso a tale ufficio è consentito soltanto alle persone espressamente autorizzate (in linea di massima soltanto al personale assegnato a tale ufficio ed ai magistrati dell'Ufficio) ed è comunque vietato a persone estranee all'Ufficio (salva specifica ed espressa autorizzazione del Procuratore). Le porte di tale Ufficio devono essere sempre chiuse a chiave quando, anche per pochi momenti, la stanza rimane vuota.

L'accesso ai locali utilizzati come archivi è consentito soltanto al personale amministrativo addetto all'archivio e diretti collaboratori, al Procuratore della Repubblica ed al Procuratore Aggiunto. L'accesso da parte di altre persone appartenenti all'Ufficio (magistrati, dipendenti, e personale di P.G.) deve essere preventivamente autorizzato dal Funzionario Responsabile del settore. La consultazione o il ritiro degli atti in archivio deve essere annotato in apposito registro, ai fini di una successiva tracciabilità.

2.2.) Custodia dei fascicoli

Altra forma di tutela della segretezza dei dati personali consiste nella custodia dei fascicoli. Tutti i fascicoli cartacei contenenti i dati personali devono essere conservati all'interno degli uffici in modo che non siano visibili ed accessibili a personale estraneo all'ufficio.

Nella fase di trasporto, al fine di evitare la visibilità, i fascicoli devono essere inseriti in faldoni, sempre presidiati dal Personale della Procura e comunque solo per il tempo strettamente necessario alla loro consegna, anticipando, sin da ora, che sulle copertine ad adottarsi non vi sarà alcuna indicazione ai dati identificativi.

2.3) Chiusura degli Uffici

Tutte le stanze degli uffici della procura della Repubblica – ed in particolare quelle dei magistrati e delle loro segreterie – devono essere sempre chiuse a chiave quando al suo interno non vi è personale dell'ufficio ed in particolare durante le ore di chiusura dell'ufficio (nel pomeriggio, di notte o nei giorni festivi).

2.4) Consultazione dei fascicoli

I fascicoli possono essere consultati, nel rispetto e nei limiti previsti *ex lege*, soltanto dalle parti del procedimento e dai loro difensori. La consultazione dei fascicoli e/o l'estrazione di copia da parte di persone diverse è possibile soltanto previa autorizzazione del magistrato titolare o dal Procuratore.

2.5) Limiti nella riproduzione di copia

È fatto divieto di fotocopiatura, scannerizzazione e di esportazione dei documenti al di fuori delle esigenze procedurali e senza l'autorizzazione del responsabile del trattamento.

Le stampe, che non servono (es. quelle di documenti poi modificati) vanno subito distrutte, evitando una diffusione di dati personali.

Se si tratta di documenti contenenti dati sensibili o riservati, occorre distruggere il documento in modo che non ne sia possibile la ricostruzione, possibilmente utilizzando una delle apposite macchine distruggi-documenti. Apposite macchine di media produzione sono state fornite alle segreterie e ad ogni magistrato. È stata acquistata anche una macchina distruggi documenti ad alta produzione.

In ogni caso i documenti cartacei contenenti dati personali non vanno mai cestinati senza averli prima fatti a pezzi.

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

Gli atti e i documenti contenenti i cd. dati particolari ex art. 9 Gdpr (es. dati relativi alla salute oppure dati che rivelino l'appartenenza sindacale) devono essere conservati in appositi armadi chiusi.

Ai soggetti esterni, che comunicano dati personali per lo svolgimento di un'attività amministrativa dell'Ufficio, deve essere fornita l'informativa a tutela dei dati personali.

2.6 Il protocollo riservato

La tutela in concreto della segretezza e della riservatezza degli atti passa, come è evidente, dalle disposizioni capaci di modulare l'organizzazione delle risorse strumentali e personali.

Vi sono molteplici atti che pervengono all'Ufficio o sono formati all'interno dell'ufficio che non sono di per sé destinati a essere inseriti nei fascicoli di uno dei modelli procedurali

previsti, ancorché sia ricorrente che, attraverso il c.d. mod. 45, si sperimenti una possibile destinazione accomunando tutto ciò che non è "notizia di reato".

Se appare corretto utilizzare il generale protocollo dell'Ufficio di segreteria in questa prospettiva, occorre al tempo stesso individuare una ripartizione interna che consenta sia la catalogazione informatica degli atti che la conservazione del cartaceo ove necessario.

Ciò consente di individuare le seguenti sottocategorie del protocollo:

- a) Protocollo/Riservato/Astensioni e Riassegnazione;
- b) Protocollo/Riservato/Revoca assegnazione;
- c) Protocollo/Riservato/Assensi e Visti;
- d) Protocollo/Riservato/ AG (richieste di altre AA.GG., verbali di acquisizione presso questo ufficio etc.);
- e) Protocollo/Riservato/Ispettorato (accertamenti in sede di ispezione mirata);
- f) Protocollo/Polizia Giudiziaria/
- g) Protocollo/ Riunioni (con le sottoripartizioni: magistrati/personale amministrativo)
- h) Protocollo/ CSM;
- i) Protocollo/ 81/08;
- j) Protocollo / PGA (Procura generale Corte di Appello);
- k) Protocollo/ PGC (Procura generale Corte di Cassazione).

L'accesso agli atti dei menzionati protocolli deve essere autorizzato dal Procuratore.

Il rilascio di copia va autorizzato per iscritto dal Procuratore.

L'istanza con l'autorizzazione e l'attestazione del rilascio di copia va inserita nella stessa sezione del protocollo.

3. Le regole di cautela generali in merito al trattamento dei dati mediante strumenti informatici ed in particolare le misure di protezione dei dati trattati con l'ausilio di strumenti informatici, che qui si confermano.

Qui di seguito appare utile richiamare i seguenti punti:

3.1 Accesso ai sistemi informativi.

L'accesso ai sistemi informativi, ai programmi informatici ed ai dati in essi contenuti è consentito soltanto alle persone autorizzate (in relazioni alle attività svolte) e mediante l'uso di credenziali personali. Le credenziali devono possedere le seguenti caratteristiche: lunghezza di almeno otto caratteri, complessità della password, vale a dire contenente caratteri di almeno 4 diverse tipologie e una frequenza di modifica della password con cadenza semestrale. Non è consentito l'utilizzo di profili di accesso alla rete giustizia da parte di soggetti non autorizzati.

3.2 Utilizzo PC.

L'utente deve utilizzare il proprio PC esclusivamente per l'attività dell'ufficio; è vietato usarlo per attività privata. È vietato, inoltre – salvo il compimento di operazioni semplici che non possano compromettere la funzionalità del P.C. (quale la sostituzione del mouse o della tastiera) – assumere iniziative personali per porre rimedio ad eventuali problemi tecnici del computer, in particolare effettuare interventi sia sull'hardware che sui software; ove necessario, occorre rivolgersi all'assistenza tecnica.

3.3 Divieto di utilizzo del PC a personale esterno.

Non permettere l'uso del proprio computer a personale esterno, a meno di non essere sicuri della loro identità. In alcuni casi personale esterno dell'assistenza informatica e sistemistica può avere bisogno di installare sui personal computer un nuovo

software/hardware; in tali casi è necessario assicurarsi dell'identità della persona e delle autorizzazioni ad operare sul proprio PC.

3.4 Sostituzione o dismissione del computer.

In ogni caso di sostituzione del P.C., di sua assegnazione ad altro utente o di sua dismissione, l'assistenza tecnica deve provvedere alla cancellazione irreversibile di tutti i dati in esso contenuti.

3.5 Spegnimento computer a seguito di allontanamento dalla postazione.

Spegnere o mettere in stand by il computer se ci si assenta per un periodo di tempo lungo dalla propria postazione di lavoro. Un computer acceso è 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 ai file in uso o ai documenti in fase di elaborazione. Ogni postazione di lavoro deve avere il salvaschermo attivato, con richiesta di password per poter riprendere il controllo della postazione.

3.6 Conservazione supporti di memoria.

Alla conservazione dei supporti di memoria (CD, pen drive, dischi esterni ecc.) si applicano gli stessi criteri di protezione dei documenti cartacei. Essi, pertanto, vanno conservati sotto chiave.

3.7 Sala server – misure CISIA

Si danno per acquisite le misure di sicurezza illustrate dal Ministero della Giustizia – CISIA di Napoli, che qui di seguito si illustrano in maniera sintetica.

L'accesso alla sala server è consentito al personale CISIA.

La sala server è dotata di impianto antintrusione e condizionatore, che rendono l'ambiente sicuro da eventi accidentali (guasti, sabotaggi, furti, intercettazioni, allagamenti o incendi...).

Per quanto riguarda le misure di sicurezza adottate per prevenire i rischi legati a programmi malware, trojan horse, e/o all'utilizzo di backdoor o ad attività generata per rendere inutilizzabili i servizi di rete, si precisa che 1) tutti i server, nonché le singole postazioni di lavoro, sono protetti da antivirus McAfee Endpoint Security; 2) la rete di comunicazione dati è protetta da apposita apparecchiatura Firewall. I server per la gestione della posta elettronica sono attualmente centralizzati presso enti indicati dal Ministero.

DISPONE

L'OSSERVANZA DELLE SUMMENZIONATE PRESCRIZIONI (e di tutte quelle non qui modificate richiamate dal progetto organizzativo e da precedenti ods) DA PARTE DEI DESTINATARI DEL PRESENTE ORDINE DI SERVIZIO, CON IL CONSEGUENZIALE OBBLIGO DI ATTIVAZIONE DELLA PROCEDURA (DATA BREACH POLICY), CHE QUI SI RICHIAMA ESPRESSAMENTE www.garanteprivacy.it/regolamentoue/databreach.

Si comunichi

- al Ministero della Giustizia;
- al Sig. Procuratore Generale presso la Corte di appello di Bari;
- al Sig. Procuratore Aggiunto e ai Colleghi;
- al personale amministrativo, al personale della Sezione di Polizia Giudiziaria, ai tecnici informatici, ai tirocinanti;
- alle RSU, RSPP, medico competente;
- alle Organizzazioni sindacali;
- al Magrif per la pubblicazione sul sito internet.

Trani, lì 9.3.13


Renato Nitti
Il Procuratore della Repubblica