



PROCURA GENERALE DELLA REPUBBLICA
presso la Corte d'appello
MILANO

N. 400/2025 Prot. Inf. Int.

14 luglio 2025

IL PROCURATORE GENERALE

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 (GDPR);

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 esecuzione 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;

ritenuta l'esigenza di individuare le figure di riferimento previste dalla normativa e di fissare un compendio di regole interne, suscettibile di integrazione in base alla consultazione in proposito avviata con il CISIA di riferimento, per garantire la sicurezza dei dati e fornire una disciplina di base della materia nella Procura generale di Milano;

DISPONE

quanto segue, limitatamente agli ambiti di pertinenza della Procura generale presso la Corte d'appello di Milano e fatta salva l'autonoma competenza dell'Amministrazione centrale per la materia amministrativa:

- 1) è **Titolare del trattamento** il Capo dell'Ufficio - analogamente al trattamento dei dati derivanti dall'attività della videosorveglianza - attualmente nella persona del Procuratore generale **dott.ssa Francesca Nanni**, o chi ne fa le veci;
- 2) è **Responsabile del trattamento** il Dirigente amministrativo, attualmente nella persona della **dott.ssa Silvia Ciccone**, o chi ne fa le veci, che opera anche in qualità di Responsabile della tenuta dei registri informatizzati;
- 3) la figura del **Responsabile della protezione dei dati (RPD)** è individuata a cura del Ministero della giustizia;
- 4) sono nominati **sub-Responsabili del trattamento dei dati**, per i servizi e le parti di rispettiva competenza, i direttori/funzionari individuati quali responsabili dei vari uffici e segreterie, come da ordini di servizio; attualmente: Antonella Beatrice Perrone per la

¹ Con provvedimento prot. int. n. 33/2020 del 7/02/2020 è stato adottato il Regolamento dell'attività di videosorveglianza all'interno degli edifici giudiziari di Milano integrato con provvedimento n. 175/2020 Prot. inf. int. del 23.6.2020.



segreteria del personale e per l'ufficio protocollo; Laura Albano per la segreteria del Procuratore Generale, dei magistrati e del Dirigente; Francesco Cantatore per l'ufficio del Funzionario delegato per le spese di Funzionamento; Flavia Xenia Cuccovillo per l'Ufficio del Funzionario delegato Spese di Giustizia; Concetta Miceli per l'ufficio Contratti; Mario Carozza per l'ufficio Economato e per l'ufficio del consegnatario economo; Cinzia Ventimiglia per l'Area giudiziaria (segreteria affari penali e segreteria affari civili), Maria Teresa Giambanco e Maria Antonietta Bacciu per l'ufficio esecuzioni penali; Barbara Cerasino per la segreteria Affari internazionali; Giorgio Picciriello per l'ufficio innovazione;

- 5) sono **Incaricati del trattamento** tutti i dipendenti – magistrati e amministrativi – e collaboratori legittimamente abilitati (anche appartenenti alla polizia giudiziaria) che accedono ad affari dell'ufficio per l'esecuzione delle operazioni di trattamento, ciascuno per quanto di rispettiva competenza.

Compiti e prescrizioni

Il Dirigente amministrativo, quale Responsabile del trattamento, provvede a garantire – di concerto con il Procuratore generale – l'effettiva realizzazione di quanto indicato nel presente provvedimento; sovrintende e vigila sul rigoroso rispetto della normativa in materia di *privacy* e di trattamento dei dati personali, sensibili e giudiziari; impartisce istruzioni dettagliate ai sub-responsabili e agli incaricati. Curerà la predisposizione del Registro delle attività di trattamento.

È compito dei sub-Responsabili del trattamento provvedere ad adattare specificamente le prescrizioni alle esigenze degli uffici e provvedere alla loro effettiva realizzazione, in conformità alle indicazioni del Titolare e del Responsabile; attuare tutte le indicazioni sulla sicurezza dei dati, la gestione delle *password* e l'autorizzazione ad accedere agli archivi, nonché vigilare sull'operato di tutti gli incaricati, anche impartendo opportune disposizioni specifiche.

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

Gli Incaricati curano il corretto utilizzo degli applicativi informatici e degli archivi cartacei nell'ambito dei rispettivi uffici; svolgono il trattamento secondo correttezza, con raccolta e registrazione di dati esclusivamente per gli scopi inerenti alla attività svolta; provvedono alla conservazione in conformità alle misure di sicurezza, garantendo in ogni operazione di trattamento – sia cartaceo sia automatizzato – la massima riservatezza, evitando l'accesso da parte di terzi anche se dipendenti dell'amministrazione. In caso di allontanamento anche temporaneo dal posto di lavoro, ogni incaricato deve accertarsi che non sia possibile l'accesso ai dati da parte di terzi, anche se dipendenti.

Nel caso si debba procedere alla distruzione (anche parziale) di dati, cartacei o informatici, anche in copia, devono adottarsi tutte le misure necessarie ad evitare che i dati possano essere individuati o recuperati dopo la distruzione e che si possa riconoscere il contenuto o la provenienza del documento.

Disposizioni sul trattamento dei dati

I dati personali sono trattati dalla Procura generale di Milano nell'esecuzione dei propri compiti di interesse pubblico o comunque connessi all'esercizio dei propri pubblici poteri.

I trattamenti connessi ai servizi *web* accessibili dal sito *internet* avverranno secondo quanto specificato nell'*Appendice 1* al presente provvedimento.

Ogni copia informatica o cartacea di documenti o dati può essere rilasciata solo a chi dimostri di avere la titolarità ad ottenerla.

In relazione a tutte le misure previste nel presente provvedimento, sono fatti salvi i diversi o più rigorosi presidi eventualmente necessari in conformità a specifiche previsioni legislative o regolamentari.

Misure di sicurezza relative a elaboratori elettronici, terminali e supporti digitali

Ogni incaricato provvede alla periodica sostituzione della propria parola-chiave, con cadenza almeno trimestrale, previa comunicazione al soggetto preposto alla custodia delle parole-chiave.

Per un eventuale accesso di emergenza, la propria parola-chiave e il relativo *username* ..sono annotati da ciascuna unità di personale su carta e conservati in busta chiusa e controfirmata. Le parole-chiave saranno custodite dal Preposto in armadio blindato o cassaforte, ciascuna inserita in busta chiusa sui cui lembi apporranno le firme sia il titolare della parola-chiave sia il Preposto. In caso di necessità di apertura di una delle buste, si redigerà verbale, specificando le ragioni per le quali si è reso necessario accedere al contenuto. È onere del titolare delle credenziali rappresentare al Preposto l'esigenza di attivare la procedura di sostituzione delle parole-chiave scadute.

I codici identificativi personali per l'utilizzazione degli apparecchi devono essere gestiti in modo che ne sia prevista la disattivazione in caso di perdita della qualità che consentiva l'accesso all'elaboratore o di mancato utilizzo dei medesimi per un periodo superiore ai sei mesi.

I dati contenuti su supporti informatici non devono essere mai accessibili indistintamente bensì in conformità ad opportuni profili di accesso.

I programmi in dotazione, di protezione contro il rischio di intrusione o danneggiamento ad opera di terzi, devono essere continuativamente verificati, quanto ad efficacia ed aggiornamento, con cadenza almeno mensile.

Nel caso in cui l'elaboratore contenga dati sensibili o dati particolari, l'accesso all'elaboratore sarà consentito sulla base di autorizzazioni assegnate agli incaricati del trattamento o della manutenzione.

Le autorizzazioni all'accesso sono rilasciate e revocate dal Titolare o dal Responsabile. Periodicamente, e comunque almeno una volta l'anno, dovrà essere verificata la sussistenza delle condizioni per le autorizzazioni all'accesso. L'autorizzazione all'accesso deve in ogni caso intendersi limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento o di manutenzione. È vietata l'utilizzazione di un medesimo codice identificativo personale per accedere contemporaneamente alla stessa applicazione da diverse stazioni di lavoro.

La *sala-server* va tenuta regolarmente chiusa a chiave; le chiavi della stanza devono essere detenute soltanto dal personale addetto.

Misure di sicurezza relative a documentazione e archivi cartacei

I fascicoli dei procedimenti sono conservati all'interno delle segreterie in armadi chiusi e in zone non accessibili al pubblico.

I fascicoli soggetti a frequenti movimentazioni non devono recare in copertina indicazioni che permettano di risalire al soggetto cui si riferiscono.

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

essere effettuato con modalità tali da garantire la riservatezza dei documenti e da impedire la visione di ogni dato a soggetti non autorizzati.

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

Nessuno può accedere a un archivio se non è autorizzato.

I fascicoli affidati agli incaricati del trattamento devono essere da questi ultimi conservati e custoditi con cura e restituiti al termine delle operazioni necessarie.

Nel caso in cui atti o documenti contengano dati sensibili o dati particolari, essi devono essere conservati in contenitori muniti di serratura anche da parte degli incaricati del trattamento.

I supporti non informatici contenenti la riproduzione di informazioni relative al trattamento devono essere conservati e custoditi con le modalità suddette.

I fascicoli personali devono essere custoditi con adeguata riservatezza e tenuti in armadi muniti di chiavi.

La documentazione del c.d. medico competente, così come qualsiasi documento inerente allo stato di salute o ad altri dati di analoga sensibilità, deve essere tenuta, in busta chiusa, negli armadi in uso alla competente segreteria, chiusi con chiave custodita dal sub-Responsabile della segreteria amministrativa. Conservano vigore tutte le rigorose prescrizioni di dettaglio impartite dal Dirigente amministrativo con appositi provvedimenti.

Registri e documentazione relativa al servizio intercettazioni dovranno essere custoditi con rigorosa riservatezza e, se cartacei, tenuti in armadi metallici muniti di chiavi.

Accesso all' Ufficio

L'accesso degli utenti avvocati, loro collaboratori e pubblico – può avvenire esclusivamente negli orari di apertura al pubblico. Dopo il controllo ai varchi di sicurezza, ogni persona potrà accedere esclusivamente all'ufficio competente alla trattazione della pratica di suo interesse, previo contatto del personale di vigilanza con detto ufficio o con l'ufficio di protocollo abilitato alla ricezione di atti.

Il personale di vigilanza e poi quello di segreteria sono tenuti a identificare il richiedente l'accesso mediante documento d'identità. Ai soggetti legittimati è garantito l'accesso uno per volta in modo tale da assicurare la riservatezza dei colloqui e delle richieste.

La consentita consultazione di atti di procedimenti deve avvenire comunque alla presenza del personale di segreteria competente.

E' subordinato alla specifica autorizzazione del Procuratore generale l'accesso al Palazzo di Giustizia da parte di alcune categorie di utenti: Fornitori, Giornalisti, Fotografi, Ausiliari del giudice, tirocinanti.

* * * * *

Il Dirigente amministrativo provvederà a verificare che le prassi in uso nell' Ufficio vengano adeguate a tutte le prescrizioni sopra impartite.

Si rinvia comunque ed in generale alle norme comportamentali e alle misure di sicurezza allegate, alle norme e regolamenti vigenti e alle linee guida del Garante, riguardanti la disciplina sulla riservatezza e segretezza dei dati trattati, nonché alle linee guida che saranno

successivamente comunicate e pubblicate sul sito internet istituzionale e nel sito del garante della privacy

Il presente provvedimento sarà diramato ai magistrati, al dirigente amministrativo, al personale amministrativo, agli appartenenti alla polizia giudiziaria in servizio presso la Procura Generale di Milano, nonché ai tirocinanti assegnati all'Ufficio. Sarà pubblicato nel sito internet della Procura Generale e diramato ai Sindacati, alla RSU e al medico competente.

IL PROCURATORE GENERALE

Francesca Nanni



² E' attualmente operativo account mail dedicato accessi.pg.milano@giustizia.it per l'inoltro delle istanze.

Appendice 1 al decreto del 14.7.2025 Prot. Inf. Int. n. 400/2025 del Procuratore generale della Repubblica presso la Corte d'appello di Milano

Trattamento dei dati connessi ai servizi web

I trattamenti connessi ai servizi *web* accessibili dal sito *internet* avranno luogo presso la sede della Procura generale o dell'eventuale responsabile esterno e saranno curati solo da personale incaricato del trattamento oppure da eventuali incaricati di occasionali operazioni di manutenzione.

I sistemi informatici e le procedure *software* preposte al funzionamento del sito *web* e dei servizi *on-line* messi a disposizione potranno acquisire, nel corso del loro normale esercizio, alcuni dati personali la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di *internet*.

Si tratta di informazioni che non sono raccolte per essere associate a interessati identificati, ma che per loro stessa natura potrebbero, attraverso elaborazioni ed associazioni con dati detenuti da terzi, permettere di identificare gli utenti.

In questa categoria di dati rientrano gli indirizzi IP o i nomi a dominio dei *computer* utilizzati dagli utenti che si connettono al sito, gli indirizzi in notazione URI (*Uniform Resource Identifier*) delle risorse richieste, l'orario della richiesta, il metodo utilizzato nel sottoporre la richiesta al *server*, la dimensione del *file* ottenuto in risposta, il codice numerico indicante lo stato della risposta data dal *server* (buon fine, errore, ecc.) ed altri parametri relativi al sistema operativo e all'ambiente informatico dell'utente.

Questi dati possono essere utilizzati al fine di ricavare informazioni statistiche anonime sull'uso del sito e per controllarne il corretto funzionamento e vengono cancellati immediatamente dopo l'elaborazione. I dati potrebbero essere utilizzati, dietro richiesta delle competenti Autorità, per l'eventuale accertamento di responsabilità in caso di ipotetici reati informatici ai danni del sito.

Dati forniti volontariamente dall'utente

Per l'accesso ad alcuni servizi erogati tramite il sito, potrà essere richiesto l'invio facoltativo, esplicito e volontario di posta elettronica agli indirizzi opportunamente indicati. L'eventuale richiesta comporta la successiva acquisizione dell'indirizzo del mittente, necessario per rispondere alle richieste, nonché degli eventuali altri dati personali inseriti nella missiva.

Specifiche informative di sintesi verranno eventualmente riportate o visualizzate nelle pagine del sito predisposte per particolari servizi a richiesta.

Cookies e altri sistemi di tracciamento

Nessun dato personale degli utenti verrà acquisito dal sito tramite tali strumenti.

Non verrà fatto uso di *cookies* per la trasmissione di informazioni di carattere personale, né utilizzati e.c. *cookies* persistenti di alcun tipo, ovvero sistemi per il tracciamento degli utenti.

L'uso di c.d. *cookies* di sessione (che non vengono memorizzati in modo persistente sul *computer* dell'utente e svaniscono con la chiusura del *browser*) sarà strettamente limitato alla trasmissione di identificativi di sessione (costituiti da numeri casuali generati dal *server*) necessari per consentire l'esplorazione sicura ed efficiente del sito.

I *cookies* di sessione utilizzati nel sito evitano il ricorso ad altre tecniche informatiche potenzialmente pregiudizievoli per la riservatezza della navigazione degli utenti e non consentono l'acquisizione di dati personali identificativi dell'utente.

Conferimento dei dati

Il conferimento dei dati personali indicati, ove richiesto, sarà obbligatorio, in quanto in mancanza di essi non sarà possibile dare inizio al procedimento amministrativo richiesto o all'utilizzo dei servizi resi disponibili dalla Procura generale.

A parte quanto specificato per i dati di navigazione, l'utente sarà libero di fornire i dati personali riportati nei moduli di richiesta all'Autorità o comunque indicati in contatti con l'Ufficio per sollecitare l'invio di materiale informativo o di altre comunicazioni. Il loro mancato conferimento potrebbe comportare l'impossibilità di ottenere quanto richiesto o l'accesso ai servizi disponibili.

Modalità di trattamento

I dati personali saranno trattati con strumenti automatizzati e manuali per il tempo strettamente necessario a conseguire gli scopi per cui sono stati raccolti ed in modo da garantire la riservatezza e la sicurezza degli stessi. I dati raccolti potranno essere trasmessi ad altre Autorità giudiziarie o Amministrazioni pubbliche nell'esecuzione di specifici compiti di interesse pubblico o comunque connessi all'esercizio di pubblici poteri.

Specifiche misure di sicurezza saranno osservate per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati.

Comunicazione dei dati

I dati personali acquisiti potranno essere comunicati o essere messi a disposizione a soggetti terzi. Tali soggetti agiranno in qualità di responsabili o incaricati del trattamento. I dati personali potranno essere comunicati ad altri soggetti pubblici o privati unicamente in forza di una disposizione di legge, di regolamento o di specifici protocolli d'intesa approvati dal Garante della *privacy*.

Diritti degli interessati

I soggetti cui si riferiscono i dati personali hanno il diritto in qualunque momento di ottenere la conferma dell'esistenza o meno dei medesimi dati e di conoscerne il contenuto e l'origine, verificarne l'esattezza o ottenere la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento.

È riconosciuto altresì il diritto di chiedere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, nonché di opporsi in ogni caso, per motivi legittimi, al loro trattamento.

Gli interessati che ritengono che il trattamento dei dati personali a loro riferiti avvenga in violazione di quanto previsto dal Regolamento hanno il diritto di proporre reclamo al Garante della *privacy* o di adire le opportune sedi giudiziarie.

IL PROCURATORE GENERALE

Francesca Nanni

