PROCURA DELLA REPUBBLICA
presso il
TRIBUNALE ORDINARIO DI PISA

Prot. 153125 I

Pisa, 27/11/2025

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI PERSONALI

MANUALE DI SICUREZZA PER GLI UTENTI
NOMINA INCARICATI DEL TRATTAMENTO DATI PERSONALI

Il Procuratore della Repubblica

- 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);
- 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, nonché 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*";
- Visto il D.M. 4 settembre 2025 con il quale il Ministro della Giustizia ha designato il Responsabile della protezione dei dati;
- Letta la nota del Ministero della Giustizia - Dipartimento dell'Organizzazione Giudiziaria n. 143392 in data 28 giugno 2018, in tema di titolarità del trattamento dei dati oggetto di lavorazione nei diversi Uffici nell'ambito dell'attività amministrativa;
- Vista la nota in data 22 marzo 2021, n. 9957 della Direzione Generale Sistemi Informativi Automatizzati in materia di "*Piano strategico della sicurezza*"
- Considerata la necessità di adottare un documento aggiornato alla luce delle modifiche normative intervenute;
- Richiamati gli atti di gestione con cui si sono assegnati i compiti al personale amministrativo;
- Premesso che, ai 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 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 si intende "*qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati pag. 2 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 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 alle finalità del trattamento;
  - esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione dei dati che risultino non necessari;
  - integrità e riservatezza: occorre garantire la sicurezza adeguata dei dati personali oggetto.

In qualità di "titolare" del trattamento dei dati per la Procura della Repubblica presso il Tribunale di Pisa, ai sensi e per gli effetti del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 e del Codice della privacy e succ. mod., e tenuto conto che la figura del Responsabile della Protezione dei dati (RPD) è individuata a cura del Ministero della Giustizia, con il presente documento,

DISPONE

quanto segue, limitatamente agli ambiti di pertinenza della Procura della Repubblica presso il Tribunale di Pisa e fatta salva l'autonoma competenza dell'Amministrazione Centrale per la materia amministrativa:

1. il responsabile del trattamento dei dati - art. 28 del Regolamento (UE) 2016/679 - è individuato nella persona del dott. Francesco Maio, cancelliere esperto in servizio presso la Procura della Repubblica di Pisa;
2. 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 che comportino il trattamento dei dati. In via esemplificativa i magistrati, il personale amministrativo, i collaboratori legittimamente abilitati (ad es. la polizia giudiziaria), i V.P.O, i tirocinanti e il personale esterno all'amministrazione autorizzato a operare nell'Ufficio.

   Più in particolare, sono nominati "incaricati del trattamento dei dati" tutti i magistrati, dipendenti ed utenti interni ed esterni che accedono alle Banche Dati, sulla base dei profili di autorizzazione dati, nel rispetto delle mansioni assegnate, come da ALLEGATO 1 "Elenco persone autorizzate al trattamento dei dati personali";
3. che vengano osservate le disposizioni contenute nel "Manuale operativo per la protezione dati e sicurezza informatica" come da ALLEGATO 2;
4. che venga comunicato il presente provvedimento, unitamente al Manuale operativo per la protezione dati e la sicurezza informatica, a tutte le figure interessate e pubblicato nella sezione "*Amministrazione Trasparente*" del sito web della Procura della Repubblica presso il Tribunale di Pisa.

IL PROCURATORE DELLA REPUBBLICA
Dott.ssa Teresa Angela Camelio

ALLEGATO 1

ELENCO PERSONE AUTORIZZATE AL TRATTAMENTO DEI DATI PERSONALI

MAGISTRATI

Dott. PORPORA Giovanni
Dott. RESTUCCIA Sisto
Dott. MANTOVANI Aldo
Dott. CELANO Egidio
Dott. PELOSI Fabio
Dott.ssa PAGNINI Lydia
Dott.ssa ROMANO Miriam Pamela
Dott. MALTOMINI Andrea
Dott.ssa FARRO Mariangela
Dott.ssa MARCHILI Elena (MOT) – dalla data di presa di possesso presso la Procura di Pisa

VICE PROCURATORI ONORARI

COSTABILE Massimiliano
GIANNONI Daniele
LOTTI Samantha
MOLINARO Vincenzo
MOSCA Mariangela
PEPE Giovanni
FOCOSI Gabriele
PICCHI Angela
SAVIOZZI Silvia

PERSONALE AMMINISTRATIVO

Dirigente Amministrativo
MAZZARA Rosaria

Direttore III area
POMAIOTTI Massimo
SAVIOZZI Silvia

Funzionario Giudiziario III area
BAZZANO Giuseppe
BUCCHIONI Barbara
FRASCOLLA Giulia
GEPPI Daniele
LEPORINI Arianna
MOLESTI Alessandra
ROBUSTELLI Maria

Cancelliere II area
CESENA Maria
GENNAI Niccolò
GIACALONE Arianna
MAIO Francesco
RUSSO Anna
ZAZZERI Simona

Assistente Giudiziario II area
BATTAGLINI Sonia
BURCHIANTI Alice
CARNESECCHI Paola
LEVANTINO Sabrina
RAMUNDO Gianpiero
SILVESTRI Silvia

Operatore Giudiziario II area
CARBONE Cecilia
DELLA ROSA Lorella
GALLO Carmela
GRASSINI Antonella
GUERRI Maria Palma
MANNA Maria
MODAFFERI Paola
MURICCIOLI Mara
RIGHETTI Marco
TONCELLI Milva
TUNDIS Liliana Assunta

Conducenti di automezzi II area
FANFARILLO Claudio
GENNARELLI Francisco Carmelo
TONELLI Giovanni

Ausiliario I area
BORGONOVO Barbara

SEZIONE POLIZIA GIUDIZIARIA

POLIZIA DI STATO

Isp. FILIPPI Lea (Responsabile)
Isp. DANERO Lara
Isp. DI SACCO Gabriele (C.I.T.)
Isp. BERNARDESCHI Andrea
Isp. GALASSO Giovanni
V. Isp. DE GUIDI Tiziano

Ass. C.C. CAPITINI Anna Paola
Ass. C.C. ROSSI Veronica

CARABINIERI

Lgt. GRONCHI Andrea (Responsabile)
Lgt. FARNETANI Galileo
Mar. Mag. DEL CESTA Matteo
Mar. Ord. POTENZA Rocco
Mar. Ord. GIORGI Serena
App. Sc. Q.S. BRENNA Massimiliano
App. Sc. Q.S. CORRIAS Salvatore
Car. Sc. MARZOCCA Aldo

GUARDIA DI FINANZA

Lgt. C.S. GALLEA Daniele (Responsabile)
App. Sc. Q.S. GIORDANO Giuseppe
App. Sc. Q.S. OSTUNI Luigi
Mar. Aiut. D'ANIELLO Angela (aggregata)
V. Brig. LAZZERINI Riccardo (aggregato)
Fin. GAUDIANO Annarita (aggregata)

POLIZIA LOCALE

Comm. MARANO Roberto (Pisa)
Comm. NOVI Marina (Pontedera)

POLIZIA PROVINCIALE

Comm. OLMI Sara

POLIZIA PENITENZIARIA

Isp.Sup. DE GRAZIA Angelo

ALLEGATO 2

MANUALE OPERATIVO PER LA PROTEZIONE DATI E LA SICUREZZA INFORMATICA

Il presente documento programmatico definisce le linee guida e le misure organizzative tecniche adottate dalla Procura di Pisa per la protezione dei dati personali, al fine di garantire la conformità alla normativa vigente e tutelare i diritti degli interessati.

Gli incaricati devono trattare i dati personali garantendo la massima riservatezza delle informazioni delle quali vengono in possesso, considerare tutti i dati personali come riservati e osservare le norme vigenti e le disposizioni dell'Ufficio in materia di sicurezza e riservatezza.
Gli incaricati accedono ai soli dati personali la cui conoscenza sia strettamente necessaria per il trattamento dei compiti loro assegnati. I documenti, gli atti e i fascicoli sono trattenuti dagli incaricati solo per il tempo strettamente necessario alle operazioni di trattamento.
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 che automatizzato, la massima riservatezza evitando l'accesso da parte di terzi.
Mantengono l'assoluto riserbo sui dati cui vengono a conoscenza nell'esercizio della propria funzione. In caso si debba procedere alla distruzione devono adottarsi tutte le misure volte ad evitare che i dati possano essere individuati e recuperati e che si possa conoscere il contenuto e la provenienza dei dati.
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.

Per quanto non su indicato si richiamano le disposizioni impartite in sede ministeriale e contenute nel "Piano strategico di sicurezza" (PSS).

PRESCRIZIONI PER TRATTAMENTI CON L'AUSILIO DI STRUMENTI ELETTRONICI

Di seguito i principali suggerimenti e le istruzioni per aumentare la sicurezza informatica e nel trattamento dei dati.

SPEGNERE IL COMPUTER IN CASO DI ASSENZA PER UN PERIODO DI TEMPO LUNGO

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 arrecare un danno.

NON LASCIARE LAVORI INCOMPIUTI SULLO SCHERMO

Occorre sempre chiudere le applicazioni con le quali si sta lavorando quando ci si allontana dal posto di lavoro per più di pochi minuti: un documento presente sullo schermo è vulnerabile a trattamenti non autorizzati.

SALVASCHERMO

Ogni postazione di lavoro deve avere il salvaschermo attivato, con richiesta di password per poter riprendere il controllo della postazione.

PROTEGGERE ATTENTAMENTE I DATI

Bisogna prestare particolare attenzione ai dati importanti di cui si è personalmente responsabili. Poiché può risultare difficile distinguere tra dati normali e dati importanti, è buona norma trattare i dati come se fossero importanti. Come minimo posizionarli in un'area protetta da password e non dare di default a nessun altro utente il permesso di lettura o modifica. Ai dati da condividere applicare i permessi opportuni solo per il tempo strettamente necessario all'interazione con gli altri utenti.

UTILIZZO SUPPORTI DI MEMORIA

Alla conservazione dei supporti di memoria (CD, pendrive, ecc.) si applicano gli stessi criteri di protezione dei documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può anche essere dovuto a un furto) può passare più facilmente inosservato. Occorre riporli in luogo sicuro non appena finito di usarli.

ABILITAZIONE OVE POSSIBILE DELL'ACCESSO TRAMITE PASSWORD PROTEGGERE IL COMPUTER CON PASSWORD

Tutti i computer offrono la possibilità di impostare una password all'accensione. Anche alcuni applicativi permettono di proteggere i propri dati tramite password. E' buona norma utilizzare queste caratteristiche che offrono un buon livello di riservatezza.

NON CONSENTIRE L'USO DEL COMPUTER O DELL' ACCOUNT A PERSONALE ESTERNO

Nel caso in cui personale esterno ha necessità di installare nuovi software/hardware nel vostro computer, occorre assicurarsi dell'identità della persona e delle autorizzazioni ad operare sul vostro PC.

NON UTILIZZARE APPARECCHIATURE NON AUTORIZZATE O PER CUI NON SI E' AUTORIZZATI

L'utilizzo di modem su postazioni di lavoro collegate alla rete di ufficio offre una porta d'accesso dall'esterno non solo al computer del dipendente ma a tutta la rete di cui fa parte. E', quindi, vietato l'uso di modem all'interno della rete locale. Nel caso che ciò sia strettamente necessario, disconnettere fisicamente la postazione di lavoro dalla rete locale prima di effettuare il collegamento via modem. Per l'uso di altre apparecchiature, chiedere consiglio all'amministratore di sistema.

NON INSTALLARE PROGRAMMI NON AUTORIZZATI

Oltre alla possibilità di trasferire involontariamente un virus o di introdurre un cosiddetto "cavallo di troia", va ricordato che la maggior parte dei programmi sono protetti da copyright, per cui la loro installazione può essere illegale.

DIFFIDARE DEI DATI O DEI PROGRAMMI LA CUI PROVENIENZA NON È CERTA

Per proteggersi da virus e da altri agenti attivi di attacco, occorre diffidare di tutti i dati e programmi che vi vengono inviati o consegnati, anche se la fonte appare affidabile o il contenuto molto interessante. Infatti, molti sistemi di attacco inviano dati che sembrano provenire da un utente noto al destinatario per vincerne la naturale diffidenza nei confronti degli estranei.

AMMINISTRARE CORRETTAMENTE LE PASSWORD

La scelta della password è estremamente importante per la sicurezza dei propri dati e dell'intera rete del Ministero della Giustizia. Le password debbono essere cambiate con frequenza:

- quadrimestrale, per gli account a rischio, di sistema o con elevati privilegi (inclusi amministratori, manutentori. ecc.);
- semestrale per gli account utenti;
- annuale per le password di accensione delle postazioni di lavoro.

Per la composizione della password si indica il link del GPDP dove è possibile trovare consigli per impostare password sicure e gestirle in modo accorto
https: //www.garanteprivacy.it/temi/cybersecurity/password

Tutti gli utenti, infine, debbono attenersi scrupolosamente alle seguenti prescrizioni:

- non rivelare le password a nessuno, inclusi amici e familiari;
- non condividere le password con altri colleghi o assistenti;
- non inviare le password tramite e-mail o altri metodi di comunicazione elettronica, né tramite telefono;
- non scrivere le password su carta o biglietti e non memorizzare le password su file o altri sistemi (palmari o agende elettroniche) senza cifratura;
- non scrivere la propria password su questionari o presunti moduli di sicurezza;
- non utilizzare sistemi informatici che permettono di memorizzare le password o gestire un database di password;
- non riutilizzare in nessun caso le password.

VIRUS E MISURE ANTIVIRUS

Gli utenti devono:

- usare soltanto programmi provenienti da fonti fidate perché copie sospette di programmi possono contenere virus o altro software dannoso;
- installare (o farsi installare dagli amministratori di sistema) l'ultima versione dell'antivirus e tenere aggiornati i file con gli identificativi dei virus.

Gli utenti non devono:

- visitare siti illegali (ad esempio depositi di software pirata) che sono spesso usati come specchietto per le allodole per attirare visitatori su cui condurre attacchi.

UTILIZZO POSTA ELETIRONICA

Gli utenti devono:

- usare solo il software di posta approvato dal Ministero della Giustizia;
- impedire ad altre persone di utilizzare il proprio account per inviare posta elettronica;
- trasmettere di preferenza messaggi con firma digitale.

Gli utenti non devono:

- utilizzare la posta elettronica per scopi in conflitto con il piano di sicurezza e, in ogni caso, non utilizzarla per scopi personali;
- partecipare alle cosiddette "Catene di Sant'Antonio" o, in generale, utilizzare la posta elettronica per spamming;
- inviare mai informazioni confidenziali tramite posta elettronica non cifrata;
- aprire posta elettronica di provenienza dubbia e, in generale, non aprire nessun allegato senza una preventiva scansione antivirus.

PRESCRIZIONI PER TRATTAMENTI) DATI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI (ATTI, DOCUMENTI E FASCICOLI CARTACEI)

Ciascun operatore si atterrà alle seguenti ulteriori prescrizioni:

a) occorre chiudere a chiave il proprio ufficio alla fine della giornata e in ogni caso di assenza. I documenti devono essere conservati in armadi o cassetti chiusi quando possibile;
b) i fascicoli e gli altri atti cartacei, nelle fasi di trasporto all'interno dell'ufficio, devono permanere nei corridoi il tempo strettamente necessario alla loro consegna.
c) nessuno può accedere all'archivio se non autorizzato;
d) i fascicoli e gli atti affidati agli incaricati del trattamento, devono essere da questi ultimi conservati e restituiti al termine delle operazioni da svolgere;
e) i fascicoli ubicati su scrivanie e/o piani di appoggio in genere devono essere posizionati in modo da non rendere visibili i dati (per es.: capovolti). Lo stesso accorgimento deve essere tenuto se fascicoli ed atti sono posizionati su carrelli per il loro trasporto o all'interno di autovetture;
f) le stampe di materiale riservato devono essere maneggiate e custodite con cura, evitando la possibilità di accesso alle stampe alle persone non autorizzate. Se la stampante non si trova sulla scrivania occorre ritirare le stampe nel più breve tempo possibile. Occorre distruggere personalmente le stampe quando non servono più. Evitare di gettare nel cestino le stampe di documenti che possono contenere informazioni confidenziali se si trattano dati di particolare riservatezza e, in ogni caso, non gettare mai documenti cartacei senza averli prima fatti a pezzi.

SERVIZIO DI ASSISTENZA APPLICATIVA

Il servizio di assistenza è raggiungibile attraverso i seguenti canali:

- portale: https://helpdesk.giustizia.it, cui si accede con le credenziali ADN;
- numero verde: 800749049 (attivo dal lunedì al venerdì dalle ore 8 alle ore 18 e il sabato dalle ore 8 alle ore 13), comunicando nominativo e PIN assegnato al momento della registrazione con ADN.

SANZIONI PER INOSSERVANZA DELLE NORME

Le presenti istruzioni integrano elementi di valutazione della condotta del lavoratore.
La violazione delle relative prescrizioni può generare, oltre a responsabilità penali e civili, l'irrogazione di sanzioni disciplinari, in considerazione della gravità della condotta.

Il Dirigente Amministrativo
Dott.ssa Rosaria Mazzara

Il Procuratore Della Repubblica
Dott.ssa Teresa Angela Camelio