



PROCURA GENERALE

della Corte di cassazione

ORDINE DI SERVIZIO N. 29/2023

IL PROCURATORE GENERALE

Oggetto: applicazione delle disposizioni relative al trattamento 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 (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»;

visto il d.lgs. 30 giugno 2003, n. 196, recante «Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 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», come modificato dal d.lgs. 10 agosto 2018, n. 101, recante «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)»;

visti i Decreti Ministeriali in materia di protezione e trattamento dei dati, nonché in materia di registri di cancelleria (DM 27 aprile 2009);

visto il decreto del Ministro della giustizia del 7 dicembre 2022 con il quale è stata nominata la responsabile della protezione dei dati;

richiamati, in particolare, l'art. 23 e l'art. 37, par. 1, lett. A del Regolamento e l'art. 2-*duodecies* (Limitazioni per ragioni di giustizia) introdotto dal d.lgs. n. 101/2018 a modifica del codice

in materia di protezione dei dati personali (d.lgs. n. 196/2003) in merito alla distinzione tra attività giurisdizionale e trattamento dei dati giudiziari, operati dagli uffici, non effettuati nell'esercizio di funzioni giurisdizionali;

premesso che con decreto adottato in data 12 ottobre 2004 è stata istituita presso l'Ufficio della Procura generale della Corte di cassazione la "Commissione per la sicurezza dei dati personali", con i compiti in questo stabiliti – in particolare, di attuare e vigilare sulle misure di sicurezza per il trattamento dei dati personali – e che detta Commissione è stata confermata nei Criteri organizzativi in seguito adottati e la composizione della medesima è stata modificata nel tempo, in conseguenza anche delle variazioni del personale di magistratura ed amministrativo;

premesso che, al fine della ricognizione degli archivi informatici e dell'elenco degli incaricati assegnatari di singoli elaboratori, nonché dell'elenco degli archivi anche cartacei, si rinvia alla relazione sulla sicurezza dei dati personali, anno 2022 (in particolare, altresì agli allegati alla stessa), da ritenersi qui riportata, contenente anche un'analisi dei rischi;

premesso che i trattamenti, le finalità e la proporzionalità degli stessi sono previsti normativamente, attengono ai compiti istituzionali dell'ufficio e sono, sul piano operativo, vincolati alla configurazione e strutturazione dei *software* con i quali sono gestiti i registri istituzionalmente previsti, sicché, ai fini della valutazione d'impatto rileva la valutazione dell'adeguatezza delle misure atte a scongiurare i rischi, con particolare riferimento all'inventario delle risorse, alla protezione fisica delle aree e dei locali, al controllo degli accessi informatici, al monitoraggio del sistema, alla integralità e disponibilità dei dati, alla continuità degli applicativi, alla copia storica dei dati e all'archiviazione ottica degli stessi, alla sicurezza delle reti e alle norme di comportamento degli utenti, contenuti, da ultimo nella relazione della Commissione per la sicurezza dei dati depositata il 2 marzo 2023, da ritenersi qui riportata e che verrà aggiornata annualmente;

ritenuta l'esigenza degli interventi organizzativi di cui all'art. 2-*quaterdecies* del d.lgs. n. 196 del 2003, anche al fine di aggiornare gli atti dell'Ufficio in ordine all'individuazione delle figure di riferimento previste dalla normativa e al compendio delle regole interne, apparendo congruo e possibile procedere all'individuazione della «persone fisiche espressamente designate», come richiesto da detta disposizione mediante riferimento alla funzione svolta nell'Ufficio, così da consentirne la sicura identificazione, garantendola allo stesso tempo anche in presenza di modifiche delle persone fisiche chiamate ad esercitarle (di regola non infrequenti), fermo che le presenti direttive forniscono altresì una riassuntiva disciplina di base della materia per garantire la sicurezza dei dati, ovviamente suscettibile di integrazione e modifica secondo l'evoluzione delle norme e la prassi;

ritenuto che, in linea preliminare, va premesso e ribadito che l'utilizzo dei dati personali nell'ambito dell'attività giurisdizionale in senso proprio (cui è riconducibile quella giudiziaria nell'esercizio della funzione disciplinare relativa ai magistrati) non deve eccedere le previsioni

processuali e la funzione alla stessa connessa, sicché tutte le figure operanti all'interno dell'Ufficio (magistrati, personale amministrativo e di polizia, tirocinanti) nel trattamento degli stessi devono attenersi ai limiti della normativa e delle direttive di seguito indicate e alle disposizioni di legge, astenendosi da un utilizzo non rispondente alle finalità proprie dell'attività istituzionale e dei servizi;

ritenuta l'opportunità di mantenere sia la figura dell'amministratore di sistema, non espressamente prevista dal Regolamento, ma elemento di *accountability*, sia la Commissione per la sicurezza dei dati personali, in applicazione anche del principio di precauzione;

emana la seguente

DIRETTIVA

Soggetti

Premesso che la Procura generale è titolare del trattamento dei dati relativi ai procedimenti giudiziari, fatte salve le competenze del Ministero della giustizia per il trattamento dei dati amministrativi, anche relativi al personale di magistratura, e rilevato che la figura del Responsabile della protezione dei dati (RPD) è individuata a cura del Ministero della giustizia (da ultimo con decreto del 7 dicembre 2022);

ritenuto che la designazione dei magistrati e del personale amministrativo preposti allo svolgimento dei compiti di seguito indicati va effettuata con riferimento alle funzioni svolte sulla base degli atti organizzativi dell'Ufficio, così da assicurare la continuità nello svolgimento degli stessi in caso di mutamento della persona designata a svolgere le relative funzioni, senza necessità di variare il presente documento;

DESIGNA

allo svolgimento dei compiti e delle funzioni in materia di trattamento dati, nei limiti che seguono e in relazione alle attività svolte secondo le proprie attribuzioni i seguenti soggetti:

- il Dirigente amministrativo, quale Responsabile del trattamento, con il compito di sovrintendere e vigilare sul rispetto da parte del personale amministrativo della normativa in materia di trattamento dati ed impartire le necessarie indicazioni;
- il Procuratore generale aggiunto e gli Avvocati generali, con il compito di sovrintendere e vigilare sul rispetto della normativa in materia di trattamento dei dati relativi al Servizio, all'Ufficio o, comunque, agli affari di competenza inerenti alla propria funzione organizzativa ed impartire le necessarie indicazioni ai magistrati. Il Procuratore generale, con autonomo provvedimento, può delegare il Procuratore generale aggiunto a sovrintendere alla vigilanza delle prescrizioni;
- i Direttori/Funzionari individuati nei provvedimenti organizzativi/ordini di servizio dell'Ufficio quali responsabili degli Uffici di seguito indicati, con il compito: di sovrintendere e vigilare sul

rispetto da parte degli addetti all'Ufficio della normativa in materia di trattamento dati e delle disposizioni di sicurezza; di curare il corretto utilizzo degli applicativi informatici e degli archivi cartacei nell'ambito dei rispettivi uffici e il trattamento secondo correttezza, con raccolta e registrazione di dati esclusivamente per gli scopi inerenti all'attività svolta; di adattare, eventualmente, le relative prescrizioni alle particolari esigenze degli uffici in conformità alle indicazioni ricevute dalla Responsabile del trattamento dei dati, dal Procuratore generale, dal Procuratore generale aggiunto e dagli Avvocati generali;

- Segretariato generale;
- Segreteria particolare del PG;
- Ufficio affari interni;
- Ufficio affari internazionali;
- Segreteria della Dirigente amministrativa;
- Segreteria del personale;
- Segreteria affari penali;
- Segreteria affari civili;
- Segreteria del servizio disciplinare;
- Ufficio acquisizione beni e servizi e contratti;
- Ufficio amministrazione e contabilità;
- Ufficio del protocollo;
- Ufficio documentazione;
- Ufficio del Referente per l'informatica;
- Ufficio del consegnatario;
- Ufficio Tirocini
- Ufficio automezzi.

Sono Autorizzati al trattamento dati – da effettuare secondo le disposizioni normative e di prassi, oltre che secondo le indicazioni dei soggetti sopra designati – tutti i dipendenti, il personale di magistratura e il personale amministrativo in servizio presso la Procura generale, anche in posizione di assegnazione, comando o distacco da altri uffici o corpi dell'Amministrazione, nonché i tirocinanti, gli stagisti e gli altri collaboratori legittimamente abilitati, in relazione agli affari, alle mansioni e ai compiti a ciascuno assegnati. In particolare: deve essere osservato il corretto utilizzo degli applicativi informatici e degli archivi cartacei; il trattamento va svolto secondo correttezza, con raccolta e registrazione di dati esclusivamente per gli scopi inerenti all'attività svolta; i dati vanno conservati 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 e, quindi, in caso di allontanamento anche temporaneo dal posto di lavoro, ogni incaricato e autorizzato al trattamento deve accertarsi che non sia possibile l'accesso ai dati da parte di terzi, anche se dipendenti.

L'Amministratore dei servizi informatici (ADSI), individuato, in ragione delle specifiche competenze, nella persona del responsabile tecnico dell'Ufficio referente per l'informatica, ha il compito di monitorare in maniera costante lo stato di sicurezza di tutti i processi di elaborazione e di indicare le esigenze di aggiornamento dei supporti hardware e software. In tale parte si intendono così modificati i Criteri organizzativi quanto alla designazione dell'amministratore di sistema.

La Commissione per la sicurezza dei dati personali, nella composizione individuata nei Criteri organizzativi del Triennio 2020/2022, con decorrenza 2 gennaio 2023, ha il compito di curare l'applicazione e l'osservanza delle misure di sicurezza per il trattamento dei dati personali e di individuare e realizzare le modifiche necessarie a garantirla e di acquisire, con cadenza annuale (entro il 1° marzo di ogni anno), informazioni in ordine alle posizioni informatiche e alla corretta tenuta degli archivi, oltre che di segnalare l'insorgere di criticità del sistema di sicurezza dei dati e suggerisce i possibili interventi.

Dati trattati e modalità di trattamento

Presso la Procura generale si trattano dati del personale amministrativo e di magistratura necessari per la gestione del rapporto di lavoro e ad essa connessi, nonché dati personali, anche particolari e relativi a procedimenti giudiziari, necessari per lo svolgimento della propria funzione istituzionale.

Il personale amministrativo e di magistratura è autorizzato al trattamento dei dati strettamente necessari allo svolgimento dei propri compiti, secondo le prescrizioni normative vigenti, le direttive sopra emanate e le ulteriori specifiche indicazioni ricevute, ed è tenuto allo stesso modo a garantirne l'integrità, la correttezza e la conservazione nonché la massima riservatezza, evitando che a essi possano accedere soggetti non autorizzati, in particolare nel caso di allontanamento dall'ufficio. Ogni copia informatica o cartacea di documenti o dati può essere rilasciata solo a chi dimostri di avere la titolarità a ottenerla.

Nel caso si debba procedere alla distruzione (anche parziale) di dati, cartacei o informatici, anche in copia, ferme restando le competenze e la disciplina relativa alla Commissione di scarto dell'Ufficio, la Dirigente amministrativa, l'Amministratore dei servizi informatici e la Commissione per la sicurezza dei dati personali devono adottare tutte le misure necessarie a evitare che i dati possano essere individuati o recuperati dopo la distruzione e che si possa riconoscere il contenuto o la provenienza del documento.

Misure di sicurezza relative al trattamento dati mediante apparecchiature hardware e software

L'accesso agli elaboratori in uso al personale amministrativo e di magistratura deve avvenire esclusivamente secondo i previsti profili di accesso ed è consentito sulla base di apposite autorizzazioni, rilasciate e revocate dal Procuratore generale, dal Procuratore generale aggiunto, dagli Avvocati generali, dal Dirigente amministrativo e dai Direttori/ Funzionari individuati quali responsabili degli uffici.

L'accesso agli elaboratori deve poter avvenire solo tramite l'utilizzo di una parola chiave, che va periodicamente sostituita.

Gli elaboratori non devono essere mai accessibili indistintamente ma esclusivamente secondo i previsti profili di accesso.

Gli account personali sono gestiti in modo che ne sia prevista la disattivazione in caso di perdita della qualità che consentiva l'accesso o di mancato utilizzo dei medesimi per un periodo superiore ai sei mesi.

A tal fine, il Segretario generale e il Dirigente amministrativo sono tenuti a informare tempestivamente l'Amministratore dei servizi informatici del venir meno di tale qualità.

Gli elaboratori non devono essere mai accessibili indistintamente ma esclusivamente secondo i previsti profili di accesso.

I programmi e le apparecchiature di protezione contro il rischio di intrusione o danneggiamento ad opera di terzi, sono gestiti a livello centrale dal Ministero della giustizia.

L'accesso ai programmi e alle banche dati di pertinenza esclusiva dell'Ufficio è consentito sulla base di autorizzazioni rilasciate e revocate dal Procuratore generale aggiunto, dagli Avvocati generali e dalla Dirigente amministrativa. 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.

La stanza in cui, allo stato, sono collocati i server (n. 60, 3° piano) va tenuta chiusa a chiave. Le chiavi di detta stanza sono detenute soltanto dal consegnatario e dall'Ufficio del magistrato referente per l'informatica.

Misure di sicurezza relative al trattamento dati contenuti in 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 sottoposti 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 persone non autorizzate.

I fascicoli devono essere conservati e custoditi con cura e restituiti al termine delle operazioni necessarie.

Gli incaricati e autorizzati al trattamento devono avere accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati e i fascicoli agli stessi affidati devono essere conservati e custoditi con cura e restituiti al termine delle operazioni necessarie. Nessuno può accedere a un archivio se non è autorizzato.

Gli atti e i documenti che contengano dati sensibili o dati particolari, i fascicoli personali e i supporti non informatici contenenti la riproduzione di informazioni relative al trattamento devono essere conservati in contenitori muniti di serratura anche da parte degli autorizzati al trattamento.

La documentazione del medico competente di cui al d.lgs. n. 81 del 2008 e qualsiasi altro documento inerente allo stato di salute o ad altri dati personali parimenti sensibili, deve essere tenuta, in busta chiusa, negli armadi in uso alla competente segreteria, chiusi con chiave custodita dal Direttore della segreteria amministrativa e nell'osservanza delle prescrizioni di dettaglio impartite dal Dirigente amministrativo con appositi provvedimenti.

Accesso all'Ufficio

Il personale di segreteria è tenuto a identificare il richiedente l'accesso mediante documento d'identità. L'accesso deve avvenire in modo tale da assicurare la riservatezza dei colloqui e delle richieste. La consultazione di atti di procedimenti deve avvenire comunque alla presenza del personale di segreteria competente.

Sito Web

Premesso che il Sito *Web* è gestito dalla DGsia in conformità alle linee-guida Agid sui siti, la tenuta, la vigilanza e la modalità di inserimento degli atti nel sito *web* sono (e restano) attribuite al Comitato di direzione dello stesso previsto dai Criteri organizzativi, competente a disporre detto inserimento degli atti nel sito, nell'osservanza delle disposizioni in tema di tutela della *privacy* e delle direttive contenute in detti Criteri. Le requisitorie, sia penali che civili, possono essere pubblicate dopo il deposito delle stesse presso la Cancelleria della Corte di cassazione, previo oscuramento di tutti i dati sensibili (quali, in particolare, il nome, il cognome o la denominazione delle parti e, nel caso in cui possano assumere valore identificativo, il luogo di svolgimento dei fatti o di celebrazione del processo, ovvero altri dati rilevanti al fine dell'anonimizzazione).

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

Si dispone che il presente provvedimento:

sia inoltrato a tutti i magistrati dell'Ufficio, alla Dirigente amministrativa, al personale amministrativo, ai tecnici informatici e agli appartenenti alla polizia giudiziaria in servizio presso la Procura generale, nonché ai tirocinanti assegnati all'Ufficio, alle RSU e al medico competente;

sia pubblicato nel sito internet della Procura generale della Corte di cassazione.

Il Segretario generale curerà l'allegazione del presente provvedimento ai Criteri organizzativi in vigore.

Roma, 1 giugno 2023

Il Procuratore Generale
Luigi Salvato

