Prot. U. 157 int. del 31/12/2021

TRIBUNALE DI SORVEGLIANZA DI CALTANISSETTA

per il Distretto della Corte di Appello di Caltanissetta

MISURE DI SICUREZZA PER IL TRATTAMENTO DEI DATI PERSONALI

IL PRESIDENTE DEL TRIBUNALE DI SORVEGLIANZA

Visto il regolamento (UE) n. 2016/679 *(General Data Protection Regulation),* di seguito G.D.P.R., in tema di protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati), entrato in vigore in data 25.5.2018;

Tenuto conto che a norma dell'art. 2, par. 2, lett. d) Reg. 679, **il Regolamento predetto non si applica al settore penale,** di cui, invece, si occupa la direttiva UE 2016/680 e il D. Lgs. attuativo n. 51/2018;

Visto il predetto D. Lgs. 51/2018 ("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") che detta una disciplina speculare rispetto a quella del Reg. 2016/679 e concerne il trattamento dei dati in ambito penale, prevedendone alcune norme specifiche. Il decreto, al fine di salvaguardare l'indipendenza dell'autorità giudiziaria, esclude i dati trattati da quest'ultima dal controllo del Garante per la protezione dei dati personali;

visto il D. Lgs. 10 agosto 2018 n. 101 (recante *"Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (EU) 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/CF E", noto come "Regolamento generale sulla protezione dei dati")" che ha modificato il D. Lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali);

letta la nota del Ministero della Giustizia - Dipartimento Organizzazione Giudiziaria - n. 143392 in data 28 giugno 2018 in tema di titolarità del trattamento dei dati nell'ambito dell'attività amministrativa svolta nei diversi Uffici;

viste le indicazioni fornite, con nota del 16 dicembre 2009 prot. 35909.U, dal Direttore Generale per i Sistemi Informativi Automatizzati;

vista la nota della D.G.S.I.A. ID 11606 del 13 dicembre 2018 in materia di *"Piano strategico della sicurezza ";*

Letta la circolare del 27.6.2018 n. 21611.U, con la quale il Ministero della Giustizia ha ritenuto, con riguardo alla titolarità dei dati, che "tutti i dati trattati relativi all'attività amministrativa svolta negli uffici giudiziari dovrebbero rientrare nella titolarità di questa Amministrazione", e che "altro è da dirsi, invece, per i dati giudiziari, la cui titolarità, in forza della richiamata previsione dell'art. 4, appartiene all'ufficio giudiziario" e, con riguardo alla nomina del Responsabile della Protezione dei dati (RPD), che è opportuno procedere alla nomina di un unico Responsabile a livello nazionale, sia per il trattamento dei dati c.d. amministrativi, sia per quello dei dati giudiziari;

Ritenuto, dunque, che i titolari del trattamento sono individuati a seconda che si tratti di dati relativi all'attività amministrativa svolta negli Uffici giudiziari e dati giudiziari, attribuendone la titolarità, rispettivamente, allo stesso Ministero e agli uffici giudiziari, in forza della previsione dell'art. 4 Reg. 679 ("[...] la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali") e della circostanza che "al Ministero della Giustizia compete l'organizzazione e il funzionamento dei servizi relativi alla giustizia". La individuazione di tali due distinte categorie di dati è stata concepita per comprensibili motivi di ordine istituzionale, in quanto funzionale alla individuazione dei due distinti titolari del trattamento sulla base dell'attività, amministrativa o giudiziaria, svolta e al formale riconoscimento dell'autonomia della funzione giudiziaria;

Tenuto conto, pertanto, che la titolarità del trattamento va ricondotta al singolo Ufficio giudiziario in riferimento a tutti i dati personali trattati nei procedimenti civili e penali, nell'ambito dei quali si evidenziano, per la loro autonoma categorizzazione e la loro correlata accentuata delicatezza, i dati afferenti a condanne penali, reati e le categorie particolari di cui all'art. 4 Reg. 679;

Visto il D.M. 7.8.2018, con il quale è stato nominato, ai sensi dell'art. 37, par.1 lett. a) del Regolamento europeo 2016/679, il **Responsabile della protezione dei dati per il Ministero della Giustizia** (nella persona della dott.ssa Doris Lo Moro) affidandogli, "nel rispetto di quanto previsto dall'art. 39, par. 1 Reg. 679", "i compiti e funzioni" indicati dal medesimo articolo, nonché la "tenuta del registro delle attività di trattamento";

Considerato, pertanto, che gli uffici giudiziari, in ordine alle funzioni della figura del R.P.D., non possono che fare riferimento al R.P.D. che il Ministro della Giustizia ha designato con il suo D.M. 7.8.2018, restando altrimenti privi di tale figura normativamente necessaria;

Tenuto conto dell'art. 30 Reg. UE 679, che pone l'obbligo di istituire registri, tenuti dal titolare e dai responsabili del trattamento, ove siano annotate le attività di trattamento;

Preso atto che l'art. 45 del D.L. n. 5/2012, convertito in Legge 4.4.2012, n. 35 (in G.U. n. 82 del 6.4.2012), **ha abrogato** la lett. g) del comma 1 dell'art. 34 del D. Lgs. n. 196/2003 citato - **che prevedeva, quale "misura minima", la tenuta di un aggiornato documento programmatico sulla sicurezza,** nell'ambito dei trattamenti che si avvalgono di strumenti informatici - e i paragrafi da 19 a 19.8 e 26 del disciplinare tecnico in materia di misure minime di sicurezza di cui all'allegato B del sopra richiamato D. Lgs. 196/2003;

Tenuto conto che la definizione di dato personale è fornita dall'art. 4, par. 1, Reg. 2016/679: "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»)" (identica la definizione data dall'art. 1, c. 1, lett. a) del D. Lgs. 51/2018).
Il medesimo art. 4 introduce il concetto di identificativo: "si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale".

Con il Reg. 679, la categoria dei dati sensibili, già prevista dall'art. 4, c. 1, lett. d) del testo originario del D. Lgs. 196/2003, è stata assorbita nella definizione di categorie particolari di dati personali, che godono di protezione rafforzata: "dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona" (art. 9 Reg. 679).

In **ambito penale,** in particolare, l'art. 7 del D. Lgs. 51/2018 prevede che il trattamento dei dati di cui al citato art. 9 Reg. 679 "è autorizzato solo se strettamente necessario e assistito da garanzie adeguate per i diritti e le libertà dell'interessato e specificamente previsto dal diritto dell'Unione europea o da legge [...] ovvero, ferme le garanzie dei diritti e delle libertà, se necessario per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica o se ha ad oggetto dati resi manifestamente pubblici dall'interessato";

Rilevato che, in attesa degli ulteriori necessari interventi di regolamentazione di competenza dell'Amministrazione centrale (predisposizione registri, formulazione delle modalità di compilazione ecc...), appare necessario, alla luce del nuovo assetto normativo, provvedere in merito alle regole sul trattamento dei dati in conformità alle indicazioni desumibili dalle richiamate disposizioni, nella prospettiva di una maggiore tutela dei dati personali e nella consapevolezza dei rischi relativi al trattamento degli stessi anche nell'esercizio delle attività amministrative connesse alla giurisdizione;

Ritenuto, pertanto, di dover procedere alla redazione di un documento, con contenuti ricognitivi e programmatici, sul trattamento e sicurezza dei dati personali, conformemente alla normativa europea e nazionale vigente;

DISPONE

quanto segue:

Figure professionali interne all'Ufficio interessate dal trattamento dei dati giudiziari

Il capo 4 del regolamento (UE) 2016/679 (GDPR), in attuazione del principio di "responsabilizzazione", prevede le seguenti figure:

1) "**titolare del trattamento**" dei dati è il capo dell'Ufficio giudiziario, quindi, il Presidente del

Tribunale di sorveglianza di Caltanissetta. In quanto tale, secondo il principio della "responsabilizzazione" introdotto dal Reg. 2016/679, ha il compito di adottare misure adeguate ed efficaci - in conformità alle norme nazionali e sovranazionali - volte alla protezione dei dati personali, relativamente all'attività giudiziaria e agli incombenti ad essa connessi. Egli è tenuto a vigilare sulla correttezza delle operazioni di trattamento dei dati e sull'osservanza, da parte dei responsabili ed incaricati, delle istruzioni impartite in materia, nonché sull'attuazione del presente documento.

Non è responsabile del trattamento dei dati relativi all'attività amministrativa svolta negli Uffici giudiziari, rientrante nella titolarità del Ministero della giustizia, secondo la nota del Capo di Gabinetto del Ministero della giustizia del 27.6.2018 e del D.M. 7.8.2018;

2) **"responsabili del trattamento"** dei dati giudiziari sono tutti coloro che elaborano i dati personali "per conto" del titolare del trattamento (artt. 4.8 Reg.2016/ 679 e 2.2. lett. I D.L. vo 51/2018);
3) **"responsabile della protezione dei dati personali"** riferibili all'attività giudiziaria è il MAGRIF dell'Ufficio;
4) **"incaricati del trattamento dei dati"** sono tutti i Magistrati, gli esperti e tutti i dipendenti amministrativi, in servizio nell'Ufficio, che accedono ad affari di pertinenza dell'Ufficio medesimo per l'esecuzione materiale di operazioni di trattamento, ciascuno in relazione all'attività istituzionalmente svolta e nell'ambito dei trattamenti consentiti, nonché gli addetti esterni a cui è consentito l'accesso a documenti cartacei e informatizzati;
5) **"responsabili amministrativi"** sono tenuti a proporre al titolare o al responsabile del trattamento i nominativi degli incaricati da accreditare o di coloro che devono essere disabilitati in caso di trasferimento presso altri Uffici giudiziari, nonché tutte le eventuali modifiche ai profili utente;
6) **"incaricati amministrativi"** sono i dipendenti amministrativi che eseguono materialmente il trattamento dei dati sensibili sotto la vigilanza dei responsabili amministrativi.

Con particolare riferimento alla figura degli incaricati del trattamento dei dati, tenuto conto della posizione all'interno dell'Ufficio ed in stretta correlazione con le specifiche responsabilità che afferiscono alla posizione stessa, anche sotto il profilo della distinzione tra attività giurisdizionale e attività amministrativa, i magistrati, gli esperti, i funzionari cui è affidata la direzione di un settore svolgono anche attività di vigilanza sul rispetto delle misure di sicurezza da parte degli incaricati del trattamento e di coordinamento delle attività, funzionale alla osservanza uniforme delle regole che presiedono alla protezione dei dati personali e alla sicurezza informatica.

Gli incaricati del trattamento devono osservare puntualmente le disposizioni contenute nel presente provvedimento nonché le vigenti prescrizioni in materia di sicurezza.
Tale attività di controllo riveste particolare importanza anche in considerazione della delicatezza e complessità dei programmi in uso e della necessità di realizzare e conservare l'integrità e correttezza dei dati ai fini della efficace digitalizzazione della giustizia.

Sono trattati i seguenti dati personali:

-Dati relativi al personale dipendente dell'ufficio;
-Dati relativi alle persone fisiche, persone giuridiche, enti o associazioni identificati o identificabili, anche indirettamente mediante riferimento a qualsiasi altra informazione, che vengono comunicati all'ufficio per motivi istituzionali o di servizio.
Si indicano a scopo esemplificativo:

- i dati relativi ai Magistrati dell'Ufficio e alle persone che svolgono funzioni giudiziarie in qualità di esperti del Tribunale di sorveglianza;
- i dati del personale in servizio presso l'ufficio;
- i dati delle ditte fornitrici;
- delle persone non dipendenti che, a qualsiasi titolo prestano servizi nell'ambito della struttura giudiziaria;
- i dati relativi a dipendenti che hanno prestato servizio in passato presso l'ufficio e che sono stati trasferiti, transitati verso altre amministrazioni o cessati dal servizio.

I rischi che incombono sui dati sono:

1. Eventi naturali e comportamenti umani: i dati devono essere disponibili per gli utenti autorizzati e devono essere messe in atto le misure idonee ad evitare che eventi naturali quali incendi, allagamenti e terremoti ed umani, quali attentati, riducano la disponibilità;
2. Comportamenti colposi o dolosi che compromettono **l'integrità dei dati**: i dati possono essere elaborati, modificati, cancellati solo dalle persone autorizzate. La registrazione, l'elaborazione, la modifica, la cancellazione e le altre operazioni sui dati possono essere svolte solo dai dipendenti autorizzati con ordine di servizio o altro provvedimento.

3. Comportamenti che compromettono **l'autenticità dei dati**: deve essere certificata e garantita la provenienza dei dati. I certificati e gli altri documenti sono rilasciati secondo procedure validate e dalle persone autorizzate.

4. Comportamenti che compromettono la **riservatezza di dati**: i dati personali e quelli giudiziari devono essere trattati secondo i principi di cui alle norme vigenti ed, in particolare, del D. Lvo n. 196 del 2003 come modificato dal D. L.vo 101/2018. Le informazioni possono essere fruite solo dalle persone legittimate ed è vietata la diffusione e la comunicazione a persone diverse da quelle autorizzate.

In relazione all'attività di trattamento dei dati, ciascun soggetto autorizzato si deve impegnare a:

- trattare i soli dati la cui conoscenza sia necessaria e sufficiente per lo svolgimento delle operazioni da effettuare;
- conservare i supporti informatici e/o cartacei contenenti dati personali in modo da evitare che siano accessibili a persone non autorizzate al trattamento dei dati medesimi o siano facilmente oggetto di danneggiamenti intenzionali o accidentali;
- restituire al termine delle operazioni affidate gli atti e documenti cartacei contenenti dati personali e loro copie;
- effettuare copie dei dati personali oggetto di trattamento esclusivamente se necessario e previa autorizzazione del titolare o responsabile del trattamento o suo soggetto designato;
- effettuare le operazioni di trattamento dei dati personali nel rispetto della normativa vigente e delle misure tecniche e organizzative adeguate al livello sicurezza a cui può essere esposto il trattamento;
- segnalare al titolare o responsabile del trattamento o suo soggetto designato eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità di raccolta;
- dare immediata comunicazione al titolare o responsabile del trattamento in tutti i casi in cui si rilevi o si sospetti una violazione dei dati personali;
- effettuare la comunicazione dei dati esclusivamente ai soggetti indicati dal titolare o dal responsabile del trattamento o suo soggetto designato e secondo le modalità stabilite dai medesimi;

- mantenere, salvo quanto precisato al punto precedente, la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento dell'incarico, per tutta la durata del medesimo ed anche successivamente ad esso;
- fornire al titolare o responsabile del trattamento o suo soggetto designato, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentirgli di svolgere efficacemente la propria attività di controllo;
- prestare la più ampia e completa collaborazione al titolare o responsabile del trattamento o suo soggetto designato, al fine di compiere quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente.

Registri dei trattamenti

L'art. 30, par. 1 lett. a) reg. 679 e l'art. 20 del D. Lgs. 51/2018, sostanzialmente identici, prevedono, a cura del titolare del trattamento, la tenuta di *Registri delle attività di trattamento*; come sopra evidenziato, il Ministero della Giustizia ha individuato, con D.M. 7.8.2018, un R.P.D. al quale ha affidato anche la *"tenuta del registro delle attività di trattamento*. Con lo stesso D.M., il Ministro ha precisato che "*i compiti del RPD attengono all'insieme del trattamento dei dati effettuati dal Ministero della Giustizia"*.

Le incertezze in ordine alla portata delle competenze del R.P.D. si ripercuotono sulla individuazione dei registri dei trattamenti da tenere presso gli uffici giudiziari. La circostanza che titolare del trattamento dei dati relativi all'attività amministrativa degli uffici giudiziari sia il Ministero della Giustizia rende, ad oggi, dubbia l'obbligatorietà del singolo Ufficio giudiziario della tenuta del registro per il trattamento di tali dati, atteso che la normativa prevede che sia il titolare del trattamento a dover tenere il registro (o il R.P.D., su incarico del titolare).

Appare, pertanto, opportuno attendere direttive ministeriali che meglio definiscano i modelli eventualmente da adottare per gli uffici giudiziari.

Elenco dei trattamenti.

L'art. 5 del Reg. n. 679/2016 elenca i "principi applicabili al trattamento di dati personali ": a) liceità, correttezza e trasparenza; b) limitazione della finalità; c) minimizzazione dei dati; d) esattezza; e) limitazione della conservazione; f) integrità e riservatezza; g) responsabilizzazione.

Il personale amministrativo è abilitato, in funzione esclusiva dei compiti svolti da ciascuno, al trattamento dei dati personali nell'ambito di:

a) iscrizioni e annotazioni - anche informatiche - nei registri ufficiali generali, nelle rubriche prescritte, nei registri di comodo e nei registri di passaggio; dette annotazioni e iscrizioni devono peraltro essere corrette e complete;

b) iscrizioni e annotazioni sulle copertine dei fascicoli;

c) comunicazioni su supporto cartaceo, telematico e/o con mezzi di comunicazione a distanza con altri uffici giudiziari e nell'ambito dell'ufficio;

d) comunicazioni relative all'informazione processuale;

e) archiviazione di atti e documenti;

f) ricezione e inoltro della corrispondenza di ufficio, anche in via telematica;

g) attività amministrativa relativa alla gestione del personale di magistratura e amministrativo;

h) attività residuale concernente i compiti istituzionali dell'ufficio.

Le attività di cui ai punti a), b), c), e d) riguardano prevalentemente od esclusivamente le cancellerie; l'attività di cui al punto e) riguarda sia le cancellerie che le segreterie della presidenza e della dirigenza amministrativa; i punti f), g) ed h) riguardano le appena citate segreterie.

Tanto premesso, le **"misure minime"** generali adottate, presso il Tribunale e l'Ufficio di sorveglianza di Caltanissetta, per la protezione dei dati trattati su supporti informatici o cartacei, ai sensi del D. L.vo 196/2003 (Codice della privacy), sono state e continuano ad essere le seguenti:

a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;

b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;

c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

Tutti i fascicoli in istruttoria vengono conservati in armadi, ubicati all'interno delle cancellerie e custoditi dal personale incaricato; successivamente, non appena completata l'istruttoria, vengono consegnati al magistrato relatore e conservati nella relativa stanza.

L'avvocato che intende visionare il fascicolo si rivolge alla cancelleria e prende visione del fascicolo in cancelleria, in presenza dell'addetto incaricato del servizio.

In caso di richieste di copie, il rilascio è subordinato alla previa autorizzazione del Magistrato e al pagamento dei relativi diritti di copia.

Appena emesso il provvedimento, si provvede alla sua esecuzione. Il fascicolo viene, quindi, custodito in cancelleria in attesa delle notifiche, per essere successivamente conservato prima in

archivio corrente e poi in archivio storico.
I locali archivio sono distinti per Tribunale e Ufficio di sorveglianza e la conservazione dei relativi atti è affidata a due unità lavorative di cui una si occupa dell'archivio del Tribunale e l'altra dell'archivio dell'Ufficio.
La movimentazione viene poi comunicata all'assistente incaricato dell'aggiornamento del registro archivio.
In archivio vi accede solo personale autorizzato.

In ottemperanza al D. L.vo 101/2018, le "**misure adeguate**" più specifiche ed efficaci per il trattamento dei **dati senza l'ausilio di strumenti elettronici** (contenuti, quindi, in documenti cartacei), cui gli incaricati del trattamento si devono attenere, sono le seguenti:

- i fascicoli cartacei, durante il trasporto all'interno dell'Ufficio, devono permanere nei corridoi il tempo strettamente necessario per la loro consegna al dipendente destinatario della lavorazione degli stessi. I fascicoli riposti nei carrelli di trasporto non possono sostare incustoditi nei corridoi e su di essi l'incaricato deve vigilare costantemente fino alla consegna al destinatario;
- gli incaricati devono avere accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati;
- l'accesso ai locali adibiti ad archivio è consentito solo al personale che per disposizione di servizio è addetto ad essi ed a soggetti diversi che operano sotto la vigilanza del suddetto personale o vengono autorizzati dai preposti; il trasporto di atti da e per l'archivio deve essere eseguito in modo da evitarne l'accesso da parte di persone non autorizzate;
- in ugual modo si procederà nella produzione di copie di atti: gli incaricati dovranno vigilare che durante la fase della riproduzione in copie di atti o documenti, nessun soggetto estraneo possa prendere visione degli stessi, ad eccezione dei periti nominati dal Tribunale o dal Magistrato di sorveglianza che avranno interesse a visionare i fascicoli per procedere all'acquisizione delle copie di documenti contenuti nei fascicoli per svolgere la loro attività giudiziaria di ausilio;
- i fascicoli, se affidati agli incaricati del trattamento, devono essere da questi ultimi conservati, curati personalmente e riservatamente dagli stessi o comunque da dipendenti dell'Ufficio per l'eventuale attività finalizzata alla riproduzione fotostatica di atti e restituiti al termine delle operazioni affidate;
- gli atti e documenti contenenti dati sensibili, affidati agli incaricati del trattamento,

devono essere conservati, fino alla restituzione, in armadi dagli stessi custoditi e, ove possibile, muniti di serratura; particolare attenzione deve essere prestata ai fascicoli e agli atti provenienti dalle Procure della Repubblica e dalla Procura Generale che devono essere trattati e movimentati esclusivamente dal personale incaricato di eseguire i prescritti adempimenti e conservati in armadi ben custoditi e possibilmente chiusi a chiave sino alla restituzione alle Procure stesse con registro di passaggio;

- analogamente si deve procedere con riferimento ai fascicoli destinati alla Procura della Repubblica di Caltanissetta o alla Procura Generale per i prescritti pareri. Anche in tal caso la movimentazione dev'essere annotata nel registro di passaggio.

I fascicoli personali dei Magistrati ordinari, anche in tirocinio, devono essere custoditi nella cassaforte blindata posta nella stanza in uso al Direttore in servizio, dott.ssa Franca Quattrocchi, mentre **i fascicoli personali dei dipendenti** sono custoditi in armadio munito di chiave sempre all'interno della medesima stanza del Direttore.

I **dati relativi alla gestione delle presenze del personale** devono essere trattati esclusivamente dagli addetti, sotto la vigilanza del responsabile, compreso l'accesso al sistema informatizzato di gestione, dal quale ciascun dipendente deve poter ricavare esclusivamente le informazioni che lo riguardano.

Le cartelle sanitarie sia del personale amministrativo sia dei Magistrati devono essere custodite nella cassaforte nella stanza del Direttore.
La documentazione relativa alla fissazione delle visite mediche, invece, deve essere conservata in armadi muniti di chiave posti nella stanza del Direttore.
L'accesso ai suddetti documenti è consentito esclusivamente agli organi di vigilanza ed al medico competente.

Oltre ai fascicoli personali dei dipendenti, anche quelli comunque contenenti dati personali, quali la corresponsione di emolumenti accessori, devono essere conservati in spazi accessibili solo al Direttore, in armadi all'interno della stanza in suo uso.

La **documentazione relativa alle assenze dei dipendenti** dev'essere custodita in spazi riservati e non accessibili al pubblico, posti nella segreteria della Presidenza e possono essere diffusi, anonimamente, solo per uso statistico.

I dati relativi ai buoni pasto devono essere custoditi in luogo riservato ed accessibile solo al Direttore e all'addetta alla segreteria (Assistente giudiziario, Sig.ra Sabrina Anzalone) ed utilizzati esclusivamente per le richieste di fornitura e per eventuali adempimenti statistici.

Tutta la documentazione inerente agli **acquisiti d'ufficio** sul Mepa o di competenza della Conferenza Permanente per importi inferiori a € 5.000 dev'essere custodita negli armadi della stanza del Direttore, mentre la documentazione inerente gli altri servizi amministrativi distribuiti ai Funzionari giudiziari è custodita negli armadi delle stanze in loro uso.

I Funzionari giudiziari, per i servizi amministrativi di loro competenza secondo l'Ordine di servizio, sono tenuti alla custodia delle pratiche contenenti dati sensibili, riponendo le stesse negli armadi situati nelle stanze in loro uso ed impedendone la presa e/o la visione a soggetti non incaricati e non autorizzati.

Quanto al **trattamento dei dati contenuti su supporti informatici**, particolare attenzione va posta alle regole di comportamento al fine di garantire la "sicurezza informatica" nei suoi tre diversi aspetti della riservatezza, della integrità e della disponibilità.
In ordine al primo aspetto della "riservatezza", ovvero della prevenzione di accessi non autorizzati alle informazioni, tutti i dati dell'Ufficio sono archiviati nella sala server ubicata al primo piano dello stabile dove si trovano il Tribunale e l'Ufficio di sorveglianza.
La stessa è dotata di impianto antincendio, impianto di condizionamento, porta blindata, con apertura tramite badge o chiave.
L'accesso alla sala server è consentito solo a personale autorizzato.
All'interno della sala server sono custoditi i supporti di back-up delle cartelle condivise e tutte le apparecchiature con basi dati sensibili, nonchè le apparecchiature di rete.
In ordine al secondo aspetto della "integrità", secondo cui le informazioni non devono essere alterabili da incidenti o abusi, si specifica che tutte le postazioni dell'Ufficio, compreso il server, hanno installato il software antivirus fornito dal Ministero della Giustizia. Gli aggiornamenti avvengono periodicamente e in modo automatico nei P.C. anche portatili presenti nell'Ufficio e collegati con la RUG.

In caso di sostituzione o riparazione dei P.C., vengono trattenuti dall'Ufficio i relativi *Hard Disk*; mentre, in caso di dismissione di un P.C., si procede con la cancellazione dei dati o con la distruzione fisica dei supporti di memorizzazione.

La rete interna dell'Ufficio è protetta dal traffico esterno da un Firewall.

Il personale è tenuto a non diffondere messaggi e-mail di dubbia provenienza e a non partecipare a catene di Sant'Antonio, a non permettere l'uso delle apparecchiature a personale esterno, a non utilizzare giochi, software peer to peer e per le Chat. E ciò in aggiunta alle limitazioni ministeriali introdotte attraverso la centralizzazione dei server proxy.

Sotto il profilo della "disponibilità" dei dati, per l'accesso al dominio "Utenti" si deve utilizzare, in via esclusiva, l'infrastruttura di autenticazione ADN.

Tutte le postazioni di lavoro sono protette da una password di accensione.

Con la migrazione degli utenti su ADN, la gestione delle password avviene a livello centrale.

Tutto il personale amministrativo e togato è tenuto al rinnovo delle password di accesso al P.C. semestralmente e, nel caso di smarrimento o dimenticanza, può effettuare una chiamata all'Help Desk per il relativo reset.

L'accesso ai vari applicativi è possibile solo mediante utilizzo di apposite credenziali composte da codici associati a parole chiave (normalmente username e password).

Il personale tutto è tenuto alla segretezza delle password che non devono essere annotate su fogli facilmente leggibili da altri soggetti né comunicate a terzi, neanche in occasione degli interventi sistemistici.

E' fatto divieto di installare nei P.C., anche portatili, dei software non autorizzati dalla D.G.S.I.A. o software che non risultino utili alle attività degli utenti (Magistrati, personale amministrativo, tirocinanti, stagisti ecc...).

Il consegnatario informatico deve mantenere l'elenco aggiornato di tutte le attrezzature informatiche dell'Ufficio, della loro destinazione, della loro collocazione materiale e dei nomi macchina.

In caso di distruzione o danneggiamento delle informazioni o di strumenti elettronici, il servizio di assistenza sistemistica, secondo le indicazioni della D.I.G.S.I.A., deve adottare le modalità di ripristino dei dati nel minor tempo possibile.

Assistenza sistemistica e applicativa. Incaricati del servizio di assistenza

Gli incaricati del servizio di assistenza sono gli assistenti tecnici che quotidianamente transitano presso l'Ufficio (Sig.ri Gianluca Callari e Vincenzo Navarra).

Per richiedere l'assistenza sistemistica, occorre seguire le istruzioni riportate nell'apposita pagina intranet da cui risultano:

numero verde: 800.868.444

e-mail: spocgiustizia@telecomitalia.it

Va, inoltre, ricordato che, con nota 23444.U del 15.10.2013, la D.G.S.I.A. ha fatto presente che il contratto di assistenza sistemistica e applicativa prevede, su richiesta dell'utente interessato, la possibilità di accedere da remoto sulla singola postazione di lavoro con le modalità indicate nella medesima nota.

Gli interventi finalizzati a preservare l'operatività e la sicurezza del sistema possono essere effettuati in assenza o impedimento dell'utente solo nel caso in cui presentino carattere di indispensabilità e indifferibilità; tale valutazione sarà previamente effettuata dal vertice giudiziario e/o amministrativo dell'ufficio, al quale dovrà essere tempestivamente richiesta specifica autorizzazione; all'interessato sarà data prontamente notizia dell'effettuato intervento a cura del responsabile della segreteria della dirigenza amministrativa , su impulso del soggetto che ha autorizzato l'intervento.

Alcuni interventi dei sistemisti sono realizzati in remoto, attraverso lo strumento BOMGAR.

Nello svolgimento dei loro compiti, i sistemisti, come tutti gli incaricati del trattamento, sono obbligati alla massima riservatezza.

Trattamento dei dati personali e udienze; accesso dei difensori alle cancellerie.

Le udienze del Tribunale e dell'Ufficio di sorveglianza sono celebrate, per la quasi totalità, a porte chiuse, secondo il rito camerale (l'udienza pubblica viene celebrata solo su espressa richiesta).

Pertanto, il ruolo di udienza dev'essere affisso all'ingresso dell'Ufficio e pubblicato nel sito web del Tribunale di sorveglianza in modo anonimo, senza indicazione dei nomi dei soggetti interessati, con la semplice indicazione del numero di registro generale e del difensore.

In ordine alla problematica relativa all'accesso dei difensori in cancelleria, la deliberazione del C.S.M. n. 294/2007 ha osservato che "il quadro normativo vigente, pur consentendo alcune deroghe all'applicazione della normativa sulla privacy, atteso che la predisposizione dei ruoli di udienza e l'accesso dei difensori alle cancellerie rientrano tra le attività svolte per ragioni di giustizia, comunque impone adeguati accorgimenti finalizzati a tutelare la riservatezza delle parti nei confronti di chi non abbia alcun interesse processuale sulle controversie che riguardino queste ultime".

E' dunque necessario: evitare in tutti i modi che "trapelino notizie sui processi a favore di persone non espressamente portatrici di interessi processuali sugli stessi"; attivarsi in modo che "le scrivanie

degli operatori siano sistemate in modo da non rendere immediatamente accessibile a chicchessia l'accesso alle scansie contenenti i fascicoli non ancora definititi"; aver cura nella custodia degli archivi; "rilasciare informazioni solo ai difensori muniti di mandato ed ai loro stretti collaboratori".

Trattamento dei dati personali relativo all'utilizzo della posta elettronica e della rete internet; disciplinare interno ex provvedimento del Garante per la protezione dei dati personali in data 1° marzo 2007.

Il provvedimento 1.3.2007 del Garante per la protezione dei dati personali ha segnalato la necessità di preservare adeguatamente la riservatezza dei lavoratori con riguardo all'utilizzo della posta elettronica e della rete internet e l'opportunità che sia redatto un disciplinare interno alla struttura.
Premesso che la posta elettronica, per gli utenti abilitati in ragione del servizio svolto, è funzionale ad una maggiore rapidità ed efficacia della comunicazione, sia tra addetti all'ufficio, sia tra addetti e soggetti allo stesso estranei; che la finalità istituzionale non può non costituire connotato assolutamente preminente dell'utilizzo di detta modalità elettronica di comunicazione; che, peraltro, non può essere sottaciuto che la posta elettronica ha natura e sostanza di "corrispondenza ", con tutte le inevitabili implicazioni in termini di pregnante riferimento del contenuto dei messaggi elettronici alla persona umana in quanto tale; che messaggi, formalmente o apparentemente avulsi da un contesto propriamente prestazionale, sono, tuttavia, spesso occasionati immediatamente dall'attività lavorativa e contribuiscono a realizzare quel clima di serenità e di virtuosa confidenzialità capace di favorire una collaborazione più efficace per il servizio; che non è preventivabile con certezza che, con riguardo a ciascun utente abilitato, il collegamento a soli siti istituzionali esaurisca le esigenze connesse con il servizio; che non sussistono esigenze particolari che consiglino controlli ulteriori rispetto a quelli che già prevede il sistema, si ritiene opportuno formalizzare il seguente disciplinare:
a) la posta elettronica, cui hanno accesso i soggetti formalmente abilitati per ragioni di servizio, deve essere utilizzata - avendo l'accortezza di non divulgare notizie riservate o dati personali il cui trattamento si riveli eccedente o non pertinente - per motivi direttamente riconducibili alla prestazione lavorativa, o dalla medesima prestazione occasionati nel senso sopra precisato; in tale ultima ipotesi l'utilizzo avviene sotto la personale responsabilità dell'intestatario dell'utenza di posta elettronica;
b) l'utilizzo della rete internet, per i soggetti formalmente abilitati per ragioni di servizio, è finalizzato alla acquisizione, attraverso la connessione a siti prevalentemente istituzionali e comunque di sicura affidabilità, di notizie e conoscenze necessarie o utili per il servizio svolto;

c) la finalità istituzionale che connota l'utilizzo della rete e la non inerenza alla specificità dell'utente-persona fisica esclude la possibilità del download di file musicali o multimediali;
d) i sistemisti hanno l'obbligo (come espressamente raccomandato dal provvedimento 1°.3.2007 del Garante) di svolgere solo operazioni strettamente necessarie al perseguimento delle finalità specifiche di manutenzione e sicurezza, senza realizzare attività di controllo a distanza, anche di propria iniziativa;
e) è necessario che i file di lavoro, non inerenti a programmi informatici, siano dallo stesso utente salvati e conservati, anche con riguardo alla posta elettronica e ad internet, in quantità tendenzialmente limitata, onde evitare, nell'interesse proprio e dell'ufficio, che la sovrabbondanza di dati contenuti nei file di ordinario lavoro comprometta le operazioni di back-up;
f) i limiti istituzionali di utilizzo della posta elettronica e della rete internet sono assistiti dai controlli effettuabili dal personale a ciò autorizzato dall'Amministrazione centrale, sulla base dell'analisi dei tracciamenti preordinati dal sistema adottato dall'Amministrazione stessa, ai quali l'ufficio non ha possibilità di autonomo e diretto accesso.

Trattamento dei dati personali nella riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica.

Con nota prot. n. 34296.U del 10.3.2011, il Ministero della Giustizia ha trasmesso la deliberazione del Garante per la protezione dei dati personali del 2.12.2010, con la quale sono state dettate prescrizioni sul trattamento dei dati riguardanti la riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica.
Per quanto la normativa sia stata oggetto di importanti modifiche e per quanto l'art. 47 del codice della privacy dal quale traeva spunto detta deliberazione sia stato abrogato dal D. Lgs. 101/2018 (le norme di riferimento, in luogo dell'art.47 predetto, possono ora essere considerate quelle contenute nell'art. 2-duodecies del D. Lgs. 101/2018, commi 1 e 3), le prescrizioni del Garante sono da considerarsi vigenti.
Premesso che le linee guida adottate dal Garante del trattamento dei dati personali riguardano esclusivamente l'attività di informazione giuridica e che restano, pertanto, esclusi dal relativo ambito di afferenza i trattamenti non effettuati per ragioni di giustizia ("si intendono effettuati per ragioni di giustizia i trattamenti di dati personali correlati alla trattazione giudiziaria di affari e di controversie, i trattamenti effettuati in materia di trattamento giuridico ed economico del personale di magistratura, nonché i trattamenti svolti nell'ambito delle attività' ispettive su uffici giudiziari", comma 4 dell'art. 2-duodecies richiamato) e che "le presenti linee guida non incidono sulle norme

processuali", come dichiara la deliberazione del Garante, il contenuto di dette linee-guida può essere così essere precisato:

- presupposto per l'applicazione delle misure prescritte è l'avvenuta pubblicazione del provvedimento dell'Autorità Giudiziaria (dal Garante definita, a tal fine, < onere >);
- a norma dell'art. 52, commi 1 e 2 del codice della privacy (tuttora in vigore), "l'interessato può chiedere per motivi legittimi, con richiesta depositata nella cancelleria o segreteria dell'ufficio ...che sia apposta a cura della cancelleria o segreteria ... un 'annotazione volta a precludere ... l'indicazione delle generalità e di altri dati identificativi..."
- la competenza a decidere sull'istanza spetta all'Autorità Giudiziaria presso cui pende il giudizio, che provvederà con decreto;
- l'annotazione in discorso può essere disposta dal magistrato anche di ufficio (comma2);
- in caso di accoglimento della richiesta, spetta alla cancelleria o segreteria giudiziaria darvi esecuzione; in attesa della eventuale acquisizione del timbro cui fa riferimento la deliberazione del Garante, gli addetti provvederanno ad annotare per iscritto la formula indicata "In caso di diffusione, omettere, a norma dell'art. 52 d. lgs. 19612003, le generalità e gli altri dati identificativi ... ";
- non sussistono a carico della cancelleria o segreteria ulteriori obblighi; in particolare, non sussiste l'obbligo di cancellare materialmente i dati dell'interessato sulle copie dei provvedimenti rilasciate a chi ne abbia diritto e che riportino la menzionata annotazione;
- in caso di accoglimento della richiesta o di decisione d'ufficio da parte del magistrato, la prescrizione in ordine alla anonimizzazione vincola tutti i soggetti che svolgono attività di diffusione e riguarda anche le massime giuridiche;
- con riferimento a quanto previsto dal comma 5 dell'art. 52 codice privacy, il Garante ha precisato, in particolare, quanto segue: "In relazione a quesiti che sono stati posti con riferimento ad alcuni particolari profili del divieto posto dal comma 5 dell'art. 52, deve essere, in primo luogo, chiarito che il divieto di diffusione delle generalità, degli altri dati identificativi e degli ulteriori dati che consentano di identificare i minori o le parti nei procedimenti in materia di rapporti di famiglia e di stato delle persone non può, ovviamente, trovare applicazione ove la lettura della sentenza o di altro provvedimento non permetta, facendo applicazione dell'ordinaria diligenza, di individuare il coinvolgimento di un minore o delle parti dei menzionati procedimenti. Ciò chiarito, si precisa che:
- la disposizione intende fare riferimento non solo alla sentenza o altro provvedimento emessi nel procedimento in cui è coinvolto il minore o in materia di rapporti di famiglia e di stato delle persone, ma anche a qualsiasi sentenza o altro provvedimento che contenga dati personali, anche di terzi, che consentono, "anche indirettamente", di svelare l'identità delle persone tutelate;

- la norma richiede ai soggetti che diffondono i provvedimenti per finalità di informazione giuridica di esercitare un'ordinaria diligenza nell'esame del testo delle sentenze e degli altri provvedimenti. In particolare, rientrano nell'oggetto del divieto le informazioni che, nella valutazione della fattispecie concreta, permettano di risalire agevolmente all'identificazione del minore o delle parti nei giudizi in questione (ad esempio, i nominativi dei genitori del minore o la scuola da questo frequentata, o l'indirizzo dell'abitazione delle parti processuali)".

Raccomandazioni della D.G.S.I.A.

Con nota 9353.U, in data 23.3.2009, la Direzione Generale S.I.A. ha raccomandato di "sensibilizzare il personale nel porre la dovuta attenzione nell'attività di inserimento dei dati nei sistemi informatici, giacché buona parte degli interventi di assistenza applicativa risultano dovuti ad errori e/o inesattezze nell'attività di data-entry effettuata dal personale dell'amministrazione e non a problematiche tecniche del sistema informatico"; in particolare per quanto concerne il settore penale, con circolare a firma dei Direttori Generali della Giustizia Penale e dei Sistemi Informativi Automatizzati prot. n. 78341.U del 11.6.2013, diramata in sede di informatizzazione dei registri penali tramite il S.I.C.P., sono state raccomandate agli uffici l'immediatezza, l'esaustività e la correttezza delle annotazioni e dell'inserimento dei dati, così da realizzare il loro allineamento e corrispondenza e rendere possibile lo scambio di informazioni provenienti dai diversi uffici.
L'inserimento dei predetti passi delle richiamate note ministeriali nel presente provvedimento è finalizzato all'ulteriore sensibilizzazione del personale sulla necessità di svolgere con attenzione l'attività di data-entry. Si richiama anche l'attività di controllo sull'utilizzo dei programmi informatici, di cui al paragrafo 2), demandata ai responsabili delle cancellerie.

L' informativa ex artt. 13 e 14 Reg. 679/2016.

L'informativa è una comunicazione 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. Essa costituisce un obbligo dei titolari del trattamento "*propedeutico alla legittimità del trattamento stesso*".
Il diritto di ricevere informazioni durante il trattamento è disciplinato dall'art. 15 Reg. 679/2016.
I contenuti dell'informativa sono elencati in modo tassativo negli artt. 13, par. 1, e 14, paragrafo 1, Reg. 679.
Tenuto conto anche della normativa vigente, di quanto indicato dal Garante e di quanto pubblicato

dal sito del Ministero della Giustizia, l'informativa da rendere a cura degli uffici giudiziari è necessario che contenga:

- le fonti normative in materia di privacy;
- l'identità e i dati di contatto del titolare del trattamento del responsabile della protezione dei dati (RPD);
- la base giuridica e le finalità del trattamento (individuate già a livello normativo, in riferimento ai compiti istituzionali);
- le modalità di trattamento (con indicazioni particolari riguardanti le procedure selettive – tirocinanti, partecipanti a gare indette per la fornitura di beni e servizi);
- i diritti degli interessati in relazione all'accesso ai propri dati, alla cancellazione, alla limitazione del trattamento, alla opposizione al trattamento, al diritto di reclamo;
- le informazioni in ordine ai *cookies* e ai dati di navigazione (i *cookies* sono piccoli *file* di testo che alcuni siti, durante la navigazione, inviano al terminale dell'utente, dove vengono memorizzati, per poi essere ritrasmessi allo stesso sito alla visita successiva);
- la data di aggiornamento dell'informativa.

Tanto premesso

D I S P O N E

Che copia del presente provvedimento venga data a tutto il personale amministrativo, nonchè ai Magistrati dell'Ufficio di Sorveglianza di Caltanissetta.

Si provveda alla pubblicazione sul sito del Tribunale di sorveglianza.

Sarà cura della segreteria della Presidenza di fornire copia del presente atto ai Magistrati e ai dipendenti che, assunto servizio nell'Ufficio successivamente alla data della sua emanazione, risulteranno automaticamente designati, in virtù dell'atto stesso, quali incaricati del trattamento.

Caltanissetta, 31 dicembre 2021

Il Presidente del Tribunale di sorveglianza
Renata Fulvia Giunta