PROT. n. 1277/int.

CORTE DI APPELLO DI CAMPOBASSO

Il Presidente della Corte di Appello e Dirigente Amministrativo f.f.

Visti gli adempimenti prescritti dal D. Lgs. 196/2003, come modificato dai D. Lgs. 101/2018 e D.M. 7.8.2018;

Dovendo dare aggiornata applicazione del Regolamento UE n. 2016/679 (c.d. GDPR - regolamento generale sulla protezione dei dati), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati, nonché ai Decreti Legislativi n. 51 e n. 101/2018, con l'individuazione di soggetti titolari, responsabili, designati e incaricati di compiti e funzioni relativi al trattamento dei dati.

COMUNICA

ex art. 4 n. 7) del Regolamento UE 2016/679, che **titolari del trattamento dei dati**, sono, nel rispetto delle relative competenze, il Ministero della Giustizia e per la Corte di Appello di Campobasso il suo Presidente pro-tempore.

In caso di assenza o impedimento del Presidente, il Vicario.

In caso di assenza o impedimento del Vicario, il magistrato della Corte di Appello con maggiore anzianità di servizio.

NOMINA

ex art. 4 n.8) del Regolamento UE 2016/679, come **responsabile del trattamento dei dati** per la Corte di Appello, ferma la responsabilità del Ministero, il Presidente e/o Dirigente amministrativo p.t.

DESIGNA

ex art. 2 comma 2-quaterdecies D. Lgs. 196/2003:

tutti i magistrati togati, per gli affari inerenti le proprie funzioni, anche se delegate o loro attribuite, alla istruzione, vigilanza e controllo degli AUPP, dei tirocinanti o di altre unità dell'Ufficio del Processo loro assegnate, ove abilitate al trattamento dei dati.

AUTORIZZA

al trattamento dei dati, nei limiti e negli ambiti della rispettiva competenza d'ufficio e servizio, tutti i dipendenti e collaboratori, a qualsiasi titolo, della Corte di Appello, come da elenco analitico allegato, e così indicati per funzioni:

- i magistrati ordinari per l'utilizzo di dati giudiziari, sia nell'esercizio dell'attività giurisdizionale che al di fuori, nei casi previsti direttamente dalla normativa o autorizzati;
- i direttori di cancelleria, ciascuno per le proprie personali competenze e specifiche funzioni;
- il personale amministrativo (compresi gli AUPP ed il personale PNRR) in servizio presso la Corte, anche in posizione di applicazione/comando/distacco;
- i MOT (magistrati ordinari in tirocinio), nei limiti e in funzione delle attività di tirocinio;
- i magistrati onorari, per gli affari inerenti alla propria funzione in materia civile e penale;
- i magistrati onorari in tirocinio, nei limiti e in funzione delle attività di tirocinio;
- il personale che svolge stage o tirocinio presso la Corte, nei limiti e in funzione delle attività di stage e tirocinio;
- eventuale personale esterno

§§§§§

Visto l'art. 16 del Trattato di Lisbona che inquadra il diritto alla protezione dei dati personali tra i diritti fondamentali della persona (art. 16 TFUE e art. 8 della Carta dei diritti fondamentali);

Visto il dlgs. 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);

Vista la 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. 18 maggio 2018, n. 51 che ha dato attuazione alla direttiva UE 2016/680, regolamentando il trattamento dei dati personali per finalità di prevenzione e repressione di reati, esecuzioni di sanzioni penali, salvaguardia contro le minacce alla sicurezza pubblica e prevenzione delle stesse sia da parte dell'Autorità giudiziaria che da parte delle Forze di Polizia;

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 del dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)";

Rilevato, in particolare, che il regolamento UE 2016/679 (entrato in vigore il 25 maggio 2016 e applicabile in tutti gli Stati membri a partire dal 25 maggio 2018) intende garantire e bilanciare la protezione dei dati di carattere personale (incrementati in maniera esponenziale nella condivisione e raccolta a seguito della rapida evoluzione tecnologica), costituente un diritto fondamentale (art. 8, par. 1, Carta dei diritti fondamentali dell'Unione europea e art. 16, par. 1,TFUE), con la libera circolazione dei dati stessi (art. 1 del regolamento UE 2016/679);

Visto il D.M. 27 aprile 2009 "Nuove regole procedurali relative alla tenuta dei registri informatizzati dell'amministrazione della giustizia";

Richiamati, in particolare, gli art. 23 e 37, par. 1, lett. A del Regolamento e l'art. 2 duodecies del D. Lgs. 196/2003 (Limitazioni per ragioni di giustizia) introdotto dal D. Lgs. n. 101/2018, in merito alla distinzione tra attività giurisdizionale e trattamento dei dati giudiziari, operati dagli uffici, non effettuati nell'esercizio di funzioni giurisdizionali;

Letto il provvedimento del Garante per la protezione dei dati personali in data 5 dicembre 2013 n. 545 (Trasmissione ai terzi di dati personali del dipendente da parte del datore di lavoro) che fa seguito ai provvedimenti emessi dalla medesima Autorità il 1° marzo 2007 (Utilizzo degli strumenti elettronici da parte dei lavoratori), il 13 ottobre 2008 (Dismissione di apparecchiature elettriche ed elettroniche contenenti dati personali), il 27 novembre 2008 (Funzioni dell'amministratore di sistema), il 2 dicembre 2010 (Linee guida in materia di trattamento di dati personali nella riproduzione di provvedimenti giurisdizionali per finalità d'informazione giuridica), il 2 marzo 2011 (Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sui web);

Visto il decreto 7 agosto 2018 con il quale il Ministro della Giustizia ha designato il Responsabile della protezione dei dati con riferimento al trattamento dei dati giudiziari nell'esercizio di funzioni non giurisdizionali;

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 oggetto di lavorazione nei diversi Uffici nell'ambito dell'attività amministrativa;

Viste le indicazioni fornite dal Direttore Generale per Sistemi informativi automatizzati (nota del 16 dicembre 2009, prot. 35909.U);

Vista la nota in data 13 dicembre 2018, n. 41553 della Direzione Generale Sistemi informativi Automatizzati in materia di "Piano strategico della sicurezza";

Richiamato, altresì, per quanto di rilievo, il Piano strategico di sicurezza, DGSIA ID 11606 del 13.12.2018;

Visto il Piano per la Sicurezza informatica dell'Amministrazione della Giustizia 2021;

Vista la Delibera ANAC 311 del 12/07/2023 - Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali. Procedure per la presentazione e gestione delle segnalazioni esterne;

Evidenziato che il **Ministero della Giustizia ha provveduto alla nomina, per tutti gli Uffici, di un unico Responsabile per la protezione dei dati personali**, quindi, non vi è ambito per diverse e nuove designazioni a livello locale;

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, nei limiti dell'attuale assetto normativo e delle risorse messe a disposizione, provvedere in merito alle regole sul trattamento dei dati da parte degli Uffici conformemente alle indicazioni desumibili dalle richiamate disposizioni nella prospettiva della tutela dei dati personali e nella consapevolezza dei rischi relativi ai trattamenti dei dati nell'esercizio anche delle attività amministrative connesse alla giurisdizione;

Considerata la complessità e la vastità delle attività giurisdizionali e amministrative svolte dalla Corte di Appello di Campobasso, tali che, al fine di garantire il rispetto della normativa e l'effettività della tutela della riservatezza dei dati, impongono di adottare i necessari provvedimenti con riguardo ai soggetti che trattano i dati;

Considerato che i principi di precauzione e la necessità di garantire la protezione dei dati personali richiedono di prevedere che l' utilizzo di essi, nell'ambito dell'attività giurisdizionale in senso proprio, comunque non debba eccedere le previsioni processuali e la funzione strettamente ad essa connessa, così che, con riguardo a tale ambito e all'eventuale gestione dei dati eccedenti il processo, i magistrati ordinari, onorari, i magistrati ordinari in tirocinio, i tirocinanti e i borsisti inseriti negli Uffici devono attenersi ai limiti propri della normativa e alle regole qui indicate e richiamate, affinché non si

determinino utilizzi dei dati giudiziari non rispondenti alle finalità proprie dell'attività giurisdizionale e dei servizi ad essi connessi;

Richiamati gli atti di gestione con cui si sono assegnati i compiti al personale amministrativo e tenuto conto dell'assetto organizzativo attuale della Corte di Appello, si

PRECISA

che tutti i soggetti titolari, responsabili, designati e incaricati di compiti e funzioni relativi al trattamento dei dati sono tenuti all'osservanza del D. Lgs. 196/2003, e del Regolamento UE n. 2016/679 (c.d. GDPR), nelle prescrizioni sotto richiamate e dettagliate.

I designati provvedono in particolare:

- ad assicurare che i soggetti incaricati del trattamento i quali agiscono nell'ambito dei settori degli uffici affidati alla loro gestione assolvano alle attività di trattamento in conformità alle prescrizioni ed istruzioni vigenti;
- a segnalare al Titolare ogni eventuale peculiarità che necessiti di valutazione anche al fine dell'adozione di specifiche e ulteriori misure di sicurezza rispetto a quelle vigenti;
- a segnalare al Titolare, senza ritardo, ogni violazione dei dati personali ai fini delle notificazioni e comunicazioni previste dalla normativa vigente.

I designati e gli incaricati sono tenuti tra l'altro a:

- trattare i dati personali garantendo la massima riservatezza delle informazioni di cui vengono in possesso e considerare tutti i dati personali come riservati e di norma soggetti al segreto d'ufficio;
- non diffondere o comunicare a terzi dati personali, fuori dai casi in cui la diffusione o comunicazione è necessaria per l'adempimento dei fini istituzionali dell'ufficio; in particolare è fatto espresso divieto di consegnare o duplicare "dati personali" per finalità diverse da quelle dell'attività lavorativa assegnata;
- tenere una condotta, in ogni fase di lavoro, tale da evitare che: a) i dati personali siano soggetti a rischi di perdita o distruzione anche accidentale; b) i dati possano accedere persone non autorizzate; c) i dati non siano esatti, completi e veritieri; d) vengano svolte operazioni di trattamento non consentite o non conformi ai fini istituzionali per i quali i dati sono stati raccolti e per i quali vengono trattati;
- osservare le disposizioni emanate dall'Ufficio in materia di sicurezza e riservatezza.

In particolare, nel caso di trattamenti di dati personali che comportino l'uso di sistemi informatici e telematici (PC, PC portatili, programmi informativi dell'amministrazione in uso all'Ufficio o altro):

- l'accesso a tali dati può avvenire solo attraverso password o codici di accesso secondo quanto disposto dall'Amministrazione o dall'Ufficio;
- ogni designato o incaricato deve mantenere segreta la password di accesso al proprio PC, evitando di divulgarla a terzi o di trascriverla su fogli;
- tutto il materiale cartaceo (quali, ad esempio, fascicoli, perizie, atti giudiziari, fascicoli personali, certificazioni riguardanti lo stato di salute dei dipendenti o altro, ecc.) relativo ai dati personali, deve essere custodito con pari diligenza in modo tale da garantire che ad esso non accedano persone non autorizzate;

A livello operativo, per il personale autorizzato al trattamento le misure di sicurezza previste sono, in via meramente esemplificativa:

- abilitazione degli "autorizzati" al trattamento secondo mansioni di competenza e le attribuzioni dell'ufficio;

- profilazione sugli strumenti operativi/informatici in uso secondo le rispettive competenze e nei limiti delle dotazioni ministeriali (ad es. PC fissi, portatili, registri/applicativi ivi installati, strumenti di protocollazione etc., con utenze individuali protette (credenziali e pw) e privilegi di accesso e interazione coerenti con le funzioni di servizio;

- generale osservanza della policy di sicurezza informatica (in particolare, lettura e rispetto del manuale di gestione dei flussi documentali del Ministero, adottato dalla DGSIA) e degli obblighi di riservatezza e protezione dei dati personali secondo i vigenti Codici di condotta per il personale;

- applicazione dei vigenti sistemi di protezione del patrimonio documentale/informativo nei processi di lavoro sia digitalizzati che analogici secondo i compiti di ufficio e le mansioni di adibizione;

- livelli di visualizzazione, trasmissione, eventuale scambio delle informazioni, aderenti al principio di minimizzazione nel trattamento di dati di natura personale.

Per le forme di trattamento connesse a forme di raccolta, registrazione, conservazione e rielaborazione (ad es. in forma aggregata, all'esito di rilevazioni statistiche) per fini di monitoraggio e/o statistici nei limiti di competenza dell'Ufficio, valgono le stesse precauzioni tecniche e misure di sicurezza insite nella profilazione di utenze coerenti con i livelli di autorizzazione/abilitazione informatica oltre all'applicazione - ove compatibile - di idonee misure di anonimizzazione/pseudonomizzazione.

Dati Personali

Nell'Ufficio giudiziario *de quo* sono trattati i dati relativi a tutti i soggetti giuridici identificati o identificabili, anche indirettamente mediante riferimento a qualsiasi altra informazione, che vengono comunicati per motivi istituzionali o di servizio al personale dell'ufficio e i dati del personale dipendente.

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 di 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";

Ai sensi dell'art. 4 punto 2) del Regolamento (UE) 2016/679, per trattamento s'intende "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati 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, raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione'";

Ai sensi dell'art. 4 punto 12) del Regolamento (UE) 2016/679, per **violazione dei dati personali** s'intende "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".

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 rispetto alle finalità del trattamento;

- esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;

- limitazione della conservazione: ossia, 6 necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali é stato effettuato il trattamento;

- integrità e riservatezza: occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento.

I SOGGETTI INTERESSATI DAL TRATTAMENTO DEI DATI SONO:

1. **Il titolare del trattamento** é, ex art. 4 n. 7) del Regolamento UE 2016/679, la persona fisica, la persona giuridica, la P.A. e qualsiasi altro organismo cui competono le decisioni in ordine alle finalità e ai mezzi del trattamento dei dati.

Il titolare vigila sulla correttezza delle operazioni di trattamento dei dati e sull'osservanza, da parte dei responsabili ed incaricati, delle istruzioni impartite al fine che interessa, nonché sull'attuazione del presente documento.

Titolari del trattamento sono nel rispetto delle relative competenze il Ministero della Giustizia e la Corte di Appello di Campobasso in persona del Presidente pro-tempore.

2. Il **responsabile del trattamento** è, ex art. 4 n.8) del Regolamento UE 2016/679), la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento. E il soggetto preposto a vigilare, nell'ambito del proprio settore e sfera di intervento, a che il trattamento medesimo avvenga in maniera corretta.
Responsabili del trattamento sono il Ministero della Giustizia e il dirigente amministrativo.

3. **Il responsabile della protezione dei dati personali è**, ex art. 37 del Regolamento UE 2016/679, individuabile nella persona fisica pro tempore nominata per tutti gli uffici dal Ministero della Giustizia. Nel caso di specie, vedasi circolare del Ministero della Giustizia n. m_dg.GAB.27/06/2018.0021611.U.

4. Gli **incaricati del trattamento** sono, in via esemplificativa, i magistrati, il personale amministrativo, i collaboratori a qualsiasi titolo, tirocinanti e il personale esterno all'amministrazione autorizzato a operare nell'ufficio.

Gli incaricati, designati mediante specifico atto, devono trattare dati personali garantendo la massima riservatezza delle informazioni di cui vengono in possesso, considerare tutti i dati personali come riservati e osservare le disposizioni emanate dall'Ufficio in materia di sicurezza e riservatezza.

"I designati" ai sensi dell'art. 2 quaterdecies, D. Lgs. 196/03, sono autorizzati al trattamento dei dati personali in relazione alle competenze esercitate dai propri uffici, nel rispetto delle misure e istruzioni adottate dai soggetti designati della rispettiva struttura di servizio.

Il personale non dirigenziale in servizio presso il Ministero (e il personale di altre amministrazioni comandato o distaccato) è autorizzato al trattamento dei dati personali nei limiti delle competenze attribuite all'ufficio o struttura di appartenenza. Sono fatte salve eventuali diverse determinazioni, volte a limitare o escludere categorie specifiche di trattamenti a determinati dipendenti, in casi che saranno debitamente motivati e predefiniti a cura dei Designati delle rispettive aree e strutture di appartenenza ovvero delle figure apicali che funzionalmente ne dipendano.
I soggetti autorizzati - in quanto preposti alle operazioni di trattamento di dati personali e legittimati, in ragione del proprio ufficio, servizio o attività, ad accedere ad informazioni personali contenute negli archivi, banche-dati e nei flussi documentali comunque acquisiti o formati presso il Ministero - sono individuati ed istruiti dai soggetti che esercitano le funzioni di Titolare, anche con riferimento alle misure di sicurezza da rispettare nell'effettuazione delle operazioni di trattamento loro affidate. Questi ultimi (anche per il tramite di soggetti dai medesimi designati) assicurano che sia sempre individuato o individuabile l'ambito di trattamento autorizzato per ogni unità di personale.

Soggetti esterni all'Amministrazione

I soggetti esterni che prestano la loro attività in favore dell'Amministrazione - ove non già individuati quali "Responsabili" ai fini e per gli effetti dell'art. 28 GDPR - devono essere espressamente autorizzati dal titolare al trattamento dei dati personali, e devono attenersi alle istruzioni loro impartite, come ricevute ai sensi dell'art. 29 del Regolamento.
Gli incaricati accedono ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati. Nel corso dell'intero ciclo necessario alle operazioni di trattamento gli incaricati devono attenersi alle seguenti disposizioni:
> i documenti, atti, fascicoli contenenti i dati personali non possono essere consultati da persone diverse da quelle incaricate del trattamento;
> i documenti, atti, fascicoli sono trattenuti dagli incaricati solo per i] tempo strettamente necessario alle operazioni di trattamento;
Tutti gli archivi, sia analogici che digitali, devono essere provvisti di dispositivi volti a impedire accessi non autorizzati.
I responsabili e 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.
In generale, va sottolineato quanto stabilito dal codice di Comportamento del personale del Ministero della Giustizia, 2023, pubblicato sul sito internet della Corte, in relazione agli obblighi di riservatezza posti dall'art. 11 che qui si riproduce:

"Il dipendente si impegna ad osservare il principio della riservatezza in relazione alla natura dell'attività svolta.
Il dipendente osserva il segreto d'ufficio e la normativa in materia di tutela e trattamento dei dati personali e, qualora sia richiesto verbalmente di fornire informazioni, atti o documenti tutelati dal segreto d'ufficio o dalle disposizioni in materia di dati personali, informa il richiedente dei motivi che ostano all'accoglimento della richiesta.
Il dipendente, nel rispetto dei principi e delle norme sulla trasparenza, si astiene dal divulgare ai mezzi di informazione le notizie riservate connesse allo svolgimento delle attività lavorative e dal rilasciare dichiarazioni pubbliche che per le forme e i contenuti possano comunque nuocere all''Amministrazione, ledendone l'immagine o il prestigio o compromettendone l'efficienza.
In caso di provvedimenti soggetti a pubblicazione obbligatoria, il dipendente segue le direttive impartite dal titolare o dal responsabile del trattamento, attenendosi in ogni caso a criteri di liceità, correttezza e minimizzazione nel trattamento dei dati personal.
Il dipendente é tenuto a non fornire informazioni riservate sui contenuti di attività, decisioni da assumere e provvedimenti relativi a procedimenti in corso, sia all'interno sia all'esterno dell''Amministrazione, prima che siano stati ufficialmente deliberati e comunicati formalmente agli interessati.
Il dipendente presta la dovuta diligenza e attenzione per evitare la divulgazione involontaria di informazioni riservate.
Il dipendente consulta i soli atti e fascicoli direttamente collegati ai compiti assegnati e ne fa un uso conforme ai doveri d'ufficio, consentendone l'accesso solo a coloro che ne abbiano titolo, nel rispetto delle istruzioni del titolare o del responsabile del trattamento.
Il dipendente non estrae dai sistemi informativi e non riproduce atti e documenti d'ufficio se non per l'attività di propria competenza e secondo le direttive che sono state impartite".

In relazione al trattamento ed alla gestione dei dati personali giusta l'art. 15 che qui si trascrive:

1. *I soggetti designati o incaricati del trattamento di dati personali devono osservare le regole di sicurezza e i principi di riservatezza e segretezza nelle operazioni di trattamento, attenendosi a tutte le misure tecniche ed organizzative messe in atto dal titolare o dal responsabile per assicurare un livello di sicurezza adeguato al rischio.*
2. *Il dipendente incaricato controlla e custodisce atti e documenti contenenti dati personali che gli sono stati affidati per lo svolgimento dei propri compiti e adotta le misure necessarie a sottrarli alla consultazione di persone prive di autorizzazione.*

3. Nel caso di fascicoli o di qualsiasi altra documentazione cartacea contenente dati personali posti presso i locali degli uffici, è responsabilità del dipendente incaricato curare che tale documentazione sia collocata in maniera che ad essa non accedano persone prive di autorizzazione.

4, Il dipendente incaricato del trattamento dei dati personali con strumenti elettronici, adotta le necessarie cautele per assicurare la segretezza delle credenziali d'accesso e la diligente custodia dei dispositivi in suo possesso ed uso esclusivo."

Formazione/sensibilizzazione del personale sui temi della *privacy/data protection.*

Il Presidente della Corte di Appello, in quanto titolare del trattamento, assicura che il personale assegnato ai rispettivi uffici abbia adeguata formazione e conoscenza delle modalità di trattamento dei dati e delle istruzioni impartite (anche per il tramite dei soggetti designati) e monitora la puntuale applicazione delle misure adottate.

Vigila inoltre sul rispetto degli obblighi stabiliti dal Regolamento e di quelli derivanti dall'incarico e dal relativo contratto o atto giuridico regolante il rapporto.

Segnala in ogni caso, eventuali inadempimenti ai soggetti designati, per il cui tramite sia esercitata la titolarità del trattamento rispetto agli ambiti di competenza ministeriale.

Nelle rispettive sfere conoscitive e di competenza i soggetti designati, in coordinamento con il RPD e con le competenti unita in materia di impiego del personale, formazione e bilancio, tenuto conto degli indirizzi degli organismi istituzionalmente preposti alla formazione per le categorie di personale interessato e degli obiettivi esigibili per le rispettive strutture curano la programmazione ed organizzazione delle attività di formazione del personale per la corretta applicazione delle disposizioni in tema di protezione di dati personali, al fine di:

- promuovere le conoscenze dei principi in materia, adeguate al proprio ruolo e ambito di trattamento,
- sensibilizzare il personale interno e i collaboratori esterni sulla rilevanza dei diritti tutelati dal vigente quadro normativo,
- potenziare il patrimonio informativo in ordine alle misure e garanzie applicabili per il trattamento di dati nel contesto delle mansioni svolte.

Tali attività possono concorrere all'adempimento dell'obbligo, in capo ai soggetti designati, di fornire istruzioni per il trattamento di dati a chiunque agisca sotto la sua autorità e abbia accesso a dati personali, anche ai fini e per gli effetti dell'art. 29 GDPR.

Principi generali di gestione e aggiornamento della documentazione

La Corte di Appello di Campobasso in tema di sistemi informatici e sicurezza tecnologica si rifà alle specifiche tecniche adottate dal Dipartimento per I 'Innovazione Tecnologica del Ministero di Giustizia cui si fa espresso rimando, m_dg.DOG07.07/08/2024.0004292.ID.
La Corte di Appello di Campobasso, nella persona del Presidente, si impegna a gestire le informazioni nel rispetto delle leggi e dei regolamenti vigenti, in particolare nel rispetto dei principi a tutela della privacy, nonché di quelli di trasparenza, correttezza, responsabilità e sostenibilità.
La documentazione relativa al trattamento dei dati personali è periodicamente controllata per verificare la necessita di un aggiornamento, che sia determinato (in via non esaustiva) da uno dei seguenti fattori: a) modifiche normative suscettibili di recepimento; b) introduzione di nuovi processi, servizi o prodotti; c) variazioni apportate a processi, servizi o prodotti esistenti, anche per l'insorgenza di nuovi rischi o a modifiche nella loro valutazione.
Le unità di personale in servizio, nell'esecuzione dei propri compiti e al fine di proteggere il patrimonio informativo ricadente nell'ambito operativo delle proprie strutture e connesse categorie di trattamento dei dati personali, si attengono alle policy di sicurezza individuate dal Presidente della Corte di Appello, con funzioni di Titolarità del trattamento (o suoi designati), anche in conformità alle lineeguida diramate con disciplinari ad hoc inclusi quelli sulla sicurezza informatica.
Ferme le disposizioni generali e di dettaglio del Codice di comportamento del personale del Ministero della giustizia (approvato con D.M. 26 ottobre 2023), applicabili nella materia della protezione dei dati e degli obblighi di riservatezza dei dipendenti, possono individuarsi dei principi operativi di base su tematiche di interesse comune per gli utenti degli applicativi e degli strumenti di lavoro ministeriali.

Principi di tenuta documentale

Nella lavorazione dei processi di competenza e nella correlata gestione di flussi documentali, siano essi cartacei o informatici, il dipendente tratta i dati di natura personale (art. 4, par. 1 GDPR) nel rispetto dei principi di cui all'art. 5 par. 1 GDPR, attenendosi in particolare al parametro della

minimizzazione, affinché il trattamento risulti adeguato, pertinente e limitato a quanto necessario rispetto alle finalità per le quali i dati sono trattati.

L'utente presta la dovuta diligenza ed attenzione per evitare una divulgazione involontaria di informazioni riservate; rispetta i principi di necessita e proporzionalità nella consultazione ed estrazione dei dati dai sistemi informativi in dotazione e nella riproduzione e/o duplicazione di atti e documenti d'ufficio, fermi in ogni caso i limiti delle attività di competenza e delle direttive organizzative impartite nella struttura di appartenenza. In particolare, accede ai soli atti e fascicoli collegati alle mansioni assegnate, consentendone a sua volta l'accesso solo a soggetti qualificabili come "autorizzati" al trattamento in ragione del rispettivo ufficio, servizio o attività, nel rispetto delle istruzioni del Titolare o del designato/responsabile del trattamento.

L'utente autorizzato al trattamento dei dati per ragioni di servizio controlla e custodisce gli atti/documenti recanti dati personali che gli sono stati affidati per l'espletamento dei propri compiti e adotta le misure necessarie a sottrarli alla consultazione di persone prive di autorizzazione. Nel caso di fascicoli o di documentazione cartacea contenente dati personali, posti presso i locali degli uffici, il dipendente incaricato della trattazione deve curarne la collocazione e la tenuta e custodia in modo che ad essa non accedano persone prive di autorizzazione.

L'utente che sia preposto con strumenti elettronici ad operazioni di trattamento di dati personali adotta le necessarie cautele per assicurare la segretezza delle credenziali d'accesso e la diligente custodia dei dispositivi in suo possesso ed uso esclusivo.

Conosce e rispetta, debitamente istruitone, le regole di sicurezza vigenti nella sua struttura e i principi di riservatezza e segretezza applicabili alle operazioni di trattamento, attenendosi a tutte le misure tecniche ed organizzative messe in atto dal Titolare o dal responsabile o designato per assicurare un livello di sicurezza che sia adeguato al rischio, rispetto all'unita di appartenenza ed alla specifica categoria di dati e contesto/finalità di trattamento.

In ogni caso, si serve con scrupolo dei beni affidati, mettendo in atto le accortezze necessarie al mantenimento della loro efficienza ed integrità e ne evita un utilizzo improprio e/o eccedente che possa risultare in contrasto con l'interesse dell'Amministrazione e con le regole di utilizzo eco-sostenibile delle risorse.

L'osservanza delle regole e dei principi funzionali al rispetto delle disposizioni vigenti in tema di protezione dei dati personali ricade nella personale responsabilità del dipendente, sotto ogni profilo di rilevanza ordinamentale (disciplinare, deontologica, civile, penale, erariale, etc).

Uso delle stampanti

L'utente, al fine di minimizzare il rischio di diffusione non autorizzata di informazioni, potrà procedere all'avvio della stampa esclusivamente attraverso la postazione assegnata, avendo cura di prelevare prontamente dalla stampante le copie degli atti rilasciati e di evitare in ogni caso divulgazioni anche accidentali di dati, specie in presenza di dotazioni condivise con altre unità di personale.

Impiego di strumenti di lavoro analogici e di dispositivi informatici

Gli utenti sono responsabili del controllo e della custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti informatici e dei documenti cartacei. Ove possibile, deve essere privilegiato l'utilizzo degli strumenti digitali. È opportuno, inoltre, che gli archivi fisici di dati, specie se contenenti categorie particolari di dati o dati giudiziari ai sensi della vigente normativa privacy, siano conservati in contenitori dotati di chiave (armadi, cassettiere, schedari) i quali, nel caso di allontanamento temporaneo del lavoratore dalla propria postazione, non devono essere lasciati incustoditi.

L'Amministrazione resta esclusiva titolare e proprietaria dei dispositivi informatici messi a disposizione degli utenti, nonché esclusiva titolare e proprietaria di tutte le informazioni e dati personali in essi contenuti e/o trattati; tali informazioni o dati devono essere trattati dagli utenti adottando criteri di adeguata riservatezza nella comunicazione dei dati conosciuti, limitandosi a quei casi che si rendano necessari per espletare al meglio l'attività lavorativa richiesta. I dispositivi assegnati sono uno strumento lavorativo nelle disponibilità degli utenti esclusivamente per un fine di carattere lavorativo. In ogni caso, nell'utilizzo dei dispositivi messi a disposizione dall'Amministrazione, gli utenti devono conformarsi a specifiche regole di buon uso volte alla tutela dei dati personali ivi contenuti.

Posta Elettronica

Sul tema, l'art. 12 del Codice di comportamento del personale del Ministero della Giustizia, 2023, dispone:

1. *Al dipendente è consentito l'utilizzo di account istituzionali per i soli fini connessi all'attività lavorativa o ad essa riconducibili e non può in alcun modo compromettere la sicurezza o la reputazione dell'Amministrazione.*
2. *Il dipendente evita di utilizzare le caselle di posta elettronica personali per attività o comunicazioni afferenti al servizio, salvi i casi di forza maggiore dovuti a circostanze in cui il dipendente, per qualsiasi ragione, non possa accedere all'account istituzionale.*

3. *È vietato l'invio di messaggi di posta elettronica, all'interno o all'esterno dell'Amministrazione, che siano oltraggiosi, discriminatori o che possano essere in qualunque modo fonte di responsabilità del Ministero.*

Ferme le citate disposizioni del vigente Codice di comportamento del personale del Ministero della Giustizia, con particolare riguardo all'impiego della tecnologia informatica, l'utilizzo della posta elettronica è da intendersi connesso e autorizzato per il solo svolgimento dell'attività lavorativa. Anche sul piano del trattamento dei dati e relativa protezione, l'uso della posta elettronica deve improntarsi alla massima cautela e diligenza, nel rispetto dei principi di salvaguardia della sicurezza e reputazione dell'Amministrazione.

Gli utenti hanno in utilizzo indirizzi nominativi di posta elettronica. Possono essere assegnate anche caselle e-mail con natura impersonale (ad esempio info, amministrazione, direzione); in questi casi, è preferibile evitare che il destinatario delle mail possa considerare l'indirizzo assegnato come "privato".

Si ricorda che l'accesso a qualunque dispositivo o sistema informatico dell'Amministrazione con le proprie credenziali ADN certifica la presenza e l'attività lavorativa del titolare delle credenziali, e qualunque attività eseguita, e pertanto registrata nei vari log, è addebitabile esclusivamente al titolare delle credenziali stesse.

È altresì consigliato non usare la password su connessioni Wi-Fi non sicure o su computer pubblici.

Per ogni altro aspetto (anche concernente lo specifico ambito operativo della struttura di servizio), si rinvia alle metodologie, misure e istruzioni elaborate dai soggetti che esercitano le funzioni di titolare e comunque alle prescrizioni poste nel citato Codice di comportamento, con particolare riguardo all'art. 15 in materia di trattamento e gestione dei dati personali.

Sito Web

La Corte di Appello di Campobasso dispone di un proprio sito web consultabile al seguente indirizzo https://ca-campobasso.giustizia.it/

Il sito è gestito in via autonoma dal personale amministrativo della Corte di Appello.

Trattamento dei dati personali nell'ambito dei sistemi informatici del processo civile e penale telematico.

La Corte di Appello di Campobasso, nella persona del Presidente, quale Titolare del trattamento nell'ambito dell'esercizio delle proprie funzioni giurisdizionali, si avvale dei servizi telematici resi

disponibili dal Ministero della Giustizia e fornisce, al tal fine, ai soggetti operanti sotto la propria autorità ed abilitati ad accedere ai dati, apposite istruzioni sul trattamento.
I soggetti operanti, sia magistrati che personale amministrativo, vengono abilitati previa autorizzazione del Presidente della Corte con modulistica che viene inviata al DGSIA di Roma ed al Presidio CISIA di Campobasso.
In questo caso, in tema di riservatezza e trattamento e gestione dei dati personali, si fa espresso rimando a quanto stabilito dagli artt. 11 e 15 del Codice di comportamento del personale del Ministero della Giustizia, sopra evidenziati.
Nei fascicoli processuali, il trattamento dei dati personali è disciplinato dal Codice della Privacy e dalle norme processuali. L'accesso è riservato alle parti in causa e presuppone che i dati siano effettivamente pertinenti al processo, mentre l'utilizzo illecito di dati contenuti nei fascicoli può comportare sanzioni e risarcimenti.

Giusta l'art. 17 del Codice di comportamento del personale del Ministero della Giustizia:

1. *Le credenziali fornite al dipendente per l'accesso ai registri informatici sono strettamente personali e non cedibili.*
2. *Il dipendente è responsabile del loro uso e risponde per ogni accesso non consentito al sistema, nonché per l'eventuale indebita divulgazione a terzi di dati riservati con esse ricavati.*
3. *L'accesso alle informazioni, agli atti, ai documenti e ai provvedimenti contenuti nei fascicoli, anche informatici, è consentito al dipendente esclusivamente nei limiti in cui si tratti di informazioni, atti e documenti di sua competenza o necessari per espletare i compiti affidati.*
4. *È vietata la divulgazione a terzi di informazioni acquisite dal dipendente nell'esercizio della propria attività istituzionale; le informazioni medesime non devono essere fornite nemmeno alle parti processuali con modalità che non consentono la sicura identificazione del destinatario.*
5. *Nel rispetto delle istruzioni del titolare o del designato al trattamento dei dati, il personale addetto ai servizi giudiziari deve osservare ogni necessaria cautela nella conservazione dei fascicoli cartacei, al fine di impedire la divulgazione non autorizzata o l'accesso, in modo accidentale o illegale, da parte di terzi ai dati personali ivi contenuti.*
6. *In fase di pubblicazione dei provvedimenti giurisdizionali, il personale dedicato si attiene alle disposizioni impartite dal*

Misure tecniche di sicurezza informatica, si rimanda anche al Piano strategico di sicurezza vigente presso il Ministero della giustizia (varato dal DIT/DGSIA).

In particolare, l'accesso al protocollo informatico SCRIPT@ avviene attraverso la Rete Unitaria Giustizia (RUG) o tramite VPN Giustizia e viene limitata la consultazione e la lavorazione dei documenti modulando i privilegi di accesso (a titolo esemplificativo: lettura, smistamento e classificazione) ai soli utenti autorizzati, attraverso la gestione dei ruoli associati, dei lettori delle singole UO, delle associazioni utente-titolari ed, infine, delle eliminazioni tempestive delle utenze cessate.

Misure per garantire la sicurezza fisica dei luoghi in cui i dati personali sono trattati

L'accesso ai locali dell'Ufficio da parte di utenti esterni è limitato ed avviene previo controllo di sicurezza e/o identificazione, compiuto dal personale di vigilanza, di servizio a turno all'ingresso dei locali del Palazzo di giustizia.

L'accesso alle postazioni di servizio dove sono ubicati applicativi informatici o archivi fisici di documentazione (comunque implicanti trattamenti di dati personali secondo le mansioni di servizio) è consentito al solo personale autorizzato e presidiato da idonei sistemi di vigilanza, tenuto sottochiave e controllato grazie ai servizi di vigilanza privati.

Per quanto riguarda i processi di lavoro manuali o analogici che comportino flussi su formato cartaceo, l'ingresso ai locali che ospitano la documentazione è consentito al solo personale autorizzato e profilato per quel tipo di servizio, con conservazione in idonei archivi sotto la custodia dei medesimi utenti abilitati, debitamente istruiti sui doveri di riservatezza e sulla non ulteriore divulgazione del materiale recante dati personali.

Misure per garantire la registrazione dei log/accessi informatici

Il protocollo informatico ovvero la gestione dei Registri in uso presso le cancellerie, giusta gli applicativi forniti dal Ministero, ha politiche di registrazione degli "accessi" predefinite e tracciabili, in favore dei soli utenti accreditati nello specifico sistema e muniti di credenziali, debitamente istruiti sui doveri di riservatezza e sui presupposti di accesso e visualizzazione, limitati a parametri di stretta necessita e pertinenza con le funzioni di servizio.
Per quanto non su indicato si richiamano le disposizioni del Regolamento sulla Privacy del maggio 2018, le disposizioni impartite in sede ministeriale e contenute nel **"Manuale di sicurezza per gli utenti"** già trasmesso a tutto personale e che è possibile consultare sul sito web della Corte di Appello di Campobasso, in uno a tutta la legislazione di riferimento;
Infine, in qualità di "Titolare" del trattamento dei dati per la Corte di Appello di Campobasso, ai sensi e per gli effetti del d.lgs. 30 giugno 2003 n. 196 e succ. mod.

IL PRESIDENTE

CONFERMA, per le parti ancora compatibili con la legislazione vigente e con i decreti ministeriali in materia di protezione e trattamento dei dati, le prescrizioni contenute nel "Documento programmatico sulla sicurezza dei dati trattati con strumenti elettronici e redatto ai sensi del d.lgs. n. 196/2003" in materia di privacy, sicurezza informatica, integralità e disponibilità dei dati del 2017 e ritrasmesso a tutti i magistrati ed al personale amministrativo con nota 1227 del 2/10/2025.
Si rinvia comunque e 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.

DISPONE

che il presente decreto si comunichi a tutti i Magistrati ordinari e onorari e al Personale amministrativo e che si provveda alla pubblicazione sul sito dell'Ufficio nella sezione "Amministrazione Trasparente".

Campobasso, 20/10/2025

Il Presidente della Corte di Appello di Campobasso
Dott. Vincenzo Pupilella