CORTE DI APPELLO DI SALERNO

Presidenza

84123 Salerno, Cittadella Giudiziaria, Palazzina Trotula de Ruggiero

DECRETO N. 28/2023

Oggetto: Aggiornamento Documento Programmatico sulla Sicurezza dei dati.

La PRESIDENTE

- Considerato che il "Documento programmatico della sicurezza dei dati trattati con strumenti elettronici", adottato ai sensi del D.lgs.196/2003 ("Codice in materia di protezione dei dati personali") - di seguito D.P.S.- deve essere aggiornato alla luce delle modifiche normative intervenute;
- 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 regolamento UE 2016/679 del Parlamento europeo (General Data Protection Regulation) di seguito G.D.P.R. e il regolamento del Consiglio d'Europa del 27 aprile 2016 in tema di protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati che ha abrogato la direttiva 95/46/CE;
- Viste le direttive (UE) 2016/680 del Parlamento europeo e del Consiglio d'Europa del 27 aprile 2016 relative 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, che hanno abrogato la decisione quadro 2008/977/GAI del Consiglio d'Europa;
- Visti 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 centro 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 (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") che ha abrogato

la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati) e ha modificato il d.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali);

- Visto il D.L. 9 febbraio 2012, n. 5, convertito con modificazioni, dalla legge 4 aprile 2012, n. 35, che ha apportato semplificazioni anche in materia di protezione di dati personali e ha abolito l'obbligo di adozione o di aggiornamento, entro il 31 marzo di ogni anno, del D.P.S (art. 45 che ha abrogato il punto 19 dell'Allegato B, nonché l'art. 34, comma 1, lett. g, e comma 1bis);
- 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 i1 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);
- Richiamati gli atti di gestione con cui si sono assegnati i compiti al personale amministrativo;
- Vista la nota in data 13 dicembre 2018, n. 41553 della Direzione Generale Sistemi Informativi Automatizzati in materia di "Piano strategico della sicurezza ";
- Considerate che le fonti in precedenza richiamate hanno innovato in maniera significativa il quadro normativo nel cui ambito erano stati adottati i precedenti documenti programmatici sulla sicurezza;
- 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);

- Richiamata la nota di questo Ufficio 190/I del 24.09.2019 "Trattamento dei dati da parte della Amministrazione Giustizia";
- Considerato che per "*dato personale*" si intende qualunque informazione relativa a persona fisica, giuridica, ente od associazione che permette l'identificazione del soggetto o ente stesso a cui si riferiscono (dati anagrafici, recapiti telefonici, fotografie ecc.).
- Atteso che per trattamento di dati deve intendersi: *"qualunque operazione o complesso di operazioni, svolte con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati";*
- Considerato che nell'ambito dello svolgimento delle proprie funzioni le suddette figure vengono necessariamente a conoscenza dei contenuti delle banche dati presenti in Ufficio;
- Rilevate le ulteriori modifiche al Codice de quo, successivamente apportate attraverso il decreto-legge n. 139 del 2021 convertito, con modificazioni, dalla legge n. 2025 del 2021.

In qualità di "titolare" del trattamento dei dati per la Corte di Appello di Salerno, ai sensi e per gli effetti del D.L.vo 30 giugno 2003 n. 196 e succ. mod., con il presente

RESPONSABILE DEL TRATTAMENTO DEI DATI:

- Dr.ssa Francesca DEL GROSSO – Dirigente Amministrativo.

CONFERMA/NOMINA i seguenti Direttori e Funzionari in servizio al 28 marzo 2023:

VALLECARO Raffaele – Segreteria amministrativa;
CAVALLO Marcello – Dirigente UNEP
GRANCAGNOLO Nicoletta – Ufficio di supporto Conferenza Permanente;
REGA Maria Laura – Consiglio Giudiziario;
BOSCO Luigi – Ufficio del Personale ed Esami Avvocato;
FORTUNATO Chiara – Cancelleria sezione penale;
DE ANGELIS Antonio-Cancelleria penale dibattimentale;
PETRAGLIA Olimpio – Cancelleria Corte Assise di Appello;
AMODEO Alda – Cancelleria sezione civile;
PENNA Fabiana – Cancelleria sezione lavoro;
BOTTA Gaetana – Ufficio Ragioneria;
MIELE Maria Ufficio economato;

Specificatamente il "Responsabile" è tenuto a:

- Impartire agli incaricati del trattamento, per iscritto, le idonee istruzioni;
- vigilare sul rispetto delle istruzioni impartite agli incaricati;

- adottare e rispettare le misure di sicurezza indicate e predisposte dal titolare del trattamento;
- verificare lo stato d'applicazione del D.L.vo 30 giugno 2003 n. 196, nonché il buon funzionamento, la corretta applicazione e la conformità alle indicazioni dell'Autorità Garante dei sistemi e delle misure di sicurezza adottate;
- adottare e fare adottare agli incaricati le modalità previste dal disciplinare tecnico in materia di misure minime di sicurezza, all. B del D.L.vo 196/2003;
- evadere tempestivamente tutte le richieste e gli eventuali reclami degli interessati;
- evadere tempestivamente le richieste d'informazioni da parte dell'Autorità Garante e dare immediata esecuzione alle indicazioni che perverranno dalla medesima Autorità;
- interagire con i soggetti incaricati di eventuali verifiche, controlli o ispezioni;
- comunicare immediatamente al titolare gli eventuali nuovi trattamenti da intraprendere nel proprio settore di competenza, provvedendo alle necessarie formalità di legge;
- distruggere i dati personali in caso di cessazione del trattamento degli stessi provvedendo alle necessarie formalità di legge;
- consentire il trattamento dei dati personali con strumenti elettronici ai soli incaricati dotati di credenziali di autenticazione in conformità a quanto previsto dall'art. 34 all. A del D.L.vo 196/2003;
- custodire, per un eventuale accesso di emergenza, la busta chiusa, controfirmata dall'incaricato contenente la parola chiave dallo stesso prescelta ed informare tempestivamente l'incaricato in caso di utilizzo della componente riservata;
- accertare costantemente che gli incaricati utilizzino la parola chiave con diligenza e che la modifichino ogni qualvolta sussista il dubbio che essa sia stata manomessa. In tale occasione occorrerà provvedere all'aggiornamento della parola chiave contenuta in busta chiusa;
- dovrà usare la massima riservatezza e discrezione nella gestione delle parole chiave e nella loro protezione, anche con riferimento agli obblighi che gli derivano dalla qualifica professionale e come previsto dall'allegato B del D.L.vo 30 giugno 2003, n. 196, così come innanzi aggiornato alla luce delle modifiche normative intervenute e riportate in premessa.

NOMINA INCARICATI DEL TRATTAMENTO DEI DATI ***(tutti i magistrati, i dipendenti ed utenti interni ed esterni che accedono alle Banche Dati dell'ufficio, sulla base dei profili di autorizzazione definiti, nel rispetto della mansioni assegnate):***

Magistrati della Corte di Appello di Salerno

BERNI CANANI	Stefano
BRANCACCIO	Alessandro
BRUNO	Francesco
CAPPIELLO	Patrizia
CARLEO	Giulia
CLEMENTE	Silvana
CONFORTI	Emma
CRESPI	Ornella
D'APICE	Rosa
DE FILIPPIS	Bruno
DE LUCA	Sergio
DEL FORNO	Maria Elena
DI BENEDETTO	Lia
DI MAIO	Gabriele
GIOCOLI	Pietro
GIULIANO	Giuliana
GUBITOSI	Aldo Giuseppe Giovanni
IANNICELLI	Guerino
IANNICIELLO	Mariella
MAINENTI	Marina
MANCINI	Donatella
MELE	Anita
NICCOLI	Maria Assunta
ORIO	Attilio Franco
PALUMBO	Massimo Sergio
PERROTTA	Ubaldo
PISAPIA	Mariagrazia

PIZZELLA Arturo
PIZZILLO Marcella
RULLI Giuliano
STASSANO Maura
SERRELLI Sabrina
SIANO Francesco
ZAMBRANO Maria
SANNINO Mariachiara

GIUDICI AUSILIARI

AGLIATA Giuliano
CASALE Mauro
DE BIASE Luigi
DE CATERINA Pierdomenico
IGLIO Roberto Antonio
PELOSI Pierpaolo
PICCOLO Paolo
ROSANOVA Anna
TERRAZZANO Giovanni Antonio

GIUDICI MINORILI

AMBROSIO Teresa
ARGENTIERE Alessandra
APUZZO Maria
AURICCHIO Armando
BATTIMIELLO Vincenzo
CRISCI Lucia
IZZO Daniela
LAMONACA Sante Massimo
SANTORO Massimo
SAPIA Carmela
VINGIANI Giuseppe
VIVONE Giocondo

PERSONALE AMMINISTRATIVO

ADINOLFI Gianluca – contabile A2 F5;
AMERICANO Marco – operatore giudiziario A2 F1;
AURIEMMA Monica – cancelliere A2 F3;
AUTUORI Maurizio – cancelliere A2 F4;
BALESTRIERI Antonio – ausiliario A1 F2.
BERNI Paola - funzionario contabile A3 F2;
BOCCHINO Annamaria – cancelliere A2 F3;
CAPACCIO Domenico – ausiliario A1 F2;
CAVALLARO Angelo – contabile A2 F5;
CIROTA Emilia – assistente giudiziario A2 F4;
CITRO Teresa – cancelliere A2 F3;
CORCILLO Ernesto – centralinista A2 F3;
CORVINO Rosa – operatore giudiziario A2 F1;
CUCCURULLO Rachele – assistente giudiziario A2 F4;
D'AMATO Lucia – cancelliere A2 F5;
D'ELIA Mariano – cancelliere A2 F4;
D'UVA Daniela – funzionario giudiziario A3 F1;
DE ANGELIS Antonio – centralinista A2 F2;
DE DIVIZIIS Veronica – funzionario contabile A3 F3;
DE MARTINO Marianna – funzionario giudiziario A3 F1;
DE MARTINO Sabato – operatore giudiziario A2 F3;
DE NOTARIS Laura – funzionario contabile A3 F4;
DE PAOLA Angela – funzionario contabile A3 F3;
DE ROSA Aldo Gabriele – ausiliario A1 F3;
DI GREGORIO Benedetto- assistente giudiziario A2 F4;
DI GRUTTOLA Michele – funzionario giudiziario A3 F1;
DI NAPOLI Oriana – assistente giudiziario A2 F2;
DONATELLI Morgan – assistente giudiziario A2 F2;
ERRICO Alessandro – assistente giudiziario A2 F3;
FERRAIOLI Maria Pia – funzionario giudiziario A3 F2;
FRACCHINI Giuseppe – operatore giudiziario A2 F3;
FRANCHELLA Rosanna – operatore giudiziario A2 F1;

FRISONE Anna Maria – contabile A2 F5;
GALLUZZI Rosanna – cancelliere A2 F3;
GERARDI Massimo – operatore giudiziario A2 F1;
GIORDANO Renato – assistente giudiziario A2 F3;
GIRARDI Francesca – assistente giudiziario A2 F4;
LICASTRI Rosita – assistente giudiziario A2 F2;
LIGUORI Giuseppina – ausiliario A1 F2;
LIGUORI Pasquale – conducente automezzi A2 F3;
MARINO Domenico - contabile A2 F4;
MASSANOVA Maria Teresa – funzionario contabile A3 F2;
MELCHIORRE Loris Aldo – ausiliario A1 F2;
MELE Eleonora – cancelliere A2 F3;
MICERA Gaetano – cancelliere A2 F3;
MICHELI Marta – funzionario statistico A3 F2;
MIGLIARO Carmine – conducente automezzi A2 F2;
MOFFA Giovanni – contabile A2 F4;
PARRILLI Angela – funzionario giudiziario A3 F1;
PECCI Nunzia – funzionario giudiziario A3 F3;
PERNA Antonella – operatore giudiziario A2 F1;
PERSIANO Raffaele – funzionario giudiziario A3 F1;
SAGGESE Assunta – assistente giudiziario A2 F3;
SALSANO Anna - contabile A2 F4;
SANTANIELLO Alfonso – funzionario giudiziario A3 F2;
SANTINI Arturo – funzionario tecnico A3 F1;
SANTORO Carlo – ausiliario A1 F3;
SARTORI Carmela – operatore giudiziario A2 F2;
SCARPA Giovanni – assistente giudiziario A2 F2;
SENATORE Fulgenzio – assistente giudiziario A2 F2;
SPATUZZI Amalia – assistente giudiziario A2 F2;
TENZI Elena – operatore giudiziario A2 F1;
TIERNO Maria Antonietta – funzionario giudiziario A3 F3;
VITALE Pasquale – operatore giudiziario A2 F1;
VITOLO Gennaro – ausiliario A1 F2;

PERSONALE UNEP:
APONE Domenico - assistente giudiziario Area 2 F4;
ARBIA Maria Grazia - ufficiale giudiziario Area 2 F1;
BARBARIA Nunzio – funzionario UNEP Area 3 F3;
CANNIZZARO Giuseppe - ufficiale giudiziario Area 3 F1;
CAPO Maria Rita - funzionario UNEP Area 3 F3;
CASABURI Antonio – assistente UNEP Area 2 F2;
CAVALLO Sergio – funzionario UNEP A3 F3;
CONIGLIO Giuseppe – assistente UNEP Area 2 F2;
CROCE Maria – assistente giudiziario Area 2 F3;
CUOMO Antonella – funzionario giudiziario Area 3 F1;
DE SIMONE Fernanda - assistente giudiziario Area 2 F3;
DI MARCO Carlo – funzionario UNEP Area 3 F3;
DI PAOLA Stefania – assistente giudiziario Area 2 F4;
DIANESE Luigi – funzionario giudiziario Area 3 F1;
FALACE Domenico - funzionario UNEP Area 3 F3;
FERRI Annamaria - funzionario UNEP Area 3 F3;
FOLLARO Domenico - assistente giudiziario Area 2 F3;
FRANCO Matteo Antonio – ufficiale giudiziario Area 2 F5;
FROIA Anna – funzionario UNEP Area 3 F2;
FUNICELLO Costabile - funzionario UNEP Area 3 F1;
GALLUCCI Stefania – funzionario UNEP Area 3 F2;
GIORDANO Antonio – funzionario UNEP Area 3 F2;
GIUNTI Virginia – funzionario UNEP Area 3 F2;
GRIECO Elisabetta - funzionario giudiziario Area 3 F1;
IACUZIO Francesco – assistente giudiziario Area 2 F4;
IMPERATORE Raffaele – funzionario giudiziario Area 3 F1;
LAUDANO Anna Speranza – funzionario UNEP Area 3 F2;
LAURETANO Laura - assistente giudiziario Area 2 F3;
MANGIACAVALLO Elena – assistente UNEP Area 2 F2;

MELE Giampiero – assistente UNEP Area 2 F2;
MONTUOLO Gianpaolo – ufficiale giudiziario Area 2 F5;
MUTALIPASSI Angela - assistente giudiziario Area 2 F3;
NOLFI Antonietta – funzionario UNEP Area 3 F1;
PALMA Patrizia – funzionario UNEP Area 3 F2;
PAOLILLO Loredana - ufficiale giudiziario Area 2 F5;
PRUDENZANO Vincenzo – funzionario UNEP Area 3 F1;
RE Virginia - funzionario UNEP Area 3 F1;
RESCIGNO Veronica – assistente giudiziario Area2 F2;
ROMANINI Ciro Iago – funzionario UNEP Area 3 F3;
SANTONICOLA Santolo - ufficiale giudiziario Area 2 F5;
SERRITIELLO Alessandra - assistente giudiziario Area 2 F4;
SOLDOVIERI Maria - funzionario UNEP Area 3 F3;
TRANCHESE Domenico - funzionario UNEP Area 3 F1;
VICINANZA Emilio - funzionario UNEP Area 3 F1.

NOMINA INCARICATI ESTERNI DEL TRATTAMENTO DEI DATI (*che svolgono attività di supporto all'Amministrazione e che hanno prestato il giuramento di rito, ai sensi della legge 401/1987 per le attività di cui alla legge 458/1993):*

Per le attività di assistenza applicativa sui sistemi legacy e distrettuali dell'area civile e penale il seguente personale tecnico del Presidio CISIA di Salerno che operano in collaborazione con i tecnici del CISIA di Napoli:
NIGRO Arcangelo;
GIURGOLA Milena;
MONTEFUSCO Antonio;
DE VIVO Marcello;
DE SANTIS Fabio;
RUSSO Marco;
PROPATO Diego.

Per l'affidamento dei servizi di assistenza agli utenti e supporto nella gestione del sistema informativo del Ministero della Giustizia-Gara informale ex art. 162 co. 1 d.lvo 50/2016- Contratto SIA 95.03.A.GM.G.5/2021P LOTTO 4 (Sud), i seguenti tecnici SPC che prestano servizio per la risoluzione dei ticket degli utenti del distretto di Corte di Appello di Salerno (l'assistenza viene erogata, come previsto dal contratto, prevalentemente con modalità di accesso ai sistemi da remoto, dalle postazioni attestate alla RUG):
ALIBERTI Marco;
ALLEGRO Gianluca;
AMADORI Simone;
AMALFITANO Pasquale;
ANGELINO Giuseppe;
ANNICIELLO Vincenzo;
ARENA Raffaele;
BARESE Ciro;
BIFANI Marco;
BOZZOLI Flavio;
BRANDI Vincenzo;
BUONFRATE Roberto;
CALABRESE Carmine;
CALAFATO Stefano;
CARUSIO Salvatore;
CATAURO Ivan;
CHIUSO Giovanni;
CIOTOLI Massimo;
COGLIANDRO Rocco;
COLUCCI Fabio;
CUCOVEICA Irina;
D'ALICANDRO Crescenzo;
DE ANGELIS Leonardo;
DE BELLIS Antonio;
DE GREGORIO Pasquale;
DE PASCALE Agostino;

DE ROSA Simone;
DEL POPOLO Giuseppe Roberto;
DI LEO Gabriele;
DI PALMA Giangaetano;
DI PIAZZA Dino;
DI ROBERTO Pietro;
ERRICHIELLO Luca;
ESPOSITO Marina Rosaria;
EVANGELISTA Angelo;
FEBBRAIO Diego;
FERRIGNO Claudio;
FIERRO Alfonso;
GALLO Odorisio;
GATTO Giuseppe;
GIACOBBE Eugenio;
ILARDO Pietro;
INDAIMO Diego;
IZZO Pietro;
LA PEGNA Emilia;
LANZARO Francesco;
LANZARO Salvatore;
LO RUSSO Gerardo;
MADDALUNO Antonio;
MAIO Mario;
MANZO Filippo;
MARINELLI Maria Carmela;
MAZZARELLA Lorenzo;
MELONI Roberta;
MEROLA Roberto;
MIGHELI Mirko;
MORETTI Francesco;
MUOIO Chiara;
OLIVO Giampaolo;
PAGANO Costantino Giovanni;
PALUMBO Francesco;
PANTALEONE Alberto;
PARIANTE Salvatore;
PELLICANO' Pasquale;
PERNA Giuseppe;
PETRONE Raffaele;
PIANESE Gianluca;
PLANTAMURA Mario;
PULLÌ Domenico;
QUERCETO Fabiano;
RACITI Angelo;
RUGGIERO Gianluca;
RUSSO Angelo;
SCALICI Giuseppe;
SCIVOLETTO Bartolomeo;
SCOGNAMIGLIO Marco;
SMERIGLIO Francesca;
SPISSO Chiara;
SPOSATO Eugenio;
STRAZZULLO Alessandro;
TIRELLA Fabio;
TRAMONTANO Luigi;
TULIPANO Dante;
UCCELLA Antonio;
VENERE Giovanni;
VERDOLIVA Gaetano;
VITIELLO Gerardo;
ZINNO Giorgi.

Personale Società ASTE GIUDIZIARIE IN LINEA S.P.A., che a seguito di proroga di convenzione sottoscritta con questa Corte in uno agli UU.GG. del distretto il 26.10.2017 svolgono le attività indicate in convenzione:
VISCARDI Maria Domenica;
MONACO Francesca;
ROBERTAZZI Simona.

Funzionari A3 F1 addetti all'Ufficio per il processo assunto a tempo determinato con i fondi del PNRR:
CAPPELLUZZO Antonio;
CASABURI Chiara;
CASOLI Archimede;
CELANO Jasmin;
CORRADO Antonia Luigia;
D'ANTONIO Vincenzo;
DE CIUCEIS Elisa;
DELL'ITALIA Mario;
DI LUCCIO Gessica;
DI MASI Ludovica;
DI VECE Maria;
DURANTE Serena;
FERRIGNO Matteo;
FLORIMONTE Alfredo;
GRIECO Giuseppina;
IDONE Diana;
LUCIANO Costantino;
MENDITTO Mariantonietta;
NESE Marzio;
PINO Valentina;
PREZIOSI Anna;
PUCA Pasquale;
RENZULLI Mariangela;
RICCIARDI Michela;
SALSANO Michael;
SANTARPIA Marco;
SANTUCCI Fioralba;
SCOGNAMIGLIO Francesco;
SICA Valeria;
SIRICO Sara;
TAGLIERI Ettore;
VILLANO Martina.

Tecnici di amministrazione A3 F1 assunti a tempo determinato con i fondi del PNRR
AMORESANO Tommaso;
ARTIBANI Silvana;
CESTARO Gerardo;
COPPOLA Angelo;
DI GIACOMO Angelo;
NATALE Fortuna;
PALERMO Giuseppe;

Operatori data entry A2 F1 assunti a tempo determinato con i fondi del PNRR
CALIENDO Vincenzo;
GIACOMAZZA Marco;
PETROSINO Rosanna;
PIRONTI Giovanna;
PIZZUTI Alessia;
PORCARO Alberto;
RAIA Roberto;
SARNO Giuseppe;
TRUCILLO Anna Roberta;
VENTURA Vittorio.

Tirocinanti, giovani laureati in giurisprudenza, ammessi dalla Corte di Appello di Salerno ai sensi ex art. 73 del D.L. n. 69 del 21/6/2013 conv. in L. 8/8/2013 n. 98:

AMATO Maria
PEPE Alfonso
AMATO Diego
CHIARIELLO Benedetta
FERRAIOLI Gennaro
DI POTO Chiara
IORIO Arianna
VIOLANTE Carlo
D'AMATO Bianca
D'AMATO Virginia
D'ANIELLO Maria
FORTE Teresa
FORTINO Paola
BARONE Chiara
SIANO Maria Erica
ARTILLO Lucia
PERRINO Lucia
MARIANO Simona
MANZO Salvatore
MARRANDINO Rosa
MASSANOVA Marta
LIMA Simona
DI STASIO Camilla Maria
PAGANO Carmen
TEDESCHI Lucrezia
TROISI Emiliano
VOLPE Stefania

Personale utilizzato presso gli Uffici della Corte di Appello percettori di indennità di mobilità individuato dal centro per l'impiego di Salerno:
CASIELLO Lorenzina;
CATALDO Giovanni;
CERUSO Ernesto;
FARRO Teodolindo;
FRASCOLLA Sebastiano;
GALLO Felice;
GENTILE Donato;
LA VIA Claudio;
MEMOLI Antonio;
NIGRO Giovanni Pietro;
PALO Rosario;
RISI Diego;
SIRICO Enrico.

Al fine di una corretta applicazione della legge citata, nonché di una adeguata tutela dei diritti degli interessati, in relazione alle attività svolte nell'ambito di questo ufficio i soggetti nominati "Incaricati" dovranno attenersi alle seguenti indicazioni:

- trattare tutti i dati personali di cui vengono a conoscenza nell'ambito dello svolgimento delle proprie funzioni, in modo lecito e secondo correttezza;
- adottare le necessarie cautele per assicurare la segretezza della componente riservata della propria credenziale di autenticazione (utilizzare password non facilmente ricostruibile dai propri dati personali) che non dovrà essere comunicata a terzi e la custodia dei dispositivi;
- evitare di lasciare aperta una sessione di lavoro, dopo essersi identificati con il proprio login e la propria password, in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
- fornire in busta sigillata la copia delle proprie credenziali di autenticazione ai soggetti individuati per la custodia per gli interventi urgenti e indifferibili necessari per garantire l'operatività e la sicurezza del sistema;
- effettuare la raccolta, l'elaborazione, la registrazione ecc. di dati personali esclusivamente per gli

scopi inerenti l'attività svolta e nei limiti strettamente necessari per adempiere ai compiti assegnati a ciascuno;

- accedere, per lo svolgimento dei relativi compiti, a tutte le banche dati e archivi cartacei relativi ai nostri clienti e fornitori, mantenendo l'assoluto riserbo sui dati di cui vengono a conoscenza nell'esercizio delle proprie funzioni;
- mantenere aggiornate tutte le banche dati cui hanno accesso e non eccedere le finalità per le quali sono stati raccolti, elaborati e registrati;
- evitare di creare banche dati nuove senza espressa autorizzazione;
- conservare negli spazi e con i metodi indicati dal titolare/responsabile, tutti i documenti contenenti dati sensibili, evitando di trattenerli per un tempo superiore a quello minimo necessario per l'espletamento dei propri compiti ed in caso di interruzione anche temporanea del lavoro verificare che i dati non siano accessibili a terzi;
- con specifico riferimento agli atti e documenti cartacei contenenti dati personali ed alle loro copie, restituire gli stessi al termine delle operazioni affidate;
- evitare di asportare supporti informatici o cartacei contenenti dati personali di terzi, senza la previa autorizzazione del titolare/responsabile;
- in caso si constati o si sospetti un incidente di sicurezza deve essere data immediata comunicazione al titolare/responsabile del trattamento.

È fatto divieto di comunicare, diffondere, utilizzare i dati personali provenienti dalle banche dati della Corte di Appello. L'incaricato/a dovrà osservare scrupolosamente tutte le misure di sicurezza già in atto, o che verranno comunicate in seguito dal Titolare/Responsabile/Sub-Responsabile del trattamento.

Per quanto non su indicato si richiamano le disposizioni impartite in sede ministeriale e contenute nel "Piano strategico di sicurezza" **(PSS)** già trasmesso a tutto il personale e che è possibile consultare sul sito web della Corte alla sezione "Amministrazione trasparente", in uno al manuale di sicurezza predisposto da questo ufficio nonché tutta la legislazione di riferimento ed il D.M. 7 agosto 2018 di nomina del Responsabile della Protezione dei Dati (R.P.D.).

MANDA

All'U.D.I. per la comunicazione del presente atto a tutte le figure interessate.

Salerno lì, 28.03.2023

Il Titolare del Trattamento Dati
La PRESIDENTE
- Iside RUSSO -

CORTE DI APPELLO DI SALERNO

- Manuale di sicurezza per gli utenti -

PREMESSA

La Direzione Generale per i Sistemi Informativi Automatizzati (DGSIA) ha racchiuso la normativa in materia di sicurezza di trasmissione, interscambio, accesso e conservazione dei documenti informatici nel **PSS** (Piano strategico di sicurezza), trasmesso a tutte le articolazioni Ministeriali ed Uffici Giudiziari; questi sono tenuti a realizzare le misure proattive e reattive previste, per ridurre i rischi nel campo della sicurezza informatica e reagire agli eventuali incidenti.

I documenti informatici[1] trattati dall'Amministrazione Giudiziaria sono comunque inerenti a un'attività fondamentale della Stato che deve essere preservata da intromissioni esterne; devono essere trattati al fine di garantirne integrità e provenienza, disponibilità e confidenzialità (secretazione) e devono essere tutelati nell'ambito di specifici flussi di lavoro, considerandone la struttura e le specifiche tecniche di conservazione fisica, oltre che la tipologia giuridica.

Il trattamento[2] dei dati personali, svolto da questo ufficio nell'ambito esclusivo delle sue finalità istituzionali[3], con o senza ausilio degli strumenti elettronici, deve avvenire nel rispetto dei principi fissati dall'articolo 5 del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (*GDPR, General Data Protection Regulation)*:

- 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: 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 di quelli che risultino inesatti rispetto alle finalità del trattamento;
- limitazione della conservazione: è necessario provvedere alla conservazione dei dati per il tempo strettamente necessario agli scopi per i quali è stato effettuato il trattamento;
- integrità e riservatezza: occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento.

Per una corretta applicazione dei principi esposti, e quindi a garanzia di un'adeguata tutela dei diritti degli interessati, è importante che i dipendenti rispettino le seguenti indicazioni, tenuto conto che l'accesso alle Banche Dati avviene per mezzo di sistemi informatici censiti dalla DGSIA, sulla base dei profili di autorizzazione definiti dalle mansioni assegnate[4]:

- ☐ garantire i diritti degli interessati e comunque osservare il principio di necessità, di esattezza e aggiornamento delle informazioni trattate, nonché il principio di pertinenza;

---

[1] Art.1 lettera p) del Codice dell'Amministrazione Digitale: *rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*

[2] Art.4 nr.2): *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, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.*

[3] Art.6 let.e):*il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento*

[4] art.4 nr.10 GDPR e Art. 2-quaterdecies d.lgs.196/2003.

- trattare i dati personali di cui vengono a conoscenza nello svolgimento delle proprie funzioni in modo lecito e secondo correttezza, essendone vietata la diffusione, la comunicazione e l'utilizzo oltre il dovuto;
- effettuare la raccolta, l'elaborazione, la registrazione ecc.. di dati personali esclusivamente per gli scopi inerenti l'attività svolta e nei limiti strettamente necessari per adempiere ai compiti assegnati;
- osservare scrupolosamente tutte le misure di sicurezza già in atto, o che verranno comunicate in seguito dal Titolare/Responsabile/Sub-Responsabile del trattamento;
- assicurare la custodia dei dispositivi e la segretezza delle proprie credenziali di autenticazione (utilizzare password non facilmente ricostruibile dai propri dati personali), che non dovrà essere comunicata a terzi;
- cambiare la password almeno ogni sei mesi se sono trattati dati personali e ogni tre mesi quando sono trattati dati sensibili o giudiziari (su espressa autorizzazione di legge che specifichi la finalità di rilevante interesse pubblico, la tipologia dei dati trattati e le operazioni di trattamento);
- evitare di lasciare aperta una sessione di lavoro, dopo essersi identificati con il proprio login e la propria password, in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
- in caso di prolungata assenza o impedimento del dipendente che tratta dati personali, saranno impartite (dal direttore amministrativo responsabile dell'ufficio/cancelleria) idonee e preventive disposizioni scritte volte ad individuare le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici. In tal caso, la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della custodia delle copie i quali informeranno tempestivamente il dipendente dopo ogni intervento effettuato con le sue credenziali;
- garantire i diritti degli interessati e comunque osservare il principio di necessità., di esattezza e aggiornamento delle informazioni trattate, nonché il principio di pertinenza;
- effettuare la raccolta, l'elaborazione, la registrazione ecc.. di dati personali esclusivamente per gli scopi inerenti l'attività svolta e nei limiti strettamente necessari per adempiere ai compiti assegnati a ciascuno;
- mantenere aggiornate tutte le banche dati cui hanno accesso e non eccedere le finalità per le quali sono stati raccolti, elaborati e registrati;
- evitare di creare banche dati nuove senza espressa autorizzazione;
- conservare negli spazi e con i metodi indicati dal titolare/responsabile, tutti i documenti contenenti dati sensibili, evitando di trattenerli per un tempo superiore a quello minimo necessario per l'espletamento dei propri compiti ed in caso di interruzione anche temporanea del lavoro verificare che i dati non siano accessibili a terzi;
- con specifico riferimento agli atti e documenti cartacei contenenti dati personali ed alle loro copie, restituire gli stessi al termine delle operazioni affidate;
- evitare di asportare supporti informatici o cartacei contenenti dati personali di terzi, senza la previa autorizzazione del titolare/responsabile;
- in caso si constati o si sospetti un incidente di sicurezza deve essere data immediata comunicazione al dirigente dell'ufficio responsabile per la successiva comunicazione al titolare/responsabile del trattamento.

Di seguito i principali suggerimenti e le istruzioni per aumentare la sicurezza globale del sistema:

TRATTAMENTO DATI CON STRUMENTI ELETTRONICI
CAUTELE GENERALI

Spegnere il computer se ci si assenta per un periodo di tempo lungo

Un computer acceso è in linea di principio maggiormente attaccabile perché raggiungibile tramite la rete o direttamente sulla postazione di lavoro; più lungo è il periodo di assenza, inoltre, maggiore è la probabilità che un'interruzione dell'energia elettrica possa portare un danno.

Non lasciare lavori incompiuti sullo schermo ed evitare di lasciare aperta una sessione di lavoro dopo essersi identificati
Chiudete le applicazioni con cui state lavorando quando vi allontanate dal posto di lavoro: potreste rimanere lontani più del previsto, e una postazione aperta è vulnerabile a trattamenti non autorizzati.

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

Non riutilizzare supporti rimovibili (CD, pen-drive ecc..) per affidare a terzi i vostri dati

Quando un file viene cancellato da un supporto magnetico, i dati non vengono effettivamente eliminati dal disco ma soltanto marcati come non utilizzati e sono facilmente recuperabili. Neanche la formattazione assicura l'eliminazione dei dati dai dischi. Solo l'uso di un apposito programma di cancellazione sicura garantisce che sul dischetto non resti traccia dei dati precedenti. Se ciò non è possibile, essi devono essere distrutti e comunque è sempre meglio usare un dischetto nuovo.

Prestare particolare attenzione all'utilizzo dei computer portatili

I PC portatili sono un facile bersaglio per i ladri. Se avete necessità di gestire dati riservati su un portatile, proteggetelo con una password sul BIOS, fate installare un programma di cifratura del disco rigido (per impedire la lettura dei dati in caso di furto) ed **effettuate periodicamente il backup**.

Fare attenzione a non essere spiati mentre si digita una password o qualunque codice di accesso
Anche se molti programmi non ripetono in chiaro la password sullo schermo, quando digitate una password questa potrebbe essere letta guardando i tasti che state battendo, anche se avete buone capacità di dattiloscrittura. Chiedete agli astanti di guardare da un'altra parte quando introducete una password o controllate che nessuno stia guardando.

Proteggere il proprio computer con una password. Abilitare ove possibile l'accesso tramite password
La maggior parte dei computer offre la possibilità di impostare una password all'accensione. Anche alcuni applicativi permettono di proteggere i propri dati tramite password. Imparate a utilizzare queste caratteristiche che offrono un buon livello di riservatezza. Non permettere l'uso del proprio computer o del proprio account da personale esterno, a meno di non essere sicuri della loro identità. Personale esterno può avere bisogno di installare del nuovo software/hardware nel vostro computer. Assicuratevi dell'identità della persona e delle autorizzazioni ad operare sul vostro PC.

Non utilizzare apparecchiature non autorizzate o per cui non si è autorizzati
L'utilizzo di modem su postazioni di lavoro collegate alla rete di ufficio offre una porta d'accesso dall'esterno non solo al vostro computer ma a tutta la rete di cui fate parte. E' quindi **vietato** l'uso di modem all'interno della rete locale. Nel caso che ciò sia strettamente necessario, disconnettere fisicamente la postazione di lavoro dalla rete locale prima di effettuare il collegamento via modem. Per l'uso di altre apparecchiature, chiedere consiglio al Presidio CISIA competente.

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

Diffidare dei dati o dei programmi la cui provenienza non è certa
Per proteggersi di virus ed altri agenti attivi di attacco, anche se la fonte appare affidabile o il contenuto molto interessante; molti sistemi di attacco inviano dati che sembrano provenire da un utente noto al destinatario per vincerne la naturale diffidenza nei confronti degli estranei.

Applicare con cura le linee guida per la prevenzione da infezioni da virus
La prevenzione dalle infezioni da virus sul vostro computer è molto più facile e comporta uno spreco di tempo molto minore rispetto alla correzione degli effetti di un virus. Inoltre, se non avete attivato adeguate misure anti-virus potreste incorrere in una perdita irreparabile di dati o in un blocco anche molto prolungato della vostra postazione di lavoro.

Proteggere attentamente i dati
Bisogna prestare particolare attenzione ai dati di cui si è personalmente responsabili. Come minimo bisogna posizionarli in un'area protetta da password e non dare di default a nessun altro utente il permesso di lettura o modifica. Ai dati da condividere applicare i permessi opportuni solo per il tempo strettamente necessario all'interazione con gli altri utenti.
L'utilizzo dei dati personali deve avvenire in base al principio del *"need to Know"*: non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative (anche se queste persone sono a loro volta incaricate del trattamento). I dati non devono essere comunicati all'esterno dell'Ufficio Giudiziario e comunque a soggetti terzi se non previa autorizzazione.

Usare, se possibile, il salvataggio automatico dei dati. Non dimenticare i salvataggi volontari
Molti applicativi, ad esempio quelli di videoscrittura, salvano automaticamente il lavoro a intervalli fissi, in modo da minimizzare il rischio di perdita accidentale dei dati. Imparate comunque a salvare manualmente il vostro lavoro con una certa frequenza, in modo da prendere l'abitudine di gestire voi stessi i dati e non fare esclusivo affidamento sul sistema.
La regola generale è quella di procedere al ***backup periodico dei dati*** *su supporti o su cartelle ospitate sui server, misure di sicurezza che devono essere eseguite da ogni utente, anche per evitare che la rottura o il malfunzionamento dell'hard disk comprometta il lavoro e causi la perdita dei dati.*

Utilizzo del PC
L'utente deve attenersi scrupolosamente all'utilizzo del PC solo ed esclusivamente per attività di Ufficio, ed è fatto divieto, salvo operazioni semplici (p.e., sostituzione di mouse, di tastiera) che non possano compromettere la funzionalità del PC, assumere iniziative personali per porre rimedio ad eventuali problemi tecnici, in particolar modo di tipo hardware; in tale caso è consigliabile rivolgersi al proprio ufficio che curerà la pratica di assistenza (Ufficio per l'Innovazione del Distretto o Ufficio Economato/Beni Patrimoniali) e in caso di urgenza contattare il Presidio CISIA.
I dati personali conservati sui PC devono essere cancellati in modo sicuro (chiamare l'assistenza sistemistica per formattare i dischi) prima di destinare i PC ad usi diversi.

Amministrare correttamente le password
Con l'arruolamento delle postazioni di lavoro sul sistema nazionale ADN vengono utilizzate dei criteri e policy di sicurezza più rigidi. In particolare se l'utente inserisce erroneamente per tre volte consecutive le proprie credenziali l'account viene bloccato per un certo lasso di tempo ed inoltre la password ha una durata 90 gg. Per quanto riguarda le regole di composizione della password valgono le seguenti regole previste dall'articolo 25 comma 3 del **DM 24/5/2001** e le Linee Guida per la configurazione per adeguare la sicurezza del software di base AGID 2020:

- devono essere composte da almeno otto caratteri in funzione delle criticità delle informazioni da difendere (es. 15 caratteri per utenze amministrative);
- devono contenere almeno tre tipi diversi di caratteri inclusi tra quelli maiuscoli, minuscoli, cifre e simboli di interpunzione;
- non devono essere parole presenti in dizionari delle lingue più diffuse;
- non devono essere basate su parole dialettali o gergali;
- non devono essere basate su informazioni personali come data di nascita, numeri di telefono, indirizzi;

- non devono essere basate su informazioni personali di familiari, amici, colleghi, attori, personaggi famosi, ecc.;
- non devono essere termini tecnici o informatici, comandi, siti, società. ecc.;
- non devono essere del tipo aaabbb, 123456, fedcba, o simili;
- non devono essere password dei tipi elencati in precedenza scritte al contrario;
- non devono essere basate su password analoghe alle precedenti con l'aggiunta di cifre prima o dopo.

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

- non rivelare le password a nessuno, inclusi amici e familiari;
- non condividere le password con altri colleghi o assistenti, salvo quanto disposto a proposito dell'utilizzo del programma "SCRIPT@";
- non inviare le password tramite e-mail o altri metodi di comunicazione elettronica, né tramite telefono;
- non mostrare a video le password (ma neanche PIN, passphrase, ecc.., in generale: chiavi segrete) quando viene inserita e non dare indicazioni sulla sua lunghezza;
- cambiare obbligatoriamente al primo log-on la password temporanea;
- non scrivere le password su carta o biglietti e non memorizzare le password su file o altri sistemi (palmari o agende elettroniche) senza cifratura;
- non scrivere la propria password su questionari o presunti moduli di sicurezza;
- non parlare della propria password o rivelare indizi su essa;
- non utilizzare sistemi informatici che permettono di memorizzare le password o gestire un database di password;
- non riutilizzare in nessun caso le password già utilizzate in precedenza.

Non violare le leggi in materia di sicurezza informatica.

Ricordatevi che anche solo un tentativo di ingresso non autorizzato in un sistema costituisce un reato. Se siete interessati a studiare la sicurezza della vostra postazione di lavoro o della rete di cui fate parte, chiedete preventivamente l'autorizzazione al Referente locale della sicurezza del singolo Ufficio. Non utilizzate senza autorizzazione software che possa creare problemi di sicurezza o danneggiare la rete, come port scanner, security scanner, network monitor, network flooder, fabbriche di virus o di worm.

Segnalare tempestivamente qualsiasi variazione del comportamento della propria postazione di lavoro

Può essere il sintomo di un attacco in corso.

Segnalare comportamenti che possano far pensare a tentativi di ridurre la sicurezza del sistema informativo

Ad esempio segnalate al Responsabile della sicurezza dell'Ufficio se un altro utente insiste per avere accesso ai vostri dati o per conoscere la vostra password o per poter lavorare sulla vostra postazione di lavoro. Analogamente non fidatevi e segnalate telefonate o messaggi che sembrano provenire da un sistema e vi chiedono di fare operazioni strane sul vostro computer (ad esempio, cambiare subito la password con una datavi al telefono o nel corpo del messaggio).

Si fa presente che per ogni ulteriore informazione sulle modalità di comportamento da tenere sul luogo di lavoro è necessario far riferimento al responsabile o al titolare del trattamento dei dati.

PRESCRIZIONI PARTICOLARMENTE IMPORTANTI
VIRUS E MISURE ANTIVIRUS

Gli utenti devono:

- usare soltanto programmi provenienti da fonti fidate perché copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato;

- assicurarsi di non far partire accidentalmente il computer da supporto esterno e, se possibile, impostare il BIOS in modo da avere come *primary boot device* il disco rigido e proteggere l'accesso al BIOS tramite password. Se il supporto fosse infetto, il virus potrebbe trasferirsi nella memoria RAM ed infettare altri file;
- proteggere i supporti da scrittura quando possibile. È il più efficace mezzo di prevenzione, infatti i virus non possono rimuovere la protezione meccanica;
- salvare o sottoporre a backup i dati importanti per evitare di perderli in caso di infezione.

Gli utenti non devono:

- aprire mail di provenienza sospetta e, in generale, non aprire nessun allegato senza una preventiva scansione anti-virus;
- visitare siti illegali, usati come specchietto per le allodole per attirare visitatori su cui condurre attacchi;
- modificare le configurazioni del software antivirus.

POSTA ELETTRONICA

Gli utenti devono:

- Prestare la massima attenzione nella apertura dei file allegati a messaggi di posta elettronica certificata, ivi compresi quelli ricevuti mediante il protocollo documentale, perché potrebbero contenere allegati malevoli;
- usare solo il software di posta approvato dal Ministero della Giustizia;
- effettuare la scansione con programmi di controllo antivirus approvati dal Ministero dei messaggi in ingresso per evitare virus o contenuti maligni;
- impedire ad altre persone di utilizzare il proprio account per inviare posta elettronica;
- trasmettere dati confidenziali solo se adeguatamente cifrati (standard S/MIME);
- trasmettere di preferenza messaggi con firma digitale (standard S/MIME con firma di tipo deatched), per garantire al destinatario l'origine del messaggio; si noti che questa tecnica, pur basandosi sui medesimi principi della firma digitale usata per la sottoscrizione di documenti elettronici con valore legale, è fondamentalmente diversa e viene usata nello standard S/MIME per garantire l'autenticità dei messaggi di posta elettronica ed evitare quindi la generazione di messaggi falsi ("fake mail") che potrebbero indurre in errore utenti inesperti;

gli utenti non devono:

- utilizzare la posta elettronica per scopi in conflitto con il piano di sicurezza ed in ogni caso non utilizzarla eccessivamente per scopi personali;
- partecipare alle cosiddette "Catene di Sant'Antonio" o, in generale, non utilizzare la posta elettronica per spamming;
- inviare mai informazioni confidenziali tramite posta elettronica non cifrata;
- aprire posta elettronica di provenienza dubbia, accertarsi sempre della provenienza dei messaggi di posta elettronica contenente allegati, nel caso che il mittente dia origine a dubbi, cancellare direttamente il messaggio senza aprire gli allegati. Per una corretta ed approfondita analisi della presunta e-mail malevola, inoltrare il messaggio all'indirizzo antispam.dgsia@giustizia.it

INTERNET

- Evitare l'accesso a siti in contrasto con il profilo etico specifico della nostra organizzazione o che possono costituire motivo di distrazione nell'espletamento dell'attività lavorativa;
- Salvaguardare la rete geografica da un uso eccessivo e non legato ad esigenze lavorative del servizio di navigazione Internet.

TRATTAMENTO DATI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

CAUTELE GENERALI

Chiudere a chiave armadi/cassetti ed uffici

Il primo livello di protezione di qualunque sistema è quello fisico. E' certamente vero che una porta chiusa può in molti casi non costituire una protezione sufficiente, ma è anche vero che pone se non altro un primo ostacolo, e richiede comunque uno sforzo volontario non banale per la sua rimozione.

È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sbirciare i documenti posti su una scrivania o visibili su uno schermo. Pertanto, chiudete a chiave il vostro ufficio alla fine della giornata ed ogni volta che vi assentate. Inoltre chiudete i documenti a chiave nei cassetti ogni volta che potete. I documenti contenenti dati personali non devono in alcun modo rimanere incustoditi e a fine giornata devono essere riposti in armadi /cassetti chiusi a chiave in modo da non essere accessibili a persone non autorizzate.

Conservare supporti di memoria e stampe in luoghi sicuri
Alla conservazione dei supporti di memoria (CD, pen-drive….) si applicano gli stessi criteri di protezione dei documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può anche essere dovuto a un furto) può passare più facilmente inosservato. A meno che non siate sicuri che contengano solo informazioni non sensibili, riponeteli sotto chiave non appena avete finito di usarli.

Maneggiare e custodire con cura le stampe di materiale riservato
Non lasciate accedere alle stampe persone non autorizzate. Se la stampante non si trova sulla vostra scrivania recatevi il più in fretta possibile a ritirare le stampe. Per stampe riservate cercate di usare una stampante non condivisa oppure usate la modalità di stampa ritardata impostando un tempo sufficiente a permettervi di raggiungere la stampante prima dell'inizio della stampa. Distruggete personalmente le stampe quando non servono più.

Non gettare nel cestino le stampe di documenti che possono contenere informazioni confidenziali.
Se trattate dati di particolare riservatezza, considerate la possibilità di dotarvi di una distruggi-documenti (shredder); in ogni caso non gettate mai documenti cartacei senza averli prima sminuzzati in modo da non essere ricomponibili.

Sanzioni per inosservanza delle norme

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

Il Dirigente Amministrativo
- dott.ssa Francesca Del Grosso -

La Presidente
- dott.ssa Isabella Russo -

NUMERI DI ASSISTENZA AGLI APPLICATIVI MINISTERIALI

(sw nazionali approvati dal Responsabile dei Sistemi Informativi Automatizzati, ai sensi dell'art. 12 dell'allegato al D.M. 27 aprile 2009):

Servizio di Help Desk per la Conduzione dei Sistemi ed il nuovo servizio di Assistenza Applicativa attivo dal 1° ottobre 2022

Per ogni problematica (guasti hardware, alla rete locale e rete geografica, per attività di system management e per applicativi area penale, civile e TIME MANAGEMENT, per servizi di Interoperabilità (posta elettronica, posta elettronica certificata ed Internet) è possibile aprire in autonomia un ticket al numero verde 800749049, comunicando nominativo e PIN attribuito al momento della registrazione in ADN, o collegandosi con le proprie credenziali ADN al sito web https://helpdesk.giustizia.it/, o mandando una mail a assistenza@giustizia.it. In caso di smarrimento, è possibile recuperare il PIN rivolgendosi al referente GSI/IAA/MultiUX dell'Ufficio.

Il CISIA di Napoli ha di recente raccomandato l'uso del portale https://helpdesk.giustizia.it quale canale primario di interazione con il servizio di assistenza e di apertura dei ticket, disponibile via web anche all'esterno della Rete Unitaria Giustizia (RUG).
Il ricorso all'uso del portale al posto della e-mail istituzionale comporta diversi vantaggi, ad esempio:

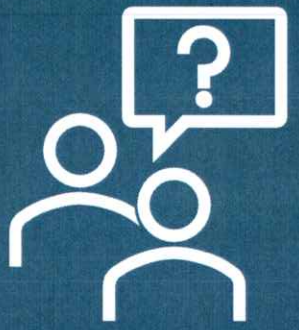
- **completa autonomia nell'apertura del ticket (anche per conto di un collega);**
- **riduzione dei tempi di presa in carico della richiesta;**
- **possibilità di monitorare lo stato del ticket in tempo reale;**
- **possibilità di inserire tutti i dettagli necessari per la risoluzione del problema;**
- **possibilità di esprimere di esprimere il proprio livello di soddisfazione sul servizio;**
- **possibilità di chiedere la riapertura del ticket in caso di risoluzione incompleta o insoddisfacente.**

Oltre al portale, si rammenta che per l'apertura dei ticket è disponibile anche il numero verde 800.749.049 disponibile dalle ore 08:00 alle ore 18:00 dal lunedì al venerdì e dalle ore 08:00 alle ore 13:00 del sabato.

L'apertura dei ticket via email all'indirizzo assistenza@giustizia.it sarà presto disattivata.

Si allega la **brochure** con ulteriori informazioni.

Nuove modalità di contatto **dell'assistenza**



Gentile Utente,

La informiamo che a partire dal 1° ottobre 2022 cambieranno i canali di contatto **dell'assistenza** (Help Desk) ed al fine di migliorare la qualità del servizio offerto saranno introdotte nuove funzionalità

I tre canali previsti

1. Portale

helpdesk.giustizia.it

2. Numero Verde

800.749.049

3. E-mail

assistenza@giustizia.it

DGSIA

1. Portale web

helpdesk.giustizia.it

Dal 1° ottobre 2022 **sarà disponibile** il nuovo portale per **l'apertura** dei ticket **che** Le consentirà di segnalare la problematica in completa autonomia, anche al di fuori **dell'orario** di servizio **dell'Help** Desk.

Principali funzionalità utili

- Monitoraggio in tempo reale dello stato di avanzamento di tutti i ticket a Lei associati, a prescindere dal canale di apertura
- Una sezione di Knowledge Base in continua crescita, che si arricchirà di contenuti informativi sempre a Sua disposizione per facilitare la risoluzione in autonomia delle problematiche più comuni
- Catalogo dei servizi per facilitare le richieste **all'Help** Desk
- Possibilità di scambiare messaggi con **l'operatore** dal portale
- Possibilità di valutare il servizio ricevuto e fornire suggerimenti per il continuo miglioramento del servizio stesso

2. Numero verde
800.749.049

Il servizio è attivo nei seguenti orari:
Lunedì – Venerdì: 08:00 – 18:00
Sabato: 08:00 – 13:00

Lotto 2: Valle d'Aosta, Piemonte, Liguria, Lombardia, Trentino-Alto Adige, Veneto, Friuli-Venezia Giulia, Emilia Romagna, Sardegna

Lotto 3: Toscana, Umbria, Lazio

Lotto 4: Marche, Abruzzo, Molise, Campania, Puglia, Basilicata, Calabria, Sicilia

Viene di seguito presentata **l'alberatura** che, mediante selezione numerica, Le permetterà di entrare in contatto con il Lotto o il servizio di Suo interesse

Nota bene: *in caso di chiamata da un numero telefonico dell'Amministrazione, dopo aver selezionato il tasto 1, sarà automaticamente messa in contatto con il Lotto a Lei associato*

1 Assistenza agli Uffici territoriali su applicativi, Postazioni di Lavoro e Reset Password

- 2 Lotto 2 (Area Nord)
- 3 Lotto 3 (Area Centro)
- 4 Lotto 4 (Area Sud)
- 5 Lotto 5 (Uffici Centrali)
- 6 Lotto 6 (Cassazione)

2 Assistenza sul processo civile telematico in Cassazione

- 1 Libero Foro e Avvocatura dello Stato
- 2 Magistrati della Suprema Corte e relativo Personale amministrativo

3 Assistenza su applicativi esterni

- 1 SICOGE

DGSIA

3. Mail

assistenza@giustizia.it

Il canale mail è uno strumento unidirezionale attraverso cui potrà segnalare **all'assistenza** la propria problematica

La mail dovrà essere inviata **dall'indirizzo** di posta personale (dominio @giustizia.it)

Potrà consultare il relativo ticket ed interagire con **l'operatore** accedendo nella sezione dedicata del portale

Di seguito alcuni suggerimento al fine di agevolare **l'operatore** nella comprensione della richiesta e velocizzarne la risoluzione:

Oggetto:

breve e conciso, utilizzando parole chiave per **l'identificazione della problematica o della** richiesta come, ad esempio, il nome **dell'applicativo con riferimento al quale si richiede l'intervento**

Corpo:

dettaglio della problematica ed eventuale **indicazione di un'utenza terza per la quale si richiede l'intervento**

Nel caso in cui le informazioni non siano sufficienti per procedere con l'apertura e la conseguente lavorazione del ticket, l'operatore La ricontatterà tramite portale per reperire ulteriori informazioni, prolungando i tempi di lavorazione