PROCURA DELLA REPUBBLICA SIRACUSA

Documento Programmatico per la Sicurezza

Anno 2016

INTRODUZIONE

Obiettivo di questo Documento è di delineare il quadro delle misure di sicurezza organizzative, fisiche e logiche da adottare affinché siano rispettati gli obblighi in materia di sicurezza del trattamento dei dati effettuato dalla Procura della Repubblica di Siracusa, con sede in Viale Santa Panagia, 109, allo scopo di ridurre ai minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Il Documento Programmatico sulla Sicurezza (di seguito denominato DPS) definisce le politiche e gli standard di sicurezza in merito al trattamento dei dati personali. Esso riguarda il trattamento di tutti i dati personali (comuni, sensibili e giudiziari) espletato per mezzo di strumenti di elaborazione elettronici e di strumenti di elaborazione non elettronici (cartacei, audio, visivi, audiovisivi, etc.) e deve essere conosciuto ed applicato da tutti coloro che fanno parte dell'organizzazione.

Eventuali situazioni di deviazione accertate rispetto a quanto precisato nel presente DPS dovranno essere rimosse nel più breve tempo possibile.

APPLICABILITA'

Le linee guida in conformità all'art. 34 codice sulla privacy e All. B, regola 19, medesimo indice, e le prescrizioni contenute nel presente DPS si applicano a tutte le procedure elettroniche, digitali e cartacee che i titolari, i responsabili, gli incaricati, a vario titolo, del trattamento e delle sessioni di trattamento dei dati effettuati dalla Procura della Repubblica di Siracusa eseguono.

Sono, altresì, soggetti alle prescrizioni del DPS la tenuta, la custodia a la sicurezza dei locali e degli uffici e la conservazione degli incarti e dei fascicoli.

REVISIONE E VALIDITA' DEL PRESENTE DOCUMENTO

II presente Documento è valido fino a quando la struttura e l'organigramma dell'Ufficio non subiranno variazioni, nel qual caso esso dovrà essere immediatamente aggiornato e portato a conoscenza del personale.

In ogni caso, il DPS dovrà essere aggiornato e riscritto immancabilmente entro il 31 marzo di ogni anno, ai sensi dell'art 19 All. B codice privacy.

Gli aggiornamenti terranno presenti anche i livelli di rischio a cui sono soggetti i dati personali, comuni, sensibili e giudiziari nonché eventuali modifiche della tecnologia informatica.

QUADRO NORMATIVO RIFERIMENTO

- D. Lgs. n. 196/2003 (Codice in materia di dati personali);
- Allegato B al D. Lgs. n. 196/2003 (Disciplinare Tecnico in Materia di Misure Minime di Sicurezza);
- L. 18 marzo 2008, n.48;
- D.Lgs. 30 maggio 2008, n. 109;
- Deliberazione 26 giugno 2006, n. 46 dell'Autorità Garante per la protezione dei dati generali sul trattamento dei dati da parte di consulenti tecnici e ausiliari del p.m.;
- L. 6 agosto 2008, n. 113 (di conversione con modifiche del D.L. 25 giugno 2008, n. 172;
- L. 30 dicembre 2008, n. 207;
- L. 4 marzo 2009, n. 15;
- L. 27 febbraio 2009, n.14;
- Delibera 2 Dicembre 2010, del Garante per la protezione dei dati personali, Linee guida in materia di trattamento di dati personali nella riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica;

- D. Lgs. 28 maggio 2012, n. 69;
- Provvedimento dell'Autorità Garante per la protezione dei dati personali del 18 luglio 2013, in materia di misure di sicurezza nelle attività di intercettazione da parte delle Procure della Repubblica;
- Parere n. 584 del 18 dicembre 2013 sullo schema di provvedimento in materia di regole tecniche per l'adozione nel processo civile e nel processo penale delle tecnologie dell'informazione e della comunicazione;
- Relazione annuale del Garante del 1998, punto 2.14;
- Relazione annuale del Garante del 2010;
- Relazione annuale del Garante del 2011;
- Relazione annuale del Garante del 2012;
- Relazione annuale del Garante del 2013;
- Relazione annuale del Garante del 2014;

STRUTTURA DEL DOCUMENTO

Conformemente a quanta prescrive il punto 19 del Disciplinare Tecnico, Allegato B al I). Lgs. n. 196/2003, nel presente DPS si forniscono idonee informazioni riguardanti:

- l'elenco dei trattamenti di dati personali;
- la elencazione dei soggetti che trattano i dati, la descrizione delle aree, dei locali e degli strumenti con i quali si effettuano i trattamenti;
- la individuazione dei tipi di dati personali trattati;
- la distribuzione dei compiti e delle responsabilità, nell'ambito delle strutture preposte al trattamento dei dati:
- l’analisi dei rischi che incombono sui dati;
- le misure, già adottate e da adottare, per garantire l'integrita e la disponibilità dei dati, nonchè la protezione delle aree e dei locali rilevanti ai fini della loro custodia e accessibilità;
- i criteri e le modalità di ripristino dei dati in seguito a distruzione o danneggiamento di cui al punto 23 dell'All. B del codice della privacy;
- la previsione di interventi formativi degli incaricati del trattamento;

• i criteri da adottare, per garantire l'adozione delle misure minime di sicurezza, in caso di trattamenti di dati personali affidati all'esterno;

• per i dati personali idonei a rilevare lo stato di salute e la vita sessuale di cui al punto 24, i criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

DEFINIZIONI

- **Trattamento**: qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, 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 di dati, anche se non registrati in una banca dati.
- **Dato anonimo**: dato che, in origine o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.
- **Dato personale**: qualunque intimazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
- **Dato identificativo**: data personale che permette l'identificazione diretta dell'interessato.

- **Dato sensibile**: dato personale idoneo a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso e filosofico, politico o sindacale, nonchè dato personale idoneo a rivelare lo state di salute e la vita sessuale.
- **Dato giudiziario**: dato personale idoneo a rivelare provvedimenti di cui all'art.3, comma I. lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli arti. 60 e 61 del Codice di Procedura Penale, con esclusione di quelli riguardanti interdizioni, inabilitazioni, amministrazioni di sostegno, concordato fallimentare, fallimento e riabilitazione del fallito.
- **Titolari del trattamento**: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
- **Responsabile del trattamento**: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati

personali. La designazione di un responsabile è facoltativa e non esonera da responsabilità il titolare, il quale ha comunque l'obbligo di impartirgli precise istruzioni e di vigilare sull'attuazione di queste. II responsabile deve essere un soggetto che fornisce, per esperienza, capacita ed affidabilità, idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Il responsabile del trattamento dei dati personali, ai fini della sicurezza, ha le responsabilità indicate nella lettera di incarico.

- **Incaricato del trattamento**: il soggetto, nominato dal titolare o dal responsabile del trattamento, che tratta i dati. L'incaricato del trattamento dei dati, con specifico riferimento alla sicurezza, ha le responsabilità indicate nella lettera di incarico.
- **Interessato del trattamento**: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.
- **Comunicazione**: il dare conoscenza del dato personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
- **Diffusione**: il dare conoscenza del dato personale a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

- **Blocco**: la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.
- **Banca dati**: qualsiasi complesso di dati personali, ripartito in una o più unità dislocate in uno più siti, organizzato secondo una pluralità di criteri determinati tali da facilitarne il trattamento;
- **Misure minime**: il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza con configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'art. 31 del D.Lgs. 196/2003.

TRATTAMENTO DI DATI SENSIBILI E GIUDIZIARI

L'art. 22 del codice detta principi applicabili al trattamento di dati sensibili e giudiziari.

Tale norma non si applica "se il trattamento è effettuato per ragioni di giustizia" (art. 47). Si intendono effettuati per ragioni di giustizia quei "trattamenti di dati personali direttamente correlati alla trattazione giudiziaria di affari e di controversie, o che, in materia di trattamento giuridico ed economico del personale di magistratura, hanno una diretta incidenza sulla funzione giurisdizionale, nonché le attività ispettive su uffici giudiziari."

Le medesime ragioni di giustizia non ricorrono "per l'ordinaria attività amministrativa e gestionale di personale, mesi o strutture, quando non è

pregiudicata la segretezza di atti direttamente connessi alla predetta trattazione" (art. 47, comma 2).

In quest' ultimo campo, pertanto, tornano applicabili i principi dell'art. 22, tra i quali le seguenti disposizioni:

a) il trattamento dei dati sensibili e giudiziari si conforma al criterio di prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato;

b) possono essere trattati solo i dati indispensabili per svolgere attività istituzionali che non possono essere adempiute mediante il trattamento di dati anonimi o di dati personali di natura diversa;

e) il soggetto pubblico che tratta i dati deve periodicamente verificarne la esattezza, l'aggiornamento, la non eccedenza e la indispensabilità rispetto alle finalità istituzionali perseguite, pena la inutilizzabilità;

d) i dati sensibili e giudiziari contenuti in elenchi, registri e banche dati sono trattati con tecniche di cifratura o mediante codici identificativi che li rendano temporaneamente intellegibili;

e) i dati idonei a rivelare lo stato di salute non possono essere diffusi.

Ai sensi dell'art. 4 n. 9 della legge 4.3.2009, n. 15 poiché "le notizie concernenti lo svolgimento delle prestazioni di chiunque sia addetto ad una funzione pubblica e la relativa valutazione non sono oggetto di protezione della riservatezza personale" non fanno parte del parte del documento tali notizie.

Gli operatori, magistrati, personale amministrativo e di polizia giudiziaria terranno presente che il trattamento di dati personali per ragioni di giustizia nell'ambito degli uffici giudiziari è soggetto solo ad alcune regole

del d. lgs. n. 196 del 2003, in ossequio al disposto di cui all’art. 4. Il Garante ha evidenziato i limiti in cui la legge è applicabile, nonché i princìpi di correttezza del trattamento, di pertinenza e non eccedenza dei dati trattati, sanciti dall'art. 9 della legge anche in riferimento alla Convenzione n. 108/1981 del Consiglio d'Europa, che sono stati richiamati fra l'altro nella decisione del Garante del 22 ottobre 1998, relativa alla notificazione di atti giudiziari e amministrativi;

DISCIPLINARE IN MATERIA DI MISURE MINIME DI SICUREZZA

1. Elenco dei trattamenti di dati personali

I trattamenti di dati personali effettuati nell'ufficio riguardano unicamente i trattamenti per ragioni di giustizia, in conformità alle disposizioni dei codici di rito, dell'ordinamento giudiziario e delle leggi speciali.
Nella ordinaria attività amministrativa - gestionale del personale, l'ufficio non tratta dati sensibili idonei a rivelare lo stato di salute o la vita sessuale dei dipendenti. Nei certificati medici prodotti dai dipendenti e nell'esito delle visite fiscali eseguite in seguito ad assenze per malattia, vengono rigorosamente omesse le diagnosi.
Allo stesso criterio si conformano le visite effettuate sul personale ai sensi della legge n. 626/1994 e successive modifiche, i cui esiti pervengono all'ufficio in plichi chiusi.

2. Distribuzione di compiti e responsabilità

Fatta salva la responsabilità del magistrato dirigente dell'ufficio Procuratore della Repubblica dott. **Francesco Paolo GIORDANO**, in ordine alle modalità del trattamento dei dati personali, all'organizzazione dell'ufficio in funzione della miglior protezione possibile dei dati personali e all'aggiornamento annuale del D.P.S. (Documento Programmatico sulla Sicurezza), nonché in ordine ai procedimenti e processi personalmente

trattati, sono nominati responsabili del servizio in materia di trattamento dei dati personali, limitatamente agli uffici ai quali sono preposti:

1) L'Assistente Capo della Polizia di Stato **Vincenzo LO IACONO**, in ordine alle sue funzioni di Responsabile del **S**istema **I**nformatico della **C**ognizione **P**enale per la Procura della Repubblica di Siracusa, secondo le direttive impartite dal magistrato dirigente dell'ufficio e in ottemperanza alle disposizioni emanate dal Ministero della Giustizia - Direzione generale dei Sistemi informatici automatizzati, per la gestione, il controllo della qualità e la sicurezza dei dati presenti nel sistema RegeWeb e nell'utilizzo degli applicativi S.I.R.I.S., Consolle Penale e Portale N.D.R.;

2) Il Dirigente Amministrativo dott.ssa **Silvana ZAPPALA'**, con riguardo alle attività proprie della sua funzione di dirigente amministrativo, per la gestione degli archivi informatici e dei fascicoli relativi al personale amministrativo;

3) Il Procuratore della Repubblica Aggiunto dott. **Fabio SCAVONE** e i Sostituti Procuratori Dott. **Andrea PALMIERI**, Dott. **Antonio NICASTRO**, Dott. **Maurizio MUSCO,** Dott. **Giancarlo LONGO**, Dott.ssa **Caterina ALOISI**, Dott. **Tommaso PAGANO**, Dott.ssa **Magda GUARNACCIA**, Dott.ssa Margherita **BRIANESE**, Dott. **Salvatore GRILLO,** Dott. **Vincenzo NITTI** Dott. **Vincenzo NITTI**, tutti con riguardo agli affari loro assegnati e alle attività

conseguenti e connesse ed alle funzioni di coordinamento dei Gruppi specializzati (come da Progetto Organizzativo);

4) Il Direttore amministrativo dott. **Gaetano ROGGIO** in ordine alla direzione e responsabilità della Sezione Civile, Ufficio Funzionario Delegato e Ufficio Spese di giustizia con riguardo agli affari ad egli assegnati e alle attività conseguenti e connesse;

5) Il Funzionario Giudiziario dott. **Michele SPINELLA** per la gestione, il controllo e la sicurezza degli archivi informatici S.I.E.S., S.I.A.P. e S.I.C. ed in ordine alle sue funzioni di Responsabile Casellario giudiziale – Carichi Pendenti, attenendosi alle disposizioni del decreto dirigenziale 25.1.2007, di Responsabile dell'Ufficio Esecuzioni, delle misure di prevenzione e delle demolizioni delle opere edilizie abusive;

6) Il Funzionario Giudiziario Sig.ra **Maria Rita STRACQUADANIO**, per la gestione, il controllo e la sicurezza della tenuta degli archivi informatici e cartacei del Registro delle Intercettazioni e con riguardo alle sue funzioni di Responsabile del Centro Intercettazioni, Archivio intercettazioni e Rilevazioni Statistiche ed adempimenti ex art. 127 disp. Att. c.p.p.;
7) Il Funzionario giudiziario **Sig.ra Milena BORGIONE**, in ordine al S.I.D.I.P., allo S.D.A.S. e al Coordinamento delle Segreterie penali

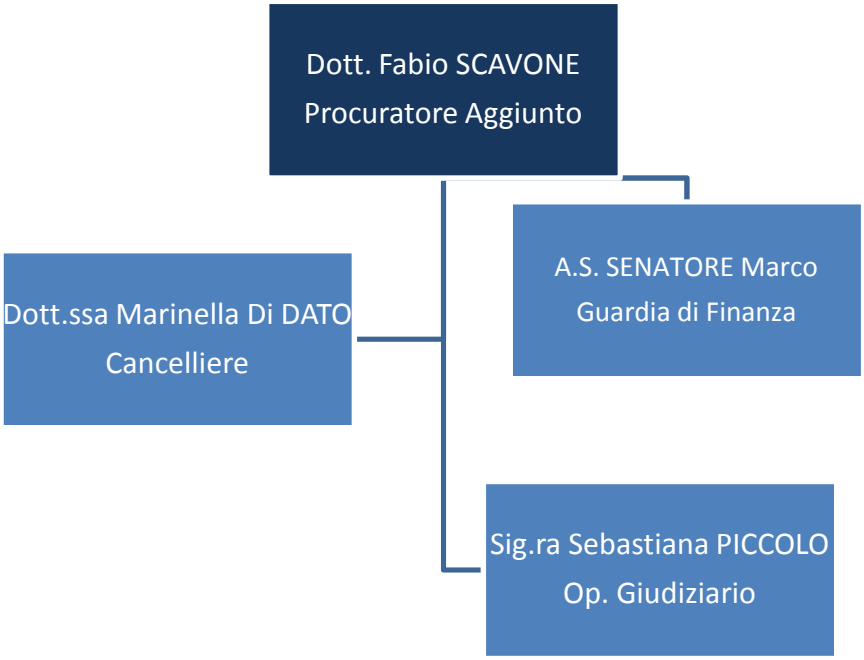
dei magistrati e dell'Ufficio iscrizioni, al Registro Astensioni del Pubblico Ministero e Registro scritti anonimi;

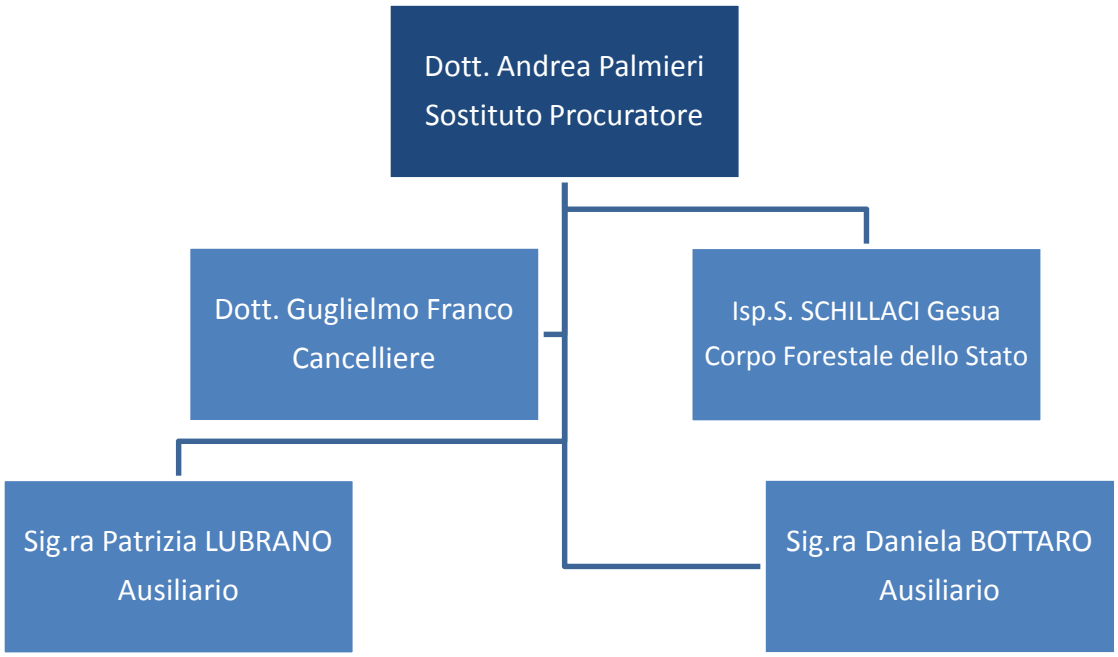
8) Il Cancelliere **Dott.ssa Laura COSENZA**, in ordine allo "Sportello Unico Ricezioni atti e Rilascio Certificazioni" ed Archivio;
9) Il Cancelliere **Dott.ssa Maria Di Dato**, in ordine alla tenuta del Registro Deleghe VPO alle udienze, mod. 25.
10) I Responsabili delle singole Aliquote di polizia giudiziaria componenti della Sezione, in ordine agli affari trattati dai rispettivi uffici per delega o d'iniziativa.

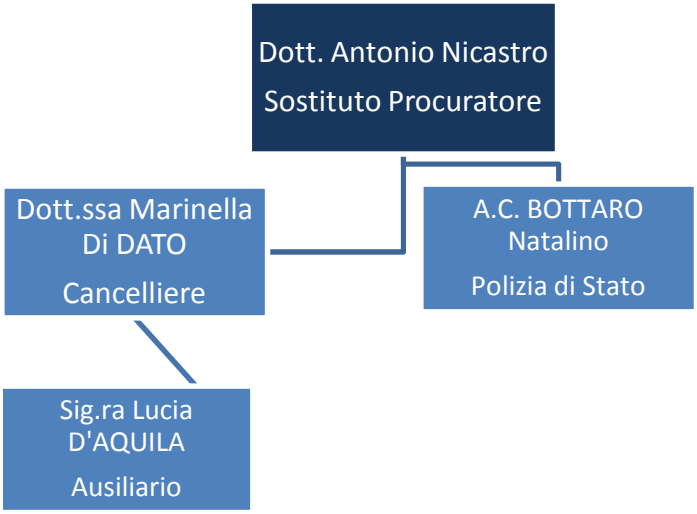
3. Organigramma dell'Ufficio

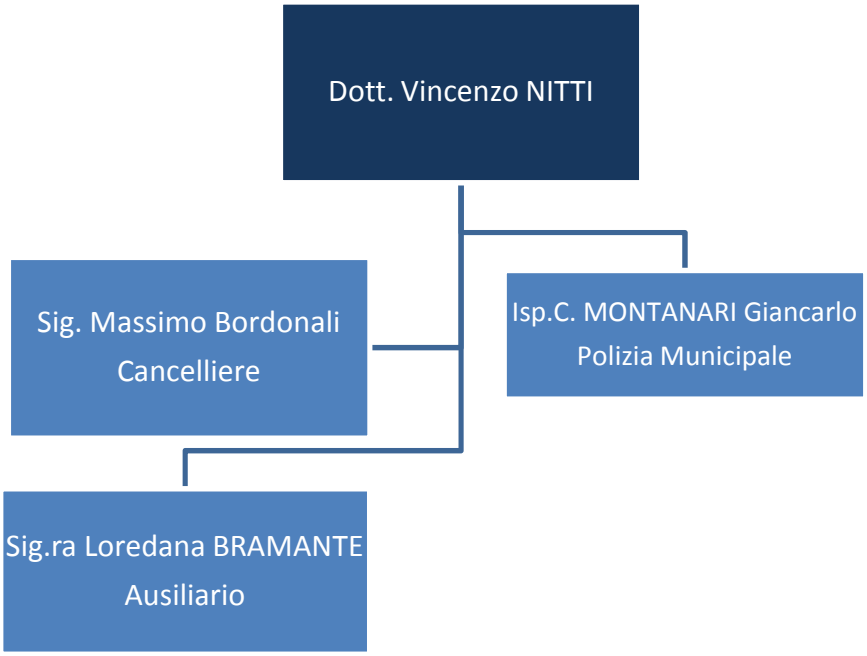
Procuratore della Repubblica - Procuratore Aggiunto

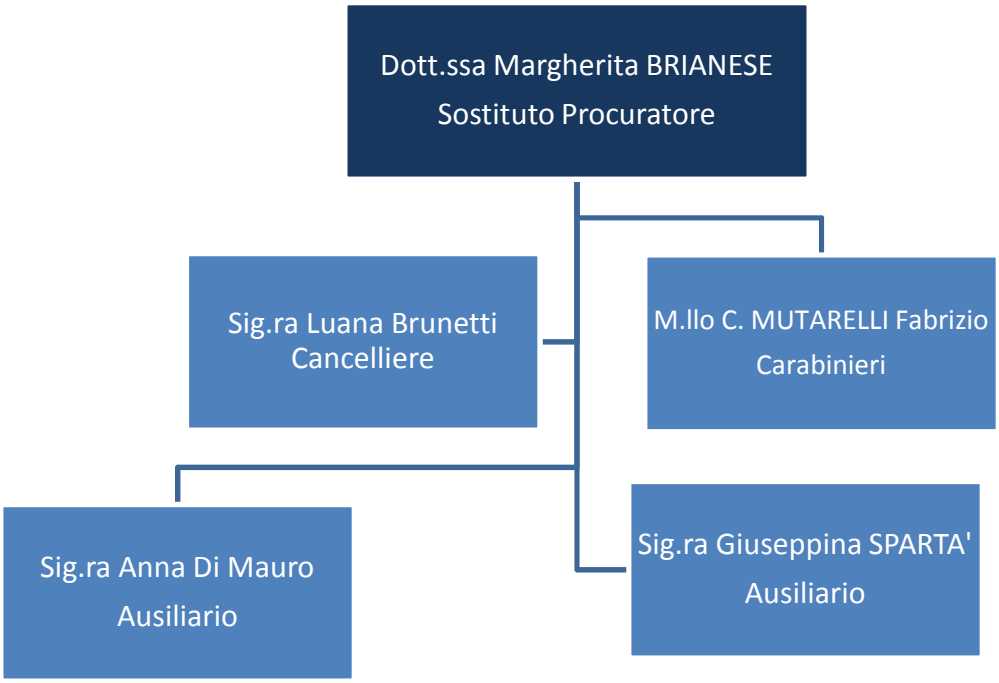
Sostituti Procuratori e relative Segreterie

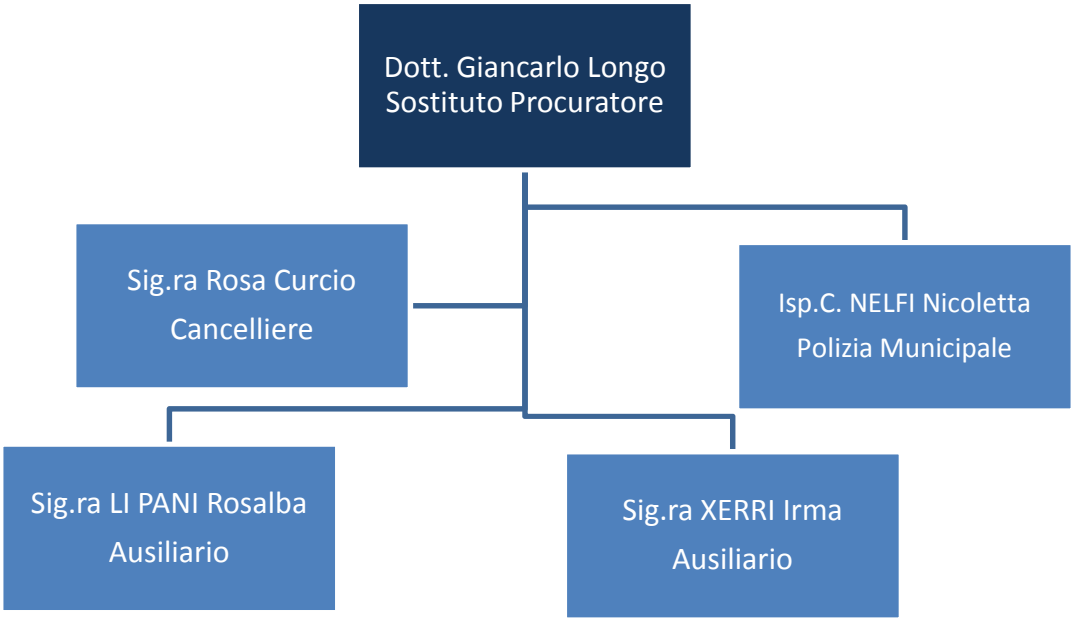

Dott. Fabio SCAVONE
Procuratore Aggiunto
A.S. SENATORE Marco
Guardia di Finanza
Dott.ssa Marinella Di DATO
Cancelliere
Sig.ra Sebastiana PICCOLO
Op. Giudiziario

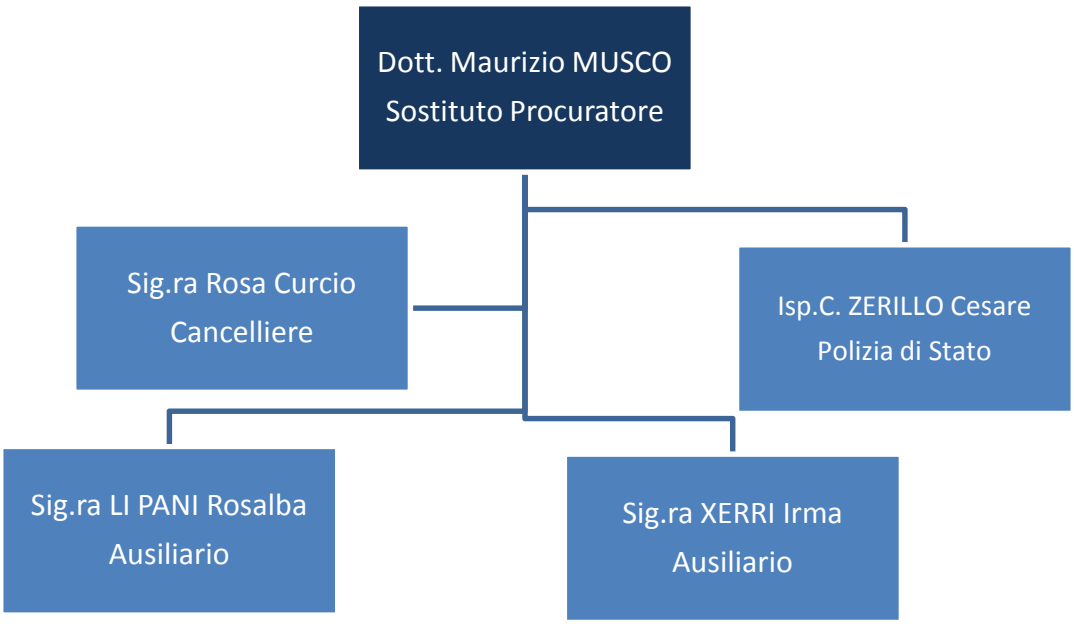

Dott. Andrea Palmieri
Sostituto Procuratore
Dott. Guglielmo Franco
Cancelliere
Isp.S. SCHILLACI Gesua
Corpo Forestale dello Stato
Sig.ra Patrizia LUBRANO
Ausiliario
Sig.ra Daniela BOTTARO
Ausiliario

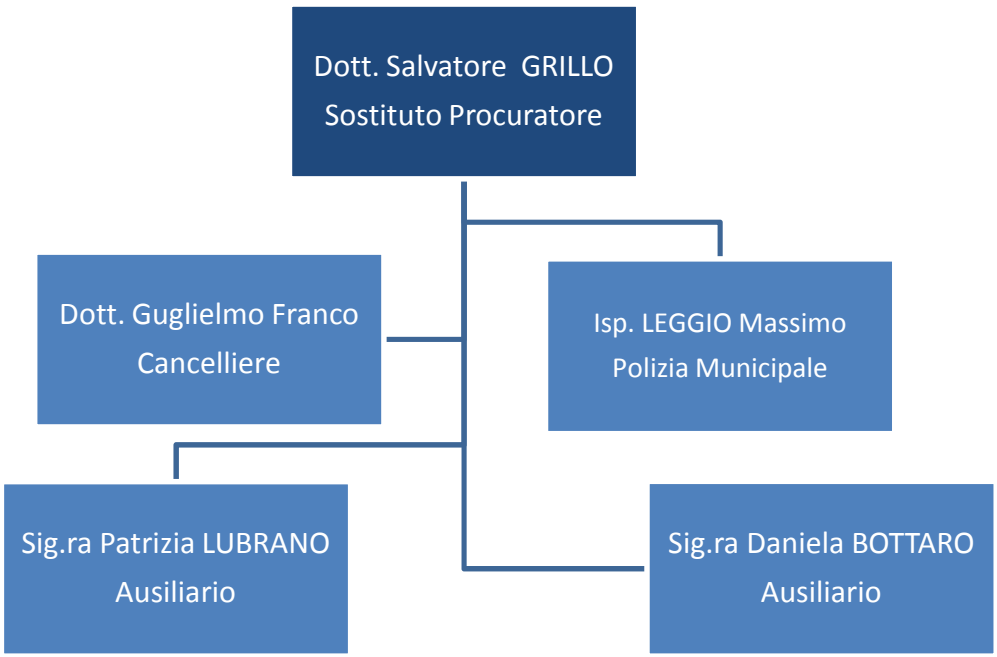

Dott. Antonio Nicastro
Sostituto Procuratore
Dott.ssa Marinella Di DATO
Cancelliere
A.C. BOTTARO Natalino
Polizia di Stato
Sig.ra Lucia D'AQUILA
Ausiliario

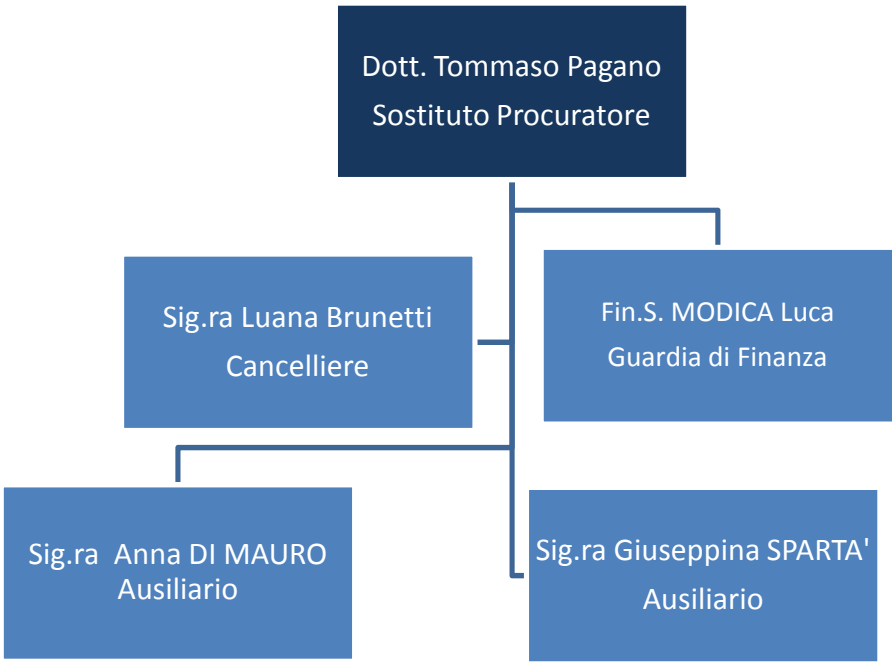

Dott. Vincenzo NITTI
Sig. Massimo Bordonali
Cancelliere
Isp.C. MONTANARI Giancarlo
Polizia Municipale
Sig.ra Loredana BRAMANTE
Ausiliario

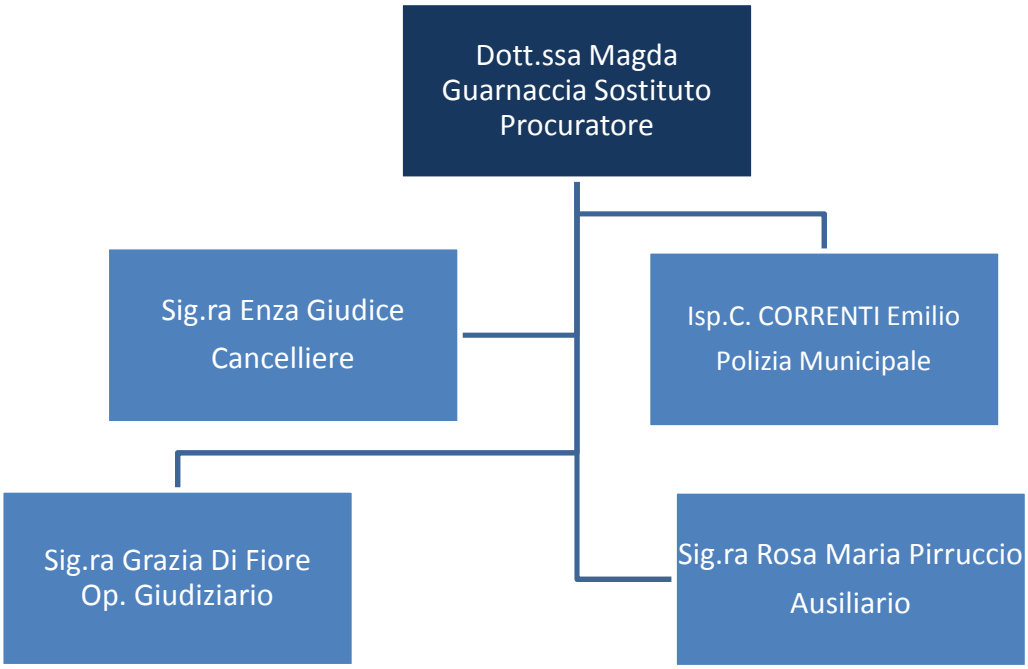

Dott.ssa Margherita BRIANESE
Sostituto Procuratore
Sig.ra Luana Brunetti
Cancelliere
M.llo C. MUTARELLI Fabrizio
Carabinieri
Sig.ra Anna Di Mauro
Ausiliario
Sig.ra Giuseppina SPARTA'
Ausiliario

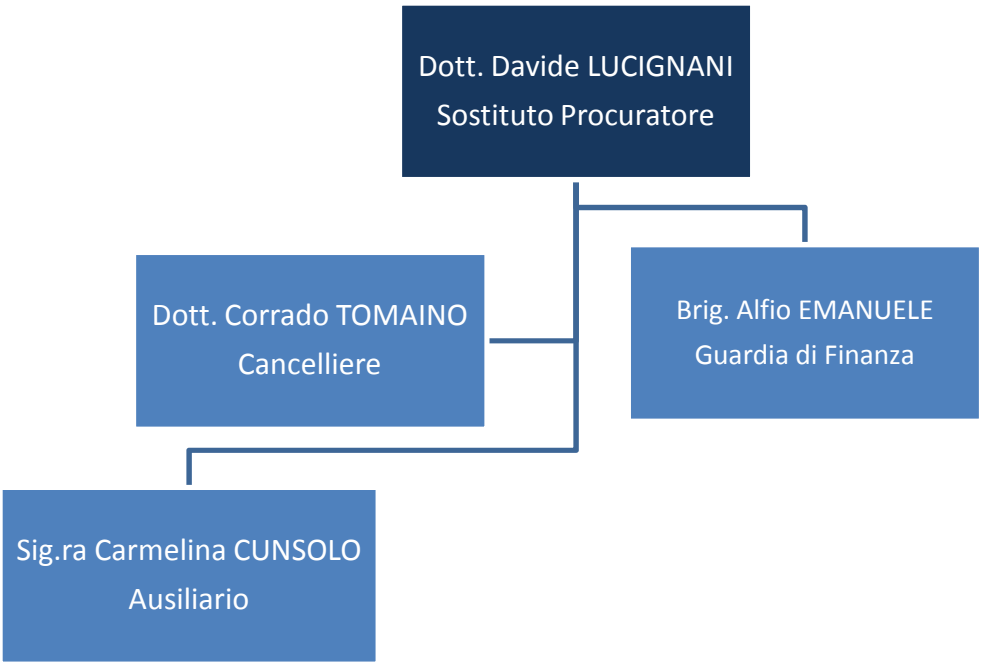

Dott. Giancarlo Longo
Sostituto Procuratore
Sig.ra Rosa Curcio
Cancelliere
Isp.C. NELFI Nicoletta
Polizia Municipale
Sig.ra LI PANI Rosalba
Ausiliario
Sig.ra XERRI Irma
Ausiliario

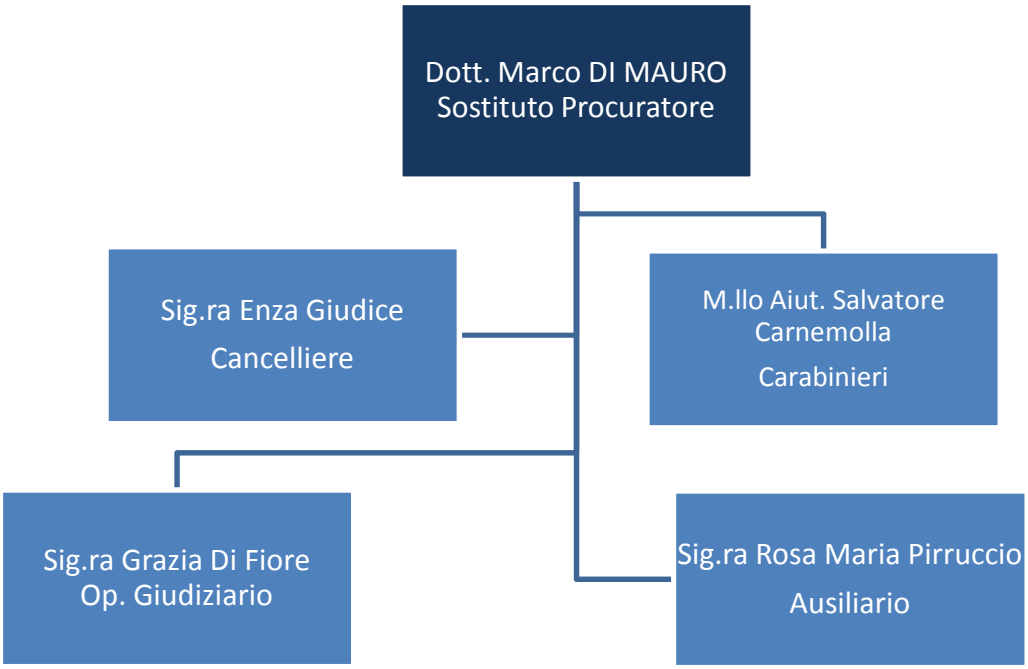

Dott. Maurizio MUSCO
Sostituto Procuratore
Sig.ra Rosa Curcio
Cancelliere
Isp.C. ZERILLO Cesare
Polizia di Stato
Sig.ra LI PANI Rosalba
Ausiliario
Sig.ra XERRI Irma
Ausiliario


Dott. Salvatore GRILLO
Sostituto Procuratore
Dott. Guglielmo Franco
Cancelliere
Isp. LEGGIO Massimo
Polizia Municipale
Sig.ra Patrizia LUBRANO
Ausiliario
Sig.ra Daniela BOTTARO
Ausiliario

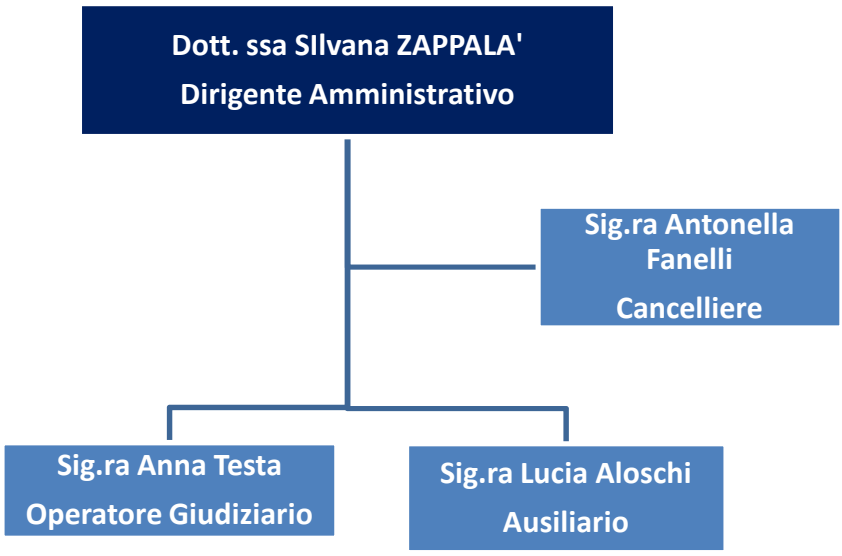

Dott. Tommaso Pagano
Sostituto Procuratore
Sig.ra Luana Brunetti
Cancelliere
Fin.S. MODICA Luca
Guardia di Finanza
Sig.ra Anna DI MAURO
Ausiliario
Sig.ra Giuseppina SPARTA'
Ausiliario


Dott.ssa Magda Guarnaccia Sostituto Procuratore
Sig.ra Enza Giudice
Cancelliere
Isp.C. CORRENTI Emilio
Polizia Municipale
Sig.ra Grazia Di Fiore
Op. Giudiziario
Sig.ra Rosa Maria Pirruccio
Ausiliario

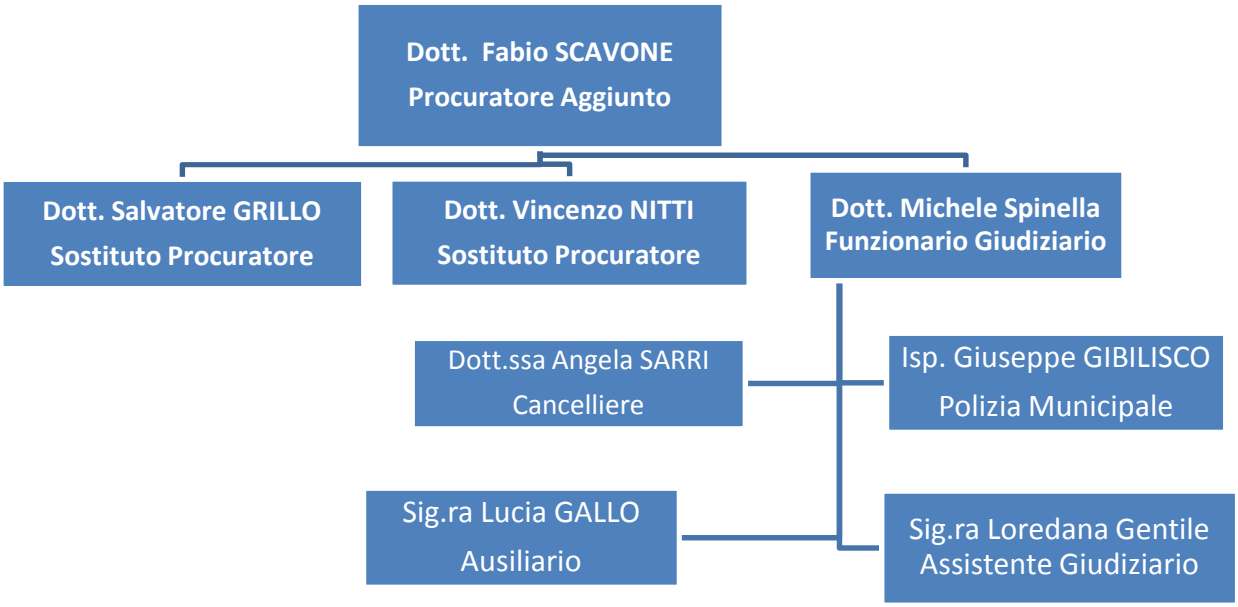

Dott. Davide LUCIGNANI
Sostituto Procuratore
Dott. Corrado TOMAINO
Cancelliere
Brig. Alfio EMANUELE
Guardia di Finanza
Sig.ra Carmelina CUNSOLO
Ausiliario


Dott. Marco DI MAURO
Sostituto Procuratore
Sig.ra Enza Giudice
Cancelliere
M.llo Aiut. Salvatore Carnemolla
Carabinieri
Sig.ra Grazia Di Fiore
Op. Giudiziario
Sig.ra Rosa Maria Pirruccio
Ausiliario

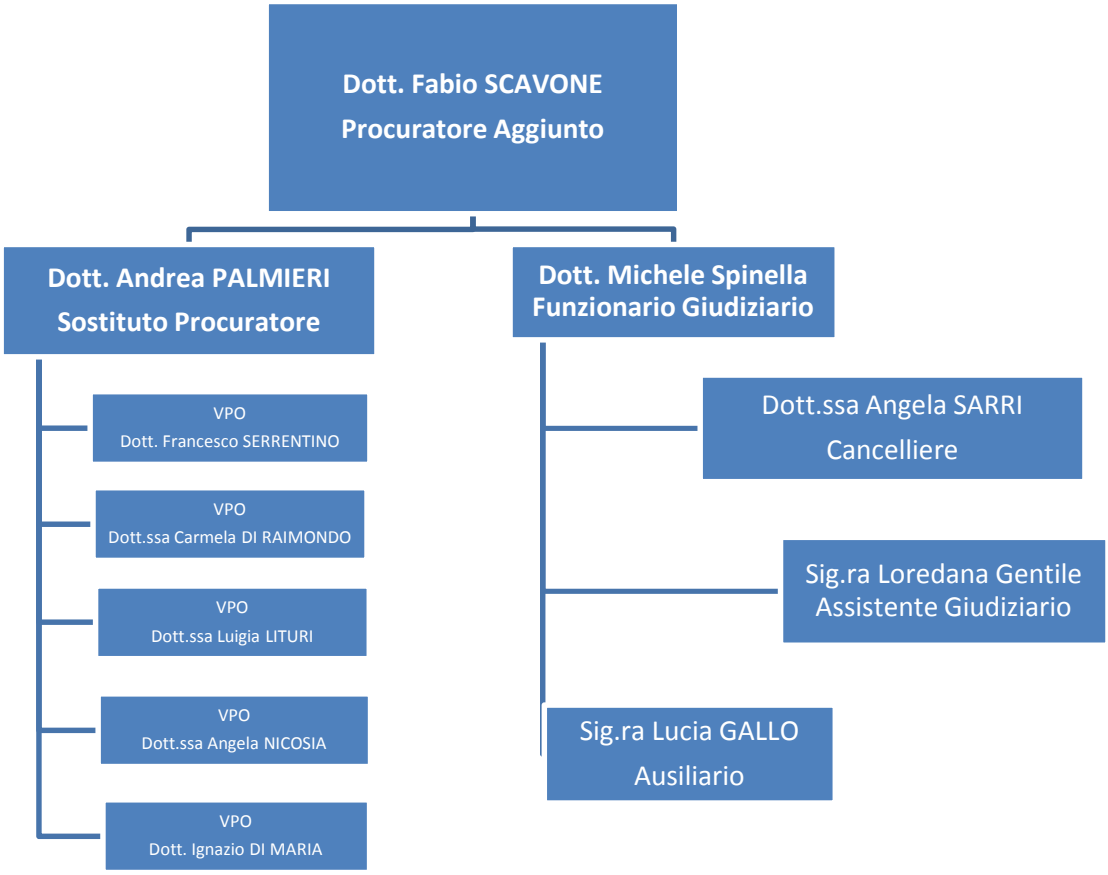
Direzione e Servizi di Segreteria Amministrativa



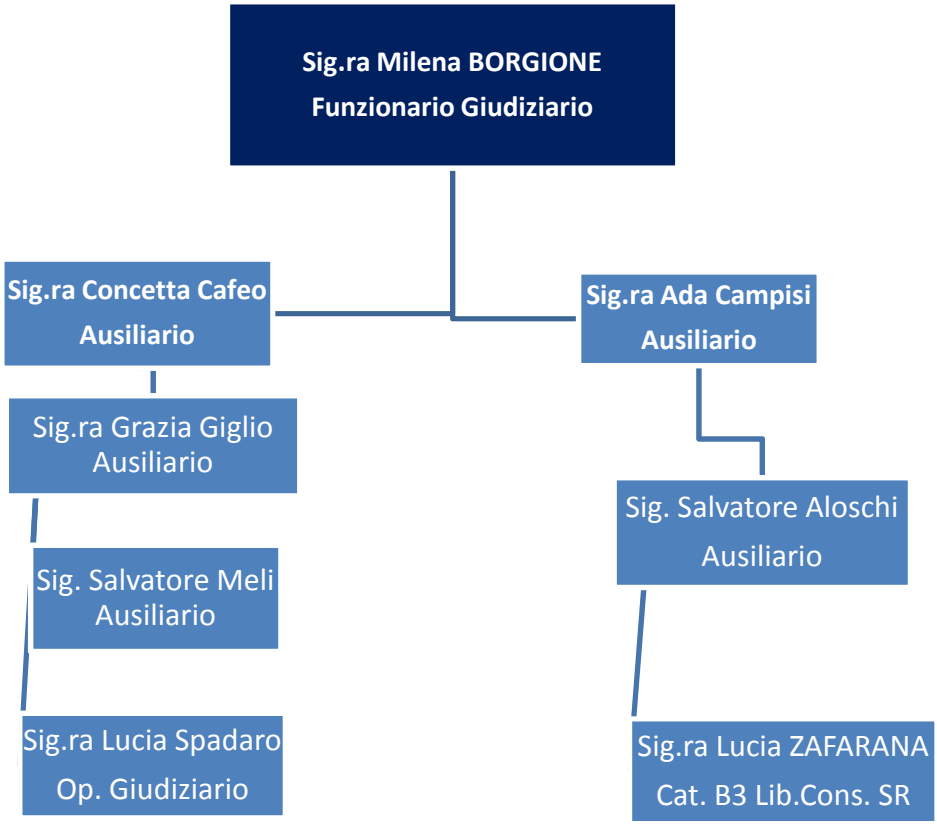
Misure di prevenzione



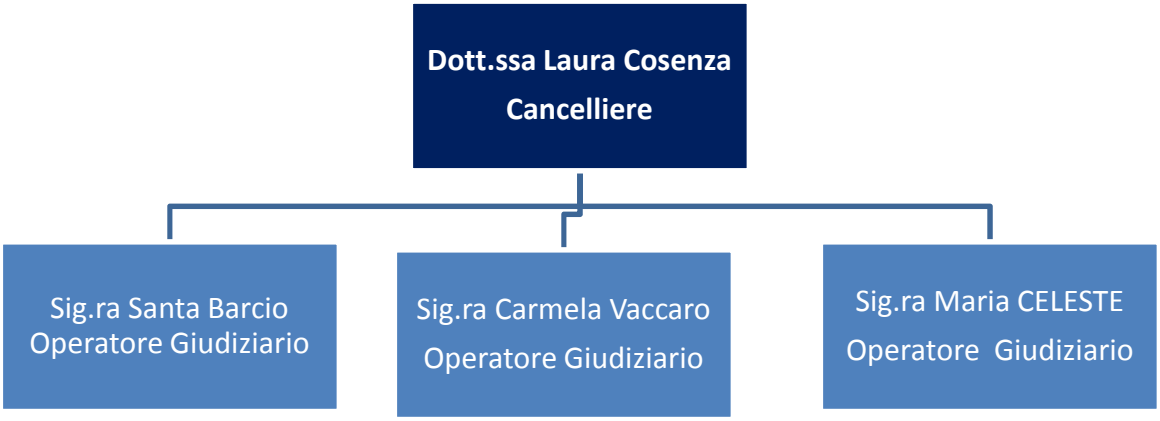
Esecuzione Penale, Misure di Sicurezza ed Esecuzione Demolizioni Opere Edilizie Abusive



Ufficio Iscrizioni

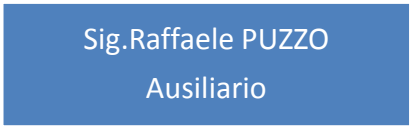


Ufficio Ricezione Atti



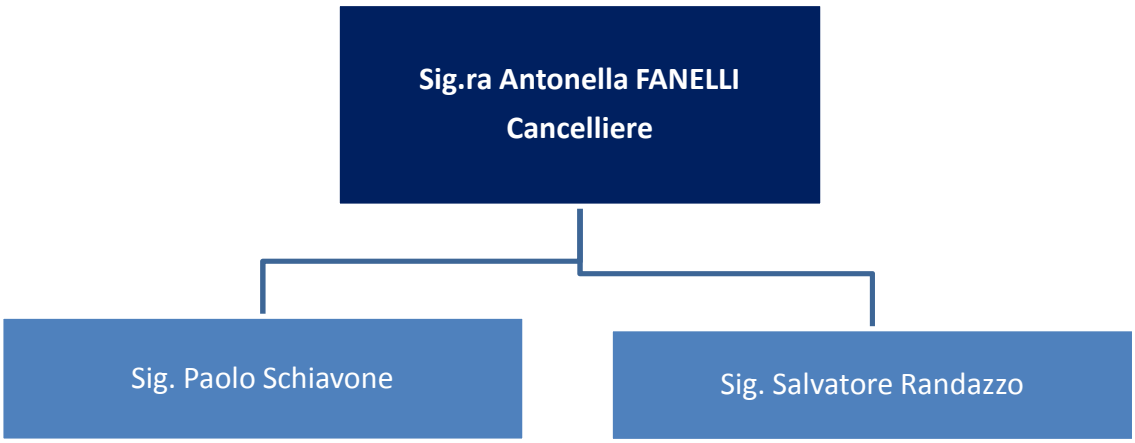
Ufficio Ricezione e Verifica posta ed atti Urgenti

Smistamento e Trasporto Posta e Atti

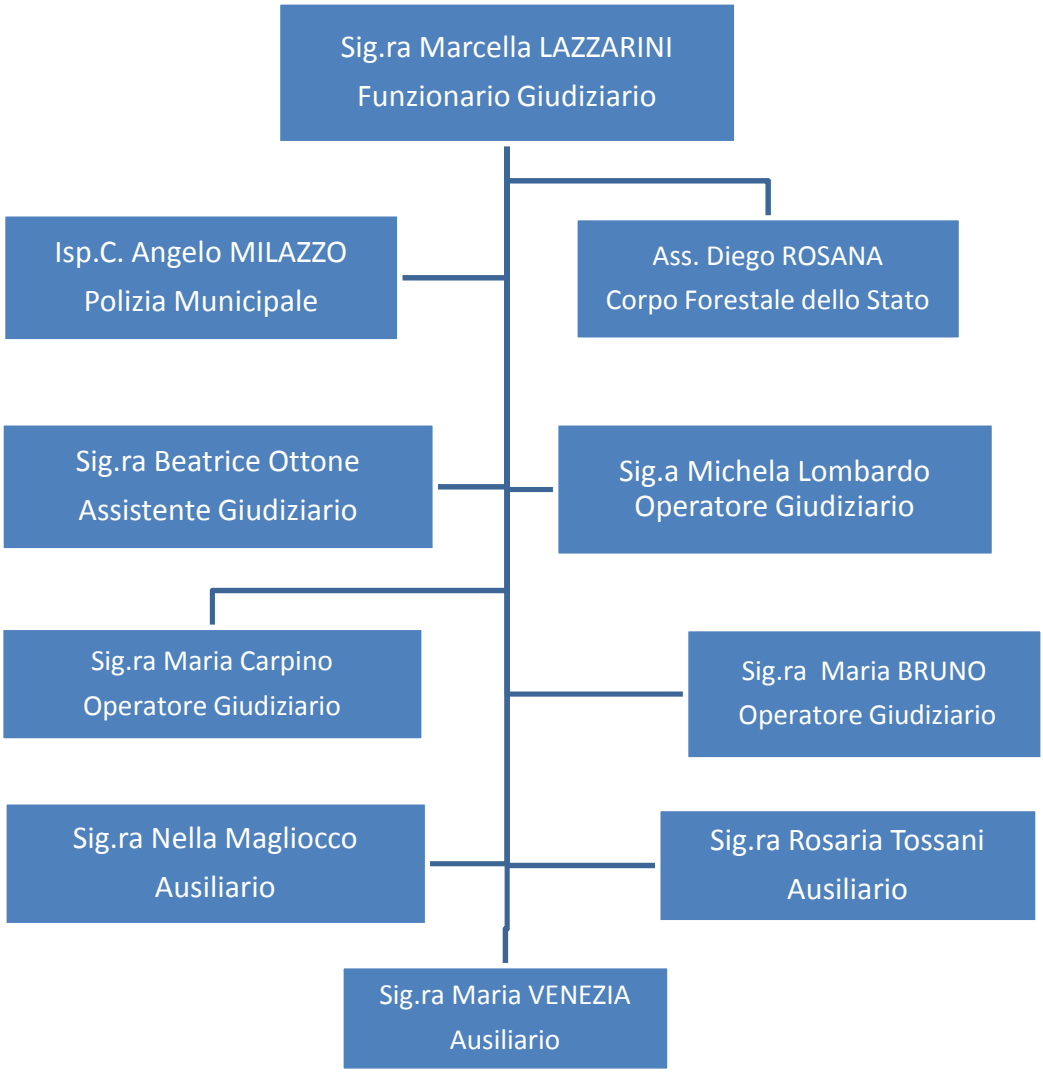


Archivio

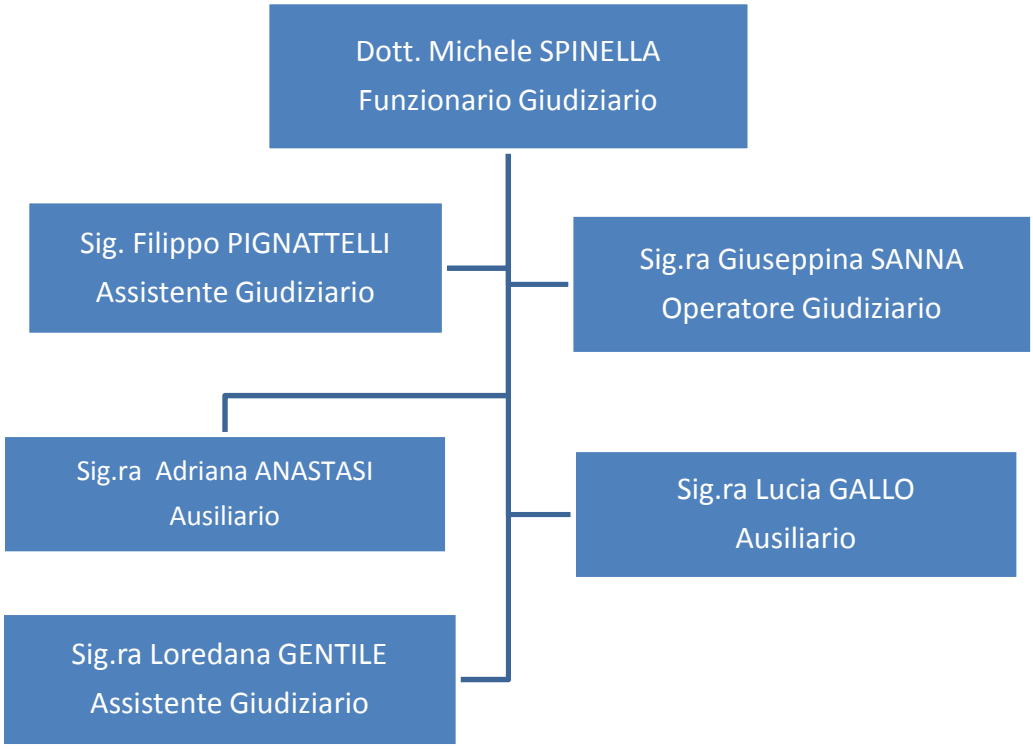
Conducenti autovetture



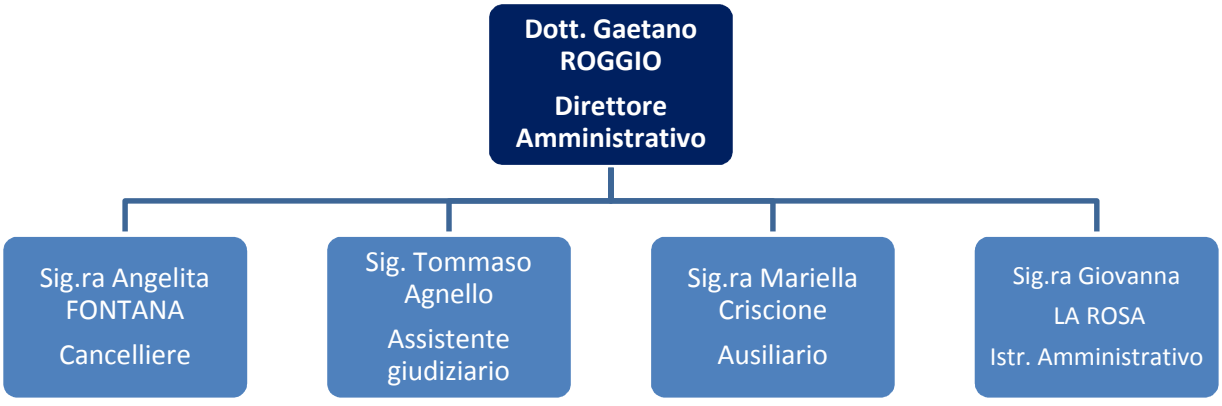
Ufficio Dibattimento



Ufficio del Casellario e U.R.P.

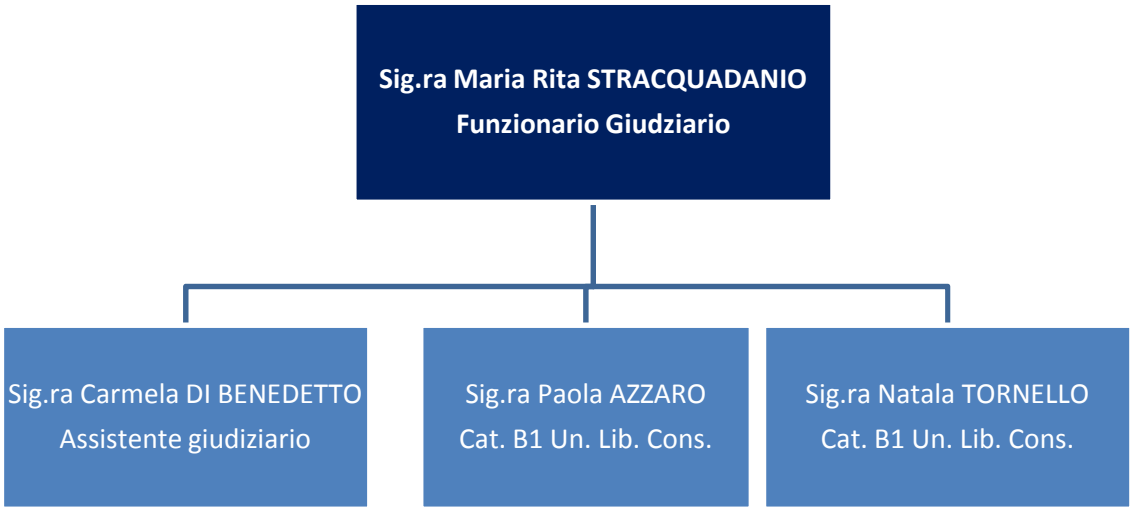


Ufficio Spese di Giustizia

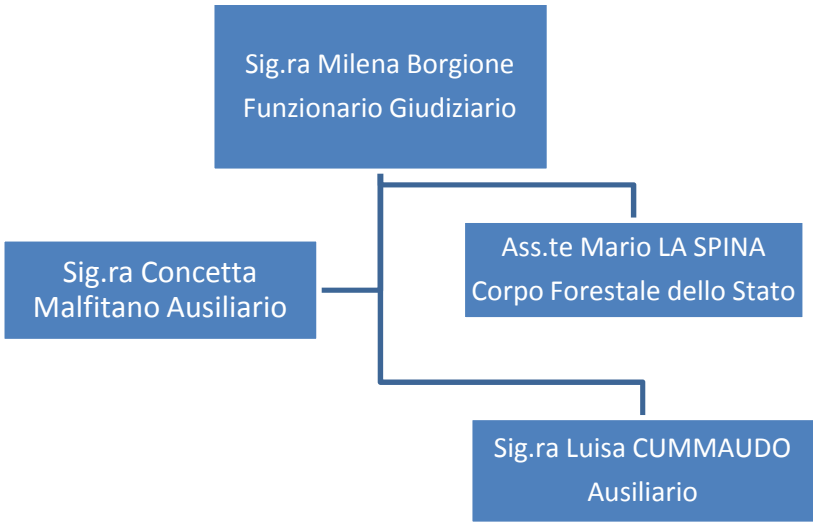


Sezione Civile

Servizio Intercettazioni – C.I.T. – Statistiche– Beni in custodia a terzi



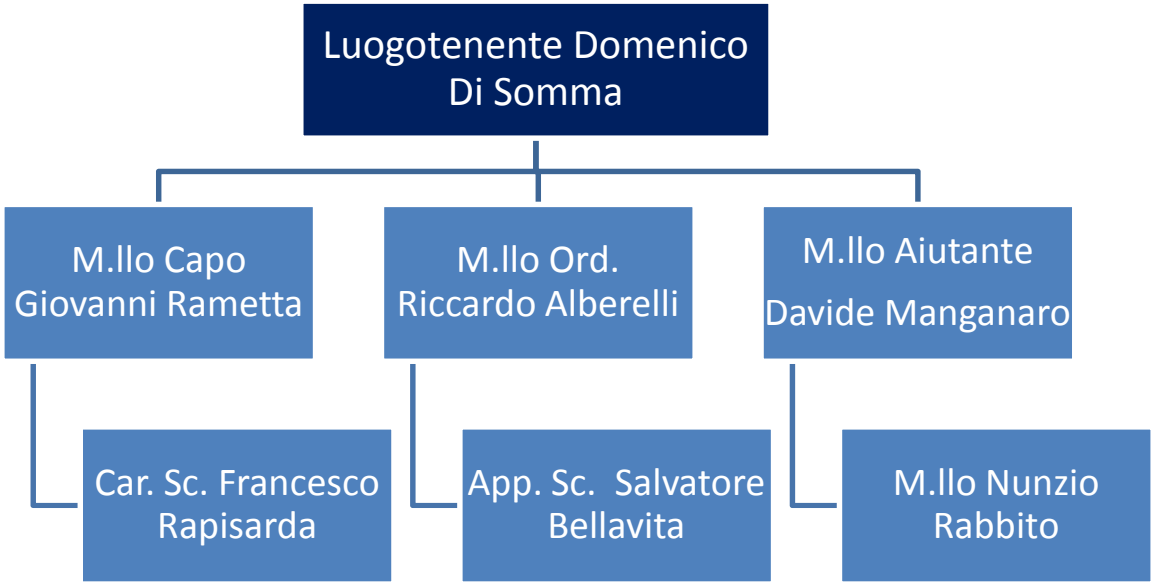
S.I.D.I.P.



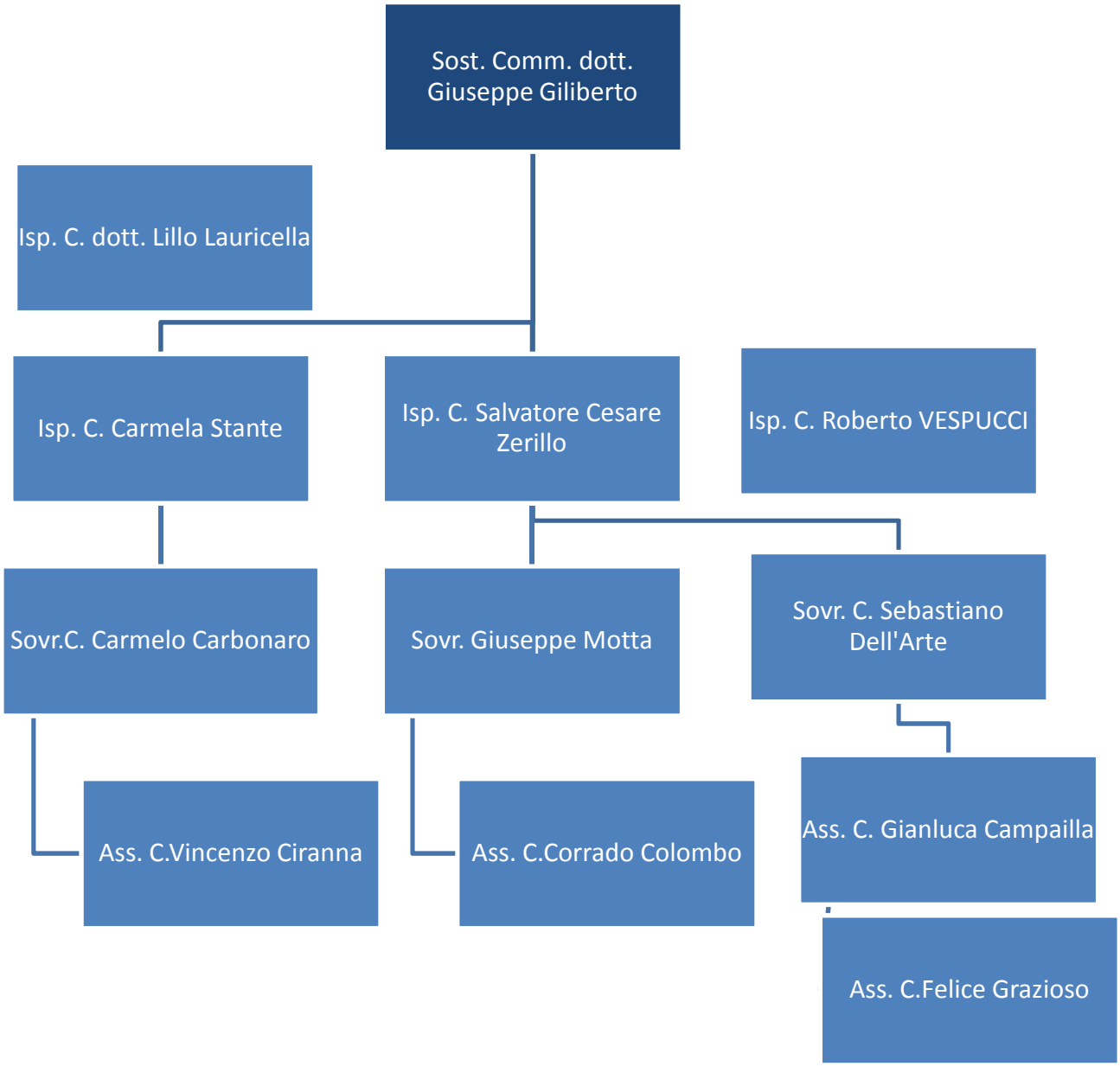
S.D.A.S. –Sezione Definizione Affari Semplici

Sezioni di Polizia Giudiziaria

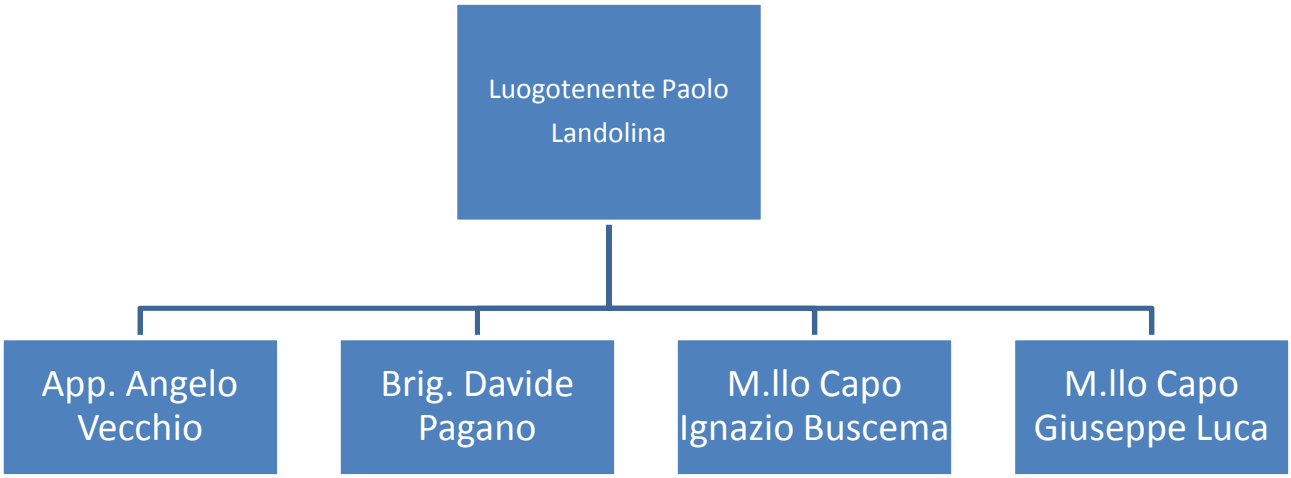
Aliquota Carabinieri



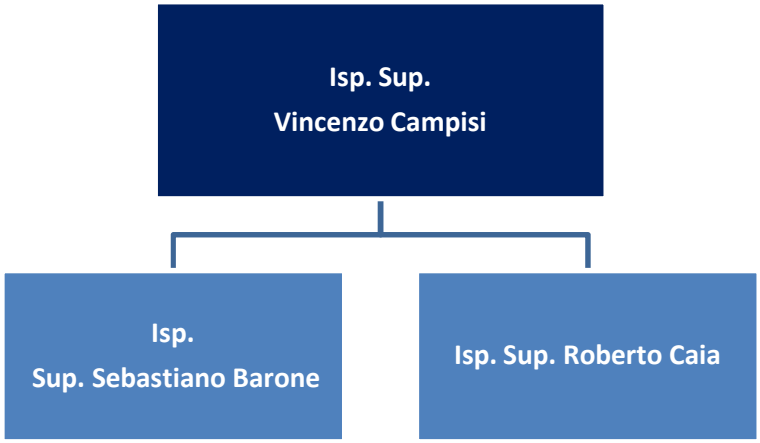
Aliquota Polizia di Stato



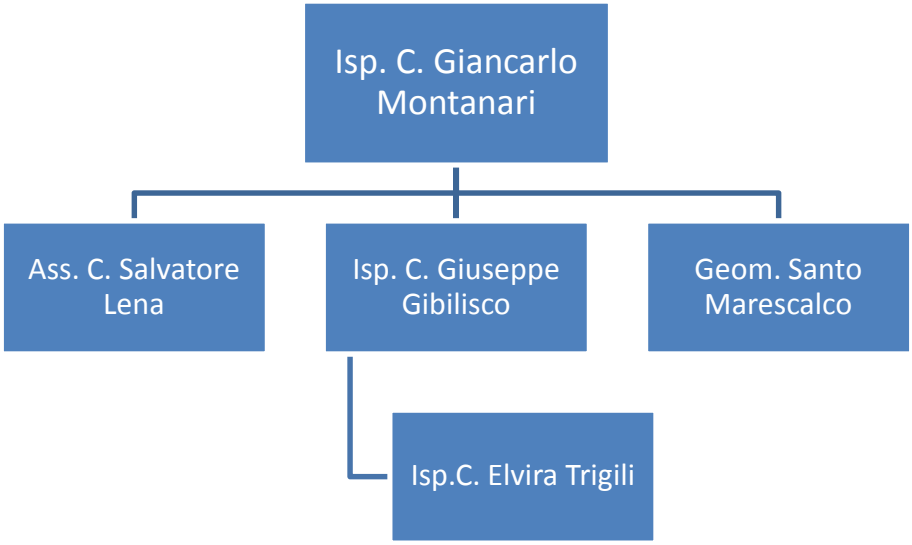
Aliquota Guardia di Finanza



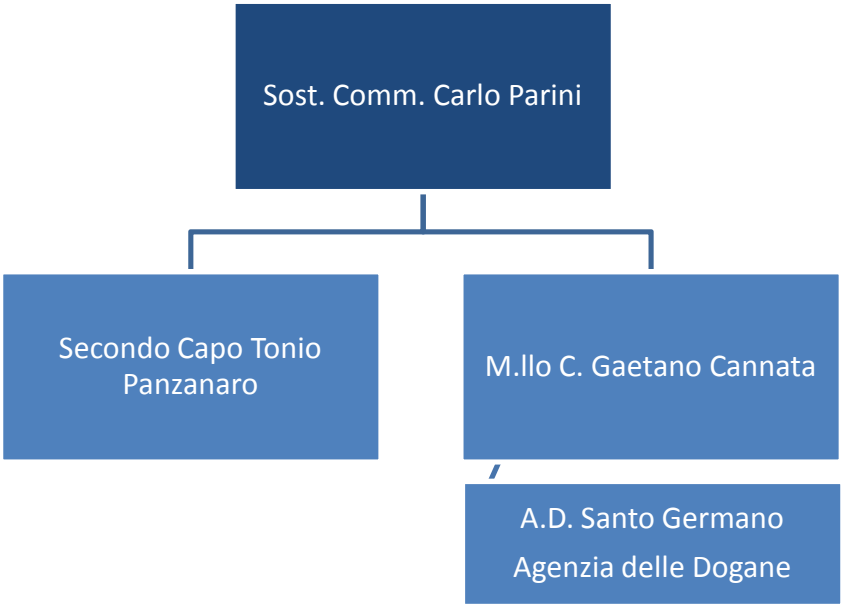
Aliquota Corpo Forestale della Regione



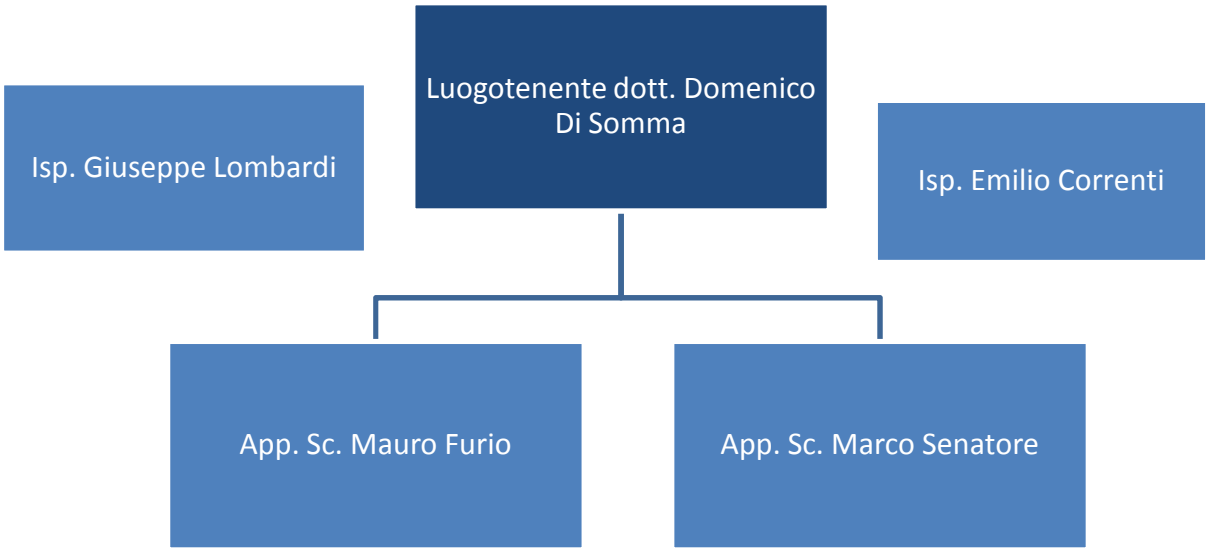
Aliquota Polizia Municipale



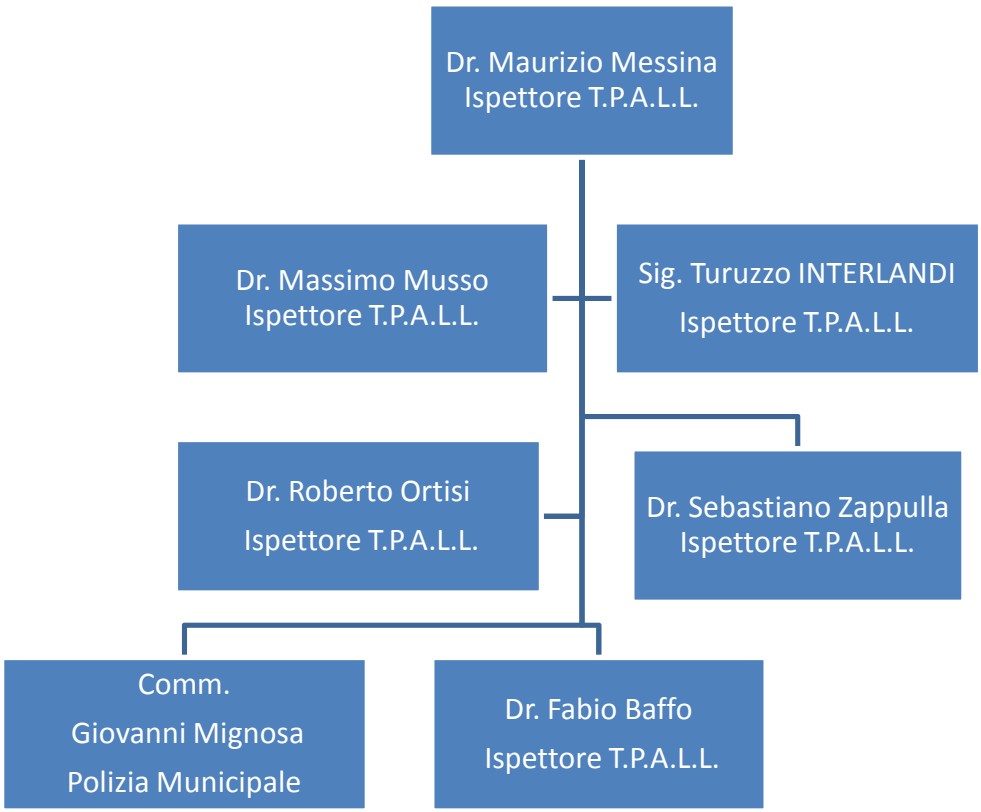
Aliquota Gruppo Interforza Contrasto Immigrazione Clandestina



Nucleo Investigativo Telematico



Aliquota N.I.C.T.A.S



ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

I. Sicurezza dei locali

Considerato che gran parte delle attività istituzionali viene svolta con l'uso dei P.C. e della rete (preparazione dei provvedimenti, elaborati, corrispondenza e consultazione delle banche dati, invio di documenti per via elettronica, etc.), si impone il problema di garantire l'integrità e la disponibilità dei dati, anche con riguardo alla protezione delle aree e dei locali in cui gli strumenti elettronici sono collocati.

Poiché gli apparati elettronici sono installati nei singoli uffici, il primo rischio per la conservazione e la riservatezza dei dati è costituito dalla sicurezza interna ed esterna degli uffici.

Quanto alla sicurezza esterna, gli uffici della Procura sono video sorvegliati e vigilati, per contratto, da agenti privati di vigilanza, che assicurano anche un servizio di ronda. Dal mese di Gennaio 2014, inoltre, è costituito un presidio fisso al piano V° costituito da un agente di polizia o da un carabiniere in orario 8-14 / 14-20 che svolge funzioni di vigilanza per l'accesso degli utenti nei corridoi dell'ufficio quale tutela del Procuratore Capo.

La sicurezza interna degli Uffici che sono regolarmente dotati di dispositivi di chiusura e l'inaccessibilità degli archivi elettronici, durante le momentanee assenze dagli uffici è affidata alla responsabilità del personale, che dispone di adeguati presidi di sicurezza.

La sala server è dotata di porta ignifuga con apertura elettronica a mezzo lettore di badge. Sono autorizzati all'ingresso in detto locale soltanto

l'amministratore di sistema, i tecnici sistemisti ed il dirigente della segreteria.

I rischi che possono incidere sulla sicurezza dei dati sono essere ricompresi in tre categorie essenziali che vanno ricondotte essenzialmente a tre macro categorie:

1) Comportamenti degli operatori;
2) Eventi relativi agli strumenti;
3) Eventi relativi al contesto

Nella tabella sotto indicata sono riassunti i rischi possibili e l'impatto degli stessi sulla sicurezza dei dati.

RISCHI		**SI/NO**	**Descrizione dell'impatto sulla sicurezza (gravità: alta/media/bassa)**
Comportamento degli operatori	Sottrazione di credenziali di autenticazione	NO	======
	Carenza di consapevolezza, disattenzione o incuria	NO	======
	Comportamenti sleali o fraudolenti	NO	======
	Altro evento	NO	=====

RISCHI		SI/NO	Descrizione dell'impatto sulla sicurezza (gravità: alta/media/bassa)
Eventi relativi agli strumenti	Azione di virus informatici o di programmi suscettibili di recare danno	SI	BASSA
	Spamming o tecniche di sabotaggio	SI	BASSA
	Malfunzionamento, indisponibilità o degrado degli strumenti	NO	BASSA
	Accessi esterni non autorizzati	NO	=======
	Intercettazioni di informazione di rete	NO	=======
	Altro evento		

Eventi relativi al contesto	Accessi non autorizzati a locali/reparti ad accesso ristretto	NO	=======
	Sottrazione di strumenti contenenti dati	SI	BASSA
	Eventi distruttivi, naturali ed artificiali nonché dolosi, accidentali o dovuti ad incuria	SI	BASSA
	Guasto ai sistemi complementari (impianto elettrico, climatizzazione ecc.)	SI	BASSA
	Altro evento		=====

Il personale è stato invitato a porre in essere tutti quei comportamenti che evitino ogni possibile pericolo per la sicurezza dei dati, quali uso di dispositivi mobili, pen-drive, hard disk esterni, software non ufficiali.

II. Sicurezza dei documenti

La documentazione cartacea — singoli atti e fascicoli processuali — induce il rischio di violazione del segreto e della riservatezza nel trattamento dei dati, quando la eventuale anomalia della conservazione di documenti, fascicoli e faldoni ne induca la indesiderata ostensione ad estranei. Il personale è stato messo a conoscenza delle misure per elidere il rischio.

Il trasferimento di dati per via informatica, digitale e telefonica è fattore di possibile intrusione e dispersione: appunto per questo l'ufficio è dotato di dispositivi di interdizione e di sicurezza (come l'autenticazione elettronica, la spedizione con posta elettronica certificata e la cifratura). Ciò non esclude che il personale debba adottare ogni doverosa cautela di tipo tradizionale per elidere il rischio di intrusioni: evitando, ad esempio, di attingere o fornire informazioni per telefono. L'uso di internet e della posta elettronica, da parte del personale di magistratura e amministrativo addetto all'ufficio, per quanto di loro competenza, si conforma ai principi e alle regole di cui alla deliberazione 1 marzo 2007, n. 13 dell'Autorità Garante della protezione dei dati personali e alla Direttiva n. 2 del 26 maggio 2009 del Ministro per la P.A. e l'Innovazione.

II trasporto dei fascicoli e lo stazionamento dei carrelli in aree incustodite può indurre danno alla riservatezza nei trattamento dei dati, se non vengono adottate le semplici precauzioni pratiche, in linea di massima già in uso. Non sempre l'ufficio di Procura può governare nel suo insieme l'integrità e la riservatezza dei dati, essendo istituzionalmente previsti,

durante la fase delle indagini preliminari, frequenti trasmissioni di atti all'ufficio del Giudice delle Indagini Preliminare, ufficio dal quale, dunque, dipendono la garanzia della protezione dei dati durante la disponibilità degli atti nel suo ufficio.

MISURE ADOTTATE E DA ADOTTARE

Il trattamento dei dati sensibili e dei dati giudiziari avviene secondo i principi di cui agli artt. 22, 46-47 e 51-52 del d.lgs. 196/2003.
I dati giudiziari vengono trattati e diffusi solo ove autorizzato, consentito o imposto da espressa disposizione di legge e con l'osservanza del provvedimento del Garante del 2 marzo 2011, sulle linee-guida del Garante in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web.

1.1 Trattamenti con strumenti elettronici.

L'ufficio si adegua al disciplinare previsto dagli artt. 33/36 del codice privacy che auspica la completa attuazione del sistema di autenticazione informatica, nonché la dotazione e il periodico aggiornamento degli strumenti elettronici idonei alla protezione dei dati personali contro il rischio di intrusione o di attacco al sistema informatico con programmi diretti a danneggiarne il contenuto (riferimento all'art. 615 *quinquies* C.P.).

Il personale che tratta dati per via elettronica è dotato di password personali di accesso, che vengono periodicamente aggiornate e custodite, in plico nella cassaforte.

E' fatto obbligo a tutti gli incaricati di depositare le password con le modalità di cui sopra.

La custodia delle password in cassaforte ha il fine di consentire la disponibilità dei dati archiviati nel caso di prolungata assenza o impedimento dell'incaricato.

La chiave della cassaforte è custodita dal dirigente della segreteria. I plichi contenenti le password possono essere aperti soltanto dal titolare o, in caso di sua prolungata assenza o impedimento, dal dirigente quando sia necessario e indifferibile intervenire per esclusive necessità di servizio.

In tal caso il dirigente informerà tempestivamente l'interessato dell'intervento effettuato, con invito ad aggiornare la password al rientro in servizio o alla cessazione dell'impedimento.

Durante le sessioni di trattamento è vietato agli incaricati di lasciare incustodito e accessibile lo strumento elettronico.

L'infrazione comporterà assunzione diretta di responsabilità al verificarsi di eventuali danni dipendenti dall'infrazione stessa.

L’accesso al sistema S.I.C.P. è invece gestito sul Dominio Nazionale Utenti. Ogni utente è tenuto a modificare la propria password di accesso periodicamente ed al massimo ogni sei mesi (così come imposto dal sistema).

Ferme restando le procedure di continuità e di salvataggio previste per i sistemi RE.GE., S.I.C.P., SIES, SIEP, SIPPI., SIAMM, e PROTEUS PA

(protocollo informatico), gli incaricati debbono, con frequenza almeno settimanale, inserire i documenti che ritengono importanti nella cartella personale (Home directory) collegata al server.

Il server esegue automaticamente (ogni notte) il backup delle cartelle personali .

Per ragioni di economia è consigliabile versare nelle cartelle personali presenti sul server solo i dati di effettivo interesse, da salvare, eliminando gli altri con le ordinarie procedure.

Analoga precauzione deve essere adottata per la custodia dei supporti removibili (floppy, CD, DVD, pen disk) e dei computer portatili.

Per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento, nella attuale mancanza di specifiche disposizioni al riguardo, potrà essere interessato CISIA per ogni utile intervento, volto alla canalizzazione e alla evasione delle richieste in tempi brevi (di regola non superiori a sette giorni), con interventi preferibilmente all'interno della struttura.

I supporti removibili contenenti dati sensibili e giudiziari, se non utilizzati, sono distrutti o resi inutilizzabili; possono essere riutilizzati da altri incaricati solo quando i dati memorizzati siano resi non intellegibili e non ricostruibili.

In caso di consegna, a qualsiasi titolo, di supporti informatici removibili contenenti dati giudiziari segreti, l’autore del supporto o del file avrà cura di inserire o di far inserire sistemi di protezione mediante password all’apertura del file, e comunque ogni rigorosa cautela atta a garantire la

riservatezza delle informazioni e ad impedire qualunque forma di circolazione illegittima, anche limitata.

In caso di conferimento a terzi di incarichi comportanti trattamento di dati personali e dati sensibili all'esterno della Procura per ragioni di giustizia (consulenze tecniche, impiego di ausiliari e simili incarichi) sarà fatto constatare nel provvedimento di conferimento del terzo incaricato di restituire, dopo l'espletamento dell'incarico, tutto il materiale consegnatogli, gli elaborati e il eventuali copie, nonché l'obbligo di distruggere o rendere comunque o non intelligibili e non ricostruibili i documenti. i supporti elettronici usati e quant'altro sia stato creato, anche su cartaceo, in occasione del lavoro svolto, sia che nell'archivio del terzo incaricato, nulla rimanga di quanto trattato.

L'Amministratore del sito WEB dell'ufficio è tenuto ad adottare tutte le misure idonee a garantire la tutela e la protezione dei dati personali sulla rete.

La Sezione e i Servizi di polizia giudiziaria, ai quali per ragioni di giustizia vengano delegati accertamenti e indagini comportanti trattamento di dati, sono tenuti ad adottare analoghe misure minime di sicurezza per la protezione dei dati personali.

1.2. Trattamenti senza l'ausilio di strumenti elettronici

La custodia e conservazione dei fascicoli e di singoli documenti si conforma, oltre che alle norme processuali e regolamentari, al criterio della protezione dei dati personali.

Atti e fascicoli processuali, pertanto, vanno custoditi in appositi armadi chiusi a chiave e in modo tale da non consentire, alla occasionale ispezione visiva di estranei, la rilevazione di dati personali.

Quando adagiati sui tavoli per studio o consultazione, la parte anteriore delle copertine dei fascicoli che ne indicano gli estremi non deve essere visibile.

II trasferimento dei fascicoli deve avvenire mediante carrelli coperti, che non debbono sostare incustoditi nei corridoi.

Nel caso di momentanea assenza del personale dagli uffici, i P.C. dovranno essere resi temporaneamente inaccessibili e gli uffici dovranno rimanere sotto costante controllo, anche mediante chiusura a chiave.

I fascicoli personali debbono essere custoditi in armadi chiusi a chiave e con ante non trasparenti.

Analoga precauzione è da adottare per la conservazione degli atti riguardanti notai, revisori di conti, vice procuratore onorari, componenti della sezione di polizia giudiziaria.

Le cartelle sanitarie relative alla normativa prevista dall' artt. 41 del D. Lgs. 81/2008 e succ. mod. sono custodite in cassaforte.

La fotoriproduzione deve essere eseguita al riparo dal rischio di violazione della riservatezza.

Massime e provvedimenti giurisdizionali estratti per fini di consultazione o per essere utilizzati come precedenti giurisprudenziali non debbono recare i nomi delle parti.

2.Intercettazioni telefoniche e ambientali.

Si premette che l'attività intercettiva telefonica e ambientale svolta dai magistrati, come pure l'acquisizione dei tabulati del traffico telefonico, non hanno mai dato luogo, per quanto consti, ad inconvenienti di sorta in ordine alla protezione dei dati personali, in quanto le procedure di acquisizione, conservazione e deposito dei dati sono state svolte con l'osservanza del segreto e delle cautele imposte dalla legge; non sono state lamentate fughe e indebite propalazioni di notizie.

La trasmissione ai fornitori delle comunicazioni relative a decreti di intercettazione e di acquisizione di tabulati è avvenuta con l'impiego dei tradizionali canali: di norma, mediante consegna brevi manu degli atti alla P.G.; rare volte e in casi di necessità, mediante spedizione per posta o trasmissione per fax e in mancanza di presidi tecnici di sicurezza tecnologicamente evoluti.

II 25 settembre 2006 il Garante per la protezione dei dati personali, nel rammentare che i fornitori di servizi di comunicazione elettronica hanno l'obbligo di proteggere adeguatamente i dati personali trattati allorché adempiono provvedimenti dell'autorità giudiziaria in materia di intercettazioni telefoniche e telematiche, ha evidenziato che analoghe cautele debbono essere adottate presso gli uffici giudiziari. Ha auspicato la urgente attuazione di ogni opportuna iniziativa del Ministero, del CSM e degli uffici giudiziari per salvaguardare la sicurezza "di delicati dati e sistemi", violati a seguito di gravissimi episodi delittuosi che preoccupano l'intera collettività.

Con nota del 21.12.2006 la Telecom Italia ha reso noto il protocollo adottato per la sicurezza del dati presso i gestori delle intercettazioni.

In ossequio a quanto disposto con circolare del 14.12.2006, n. 451740, del Ministero - Dipartimento dell'Organizzazione Giudiziaria - questo Ufficio ha attivato la PEC per il Procuratore della Repubblica e il Dirigente della Segreteria, adeguandosi alle prescrizioni del Garante. Altre caselle di PEC sono disponibili per gli usi di ufficio, in particolare per le notifiche con mezzi idonei dei decreti di conclusione indagini ai difensori.

Si è, inoltre, provveduto ad allestire una area riservata con accesso riservato e autonomo sistema di video-sorveglianza, un locale ove sono concentrate le attrezzature elettroniche e ove vengono svolte da parte del personale di polizia giudiziaria le attività di intercettazione.

Il locale è munito di due telecamere ad infrarossi: una monitora l'ingresso primario della porta blindata di accesso; la seconda monitora la porta di ingresso della sala server, con registrazione h 24 su apposito sistema DVR

L'accesso ai sistemi di intercettazione è consentito solo da postazioni preventivamente abilitate e censite, connesse a reti dotate di sistemi di protezione. Tale architettura di sistema non consente ai computer che non siano preventivamente censiti dall' amministratore di sistema di accedere alla rete.

Utilizzando un' autenticazione KERBEROS, l'accesso è consentito, sia per scopi di configurazione delle intercettazioni che per ascolto o riascolto solo ad operatori autenticati tramite KERBEROS, qualunque sia

la modalità, locale o remota, con cui venga realizzato l'accesso. Ogni accesso al sistema è sempre registrato.

In ottemperanza alle disposizioni del garante della Privacy (provvedimenti 27/11/08 e 25/06/09), ogni accesso al sistema amministratore sarà debitamente registrato in apposito data base.

I collegamenti telematici tra la Procura della Repubblica ed uffici di Polizia Giudiziaria esterni sono effettuati tramite connessioni "punto-punto", per mezzo di ponti wi-fi ottenuti tramite VPN (Virtual Private Lan) che inibiscono l'accesso a sistemi non autorizzati.

Tutte le operazioni di accesso sono "loggate", con annotazione in registri informatici, con tecniche che ne assicurano la inalterabilità, previa indicazione dei riferimenti temporali relativi alle attività svolte e al personale operante, dell'esecuzione delle operazioni (quali l'ascolto, la consultazione, registrazione, masterizzazione, archiviazione e duplicazione delle informazioni, trascrizione delle intercettazioni, la manutenzione e la gestione dei sistemi, la distruzione dei supporti, dei verbali, delle registrazioni, e di ogni altra documentazione attinente alle intercettazioni) effettuate nell'ambito delle attività di intercettazione sia presso gli uffici Centrali sia presso gli uffici della Polizia Giudiziaria delegata alle indagini .

E' garantita la conservazione in forma cifrata delle eventuali copie di sicurezza dei dati allo stesso modo di quanto previsto per i dati online; ogni estrazione di dati, anche parziale, su qualsiasi tipo di supporto removibile deve essere assistita da procedure crittografiche per la

protezione dei contenuti. E' parimenti assicurata la conservazione in forma cifrata, indipendentemente dal formato di registrazione, delle tracce foniche e delle altre informazioni, in modo da impedirne l'ascolto o la intelligibilità a soggetti non legittimati anche in caso di acquisizione fortuita o a seguito di guasti o interventi manutentivi sulle apparecchiature informatiche. Eventuali file esportati saranno protetti con algoritmo (MD5) o similare, con chiave di protezione. La password per decriptare i file sarà assegnata per singola utenza intercettata e per procedimento penale. Ogni intercettazione sarà identificata esclusivamente dal RIT, senza riferimento al nominativo dell'intercettato ed all'utenza monitorata.

E' stato creato un archivio riservato per la conservazione dei supporti informatici. E' stata istituita apposita Segreteria R.i.t., assegnando il servizio ad un funzionario giudiziario. Sin dal 4.11.2013, il procuratore capo ha incaricato il magistrato referente per le intercettazioni e la società di servizi GR Sistemi di monitorare la situazione e di introdurre i necessari accorgimenti per adeguare tutta la struttura ai provvedimenti del Garante, adeguamento che è stato completato.

Le bobine di registrazione magnetica delle intercettazioni sono conservate in armadi metallici regolarmente chiusi a chiave.

E' stato nominato il sostituto procuratore della Repubblica dott. Nicastro quale referente delle Intercettazioni.

Il funzionario giudiziario Sig.ra Maria Rita Stracquadanio è stata nominata Responsabile del C.I.T., mentre il Direttore Aministrativo dott. Gaetano Roggio, provvede alla liquidazione delle fatture.

Al medesimo funzionario sig.ra Stracquadanio, pertanto, compete la direzione e responsabilità del servizio, inoltre la stessa cura i rapporti con le forze di PG, realizzando in tal modo il controllo complessivo di tutto il servizio e, laddove necessario ed opportuno, ha la possibilità di facilmente intervenire.

Al dott. Roggio è stato affidato anche il compito di procedere al riscontro contabile, alla liquidazione delle fatture e alla predisposizione dei mandati di pagamento, in relazione a tutte le operazioni tecniche svolte ed inerenti al servizio.

La suddetta ditta ha altresì fornito anche apposito **software gestionale del Mod.37** che, nel rispetto del segreto e dell'autonomia di ciascun magistrato, consente autonomamente a ciascun PM l'emissione e registrazione dei provvedimenti di intercettazione che, comunque, vengono supervisionati dal Procuratore Capo. Il mod.37 in versione informatica viene gestito dal Funzionario responsabile del CIT, cui compete anche la tenuta del modello cartaceo Mod. 37 ancora utilizzato, così come indicato dalla D.G.S.I.A. con nota del 24.09.2015 .

Il citato registro informatico consente non solo un controllo immediato delle varie attività di intercettazione espletate ed in corso ma anche un controllo contabile - in tempo reale - e l'emissione abbastanza precisa - e sempre in tempo reale – della relativa statistica sia nel formato richiesto a livello ministeriale che, a richiesta del Procuratore Capo, delle varie tipologie di servizio.

3.Certificati e certificazioni amministrative e penali.

Il conferimento dei dati personali richiesti in moduli o anche su supporti cartacei in banco, se è obbligatorio per la trattazione della formalità di rilascio dei certificati, dev'essere circondato da ogni cautela per garantire con ogni mezzo il trattamento dei dati secondo metodologie conformi alla legge primaria e ai provvedimenti del garante. I dati saranno raccolti e trattati dalla Procura della Repubblica di Siracusa, dal funzionario responsabile di area e dagli operatori esclusivamente per le finalità inerenti al rilascio delle certificazioni. I diritti di accesso ai dati medesimi e di rettifica, aggiornamento, cancellazione dei dati erronei, incompleti o raccolti con modalità non conformi alla legge, nonché il diritto di opporsi al loro trattamento per motivi illegittimi può essere esercitato mediante comunicazione scritta alla Procura della Repubblica di Siracusa in conformità alle previsioni di legge, in particolare al disposto di cui agli artt. 7-10 d.lgs. n. 196 del 2003.

Nella materia delle certificazioni, l'Autorità Garante ha, peraltro, ribadito che restano fermi, in quanto applicabili anche a tali attività, i princìpi posti dall'art. 11 del Codice, in base ai quali l'accesso ai dati personali può essere consentito solo previa verifica dell'esistenza di uno scopo determinato, esplicito e legittimo (comma 1, lett. b)) e relativamente alle sole informazioni pertinenti e non eccedenti rispetto allo scopo medesimo (comma 1, lett. d)), sollecitando quindi le autorità giudiziarie a valutare attentamente la possibilità di omettere informazioni atte a consentire l'identificazione dei soggetti coinvolti nei giudizi, ove ciò non sia

strettamente necessario al perseguimento delle finalità perseguite dai richiedenti (note 5 e 21 gennaio 2011).

4. Scarto degli atti.

Si è proceduto ad incaricare un Funzionario Giudiziario, d'intesa con lo scrivente, e nelle more del rinnovo della Commissione di sorveglianza degli archivi, di elaborare i criteri generali cui la Commissione di sorveglianza dovrà uniformarsi nella scelta dei documenti da scartare, in conformità al disposto di cui agli artt. da 6 a 9 del d.p.r. 8.1.2001, n. 37 e 19 n. 1 del d.p.r. 20.10.1998, n. 428 e 35 d.p.r. 30.9.1963, n. 1409. Si è proceduto a richiedere al Procuratore Generale della Repubblica la designazione, in conformità al disposto di cui all'art. 2 comma 2 e 3 comma 1 d.p.r. 8.1.2001, n. 37, regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di sorveglianza sugli archivi e per lo scarto dei documenti degli uffici dello Stato, dei componenti della Commissione medesima. La Commissione si è insediata ed ha espletato regolarmente le sue attività, si è in attesa delle autorizzazioni necessarie all'espletamento ed attuazione dello scarto degli atti.

5. Criteri e modalità per il ripristino della disponibilità dei dati a seguito distruzione o danneggiamento.

Tutti i dati relativi ai sistemi che operano in rete locale sono giornalmente salvati su server dedicati e il loro ripristino è demandato all'amministratore di sistema.

I dati, invece, relativi a sistemi che operano su rete nazionale sono lavati su stazioni di backup nazionali che garantiscono l'immediato ripristino degli stessi.

6. RE.GE . (Registro generale penale), S.I.C.P. (Sistema Informativo della Cognizione Penale) e S.I.C. (Sistema informativo del Casellario)

I funzionari e gli addetti all'uso dei sistemi informatici Re.Ge., S.I.C.P. e S.I.C. avranno cura di attenersi alle procedure operative dei detti software al fine di garantire l'integrità dei dati sensibili.

7. Notificazione di atti.

Per quanto riguarda la notificazione di atti, ivi compresi i decreti di perquisizione, i magistrati e la polizia giudiziaria osserveranno le regole del codice di procedura penale e delle leggi speciali, curando con particolare attenzione che la notifica a persone diverse dal destinatario abbia luogo con plico chiuso e sigillato, con l'indicazione all'esterno della busta del solo numero cronologico della notificazione, dandone atto nell'originale e nella copia, in conformità al disposto di cui all'art. 148 c. 3 c.p.p., come modificato dall'art. 174 d.lgs. n. 196 del 2003 e le comunicazioni, gli avvisi ed ogni altro biglietto o invito consegnati non in busta chiusa a persona diversa dal destinatario recano le indicazioni strettamente necessarie, ai sensi del comma 5 bis dell'art. 148, come modificato dall'art. 174 d.lgs. n. 196 del 2003.

Il codice di procedura penale ammette la notificazione anche a mezzo fax (art. 148 c. 2 bis c.p.p. e 54 c. 3 disp. att. c.p.p., dove si stabilisce che

l'autorità giudiziaria può disporre che le notificazioni o gli avvisi ai difensori siano eseguiti con mezzi tecnici idonei e che l'ufficio che invia l'atto attesta in calce ad esso di avere trasmesso il testo originale.

Dal mese di Luglio 2014 è stata avviata la sperimentazione delle procedura per le notifiche telematiche a soggetti diversi dall'indagato, secondo le indicazioni della normativa vigente in materia di firma digitale, per cui l'apposito decreto è stato comunicato al Consiglio dell'Ordine degli avvocati e alla Camera Penale di Siracusa oltreché al CISIA e alla DGSIA, come più compiutamente si espone al paragrafo 20.

Dal mese di Luglio 2015 ha preso avvio l'istituzione del Portale NDR, Notizie di reato per la trasmissione telematica delle Notizie di reato da parte degli organi di p.g.

L'avvio del sistema di notificazioni e comunicazioni telematiche è stato disposto dal procuratore della Repubblica con decreto del giorno 11.7.2014, col quale si istituiva a titolo sperimentativo e per la durata temporale dal 15 luglio al 30 settembre 2014 il sistema di notifiche telematiche, mediante l'uso di notifiche agli indirizzi di posta elettronica certificata a soggetti diversi dall'imputato, pertanto ai difensori delle parti, anche se domiciliatari, periti e consulenti, alla persona offesa, alla parte civile, al responsabile civile, sempreché fossero dotati di un indirizzo di posta elettronica certificata, abilitando all'uso del sistema i cancellieri, gli operatori e i funzionari giudiziari preposti ai vari servizi e alle segreterie dei magistrati. Con decreto del 30 settembre 2014, fu disposta la proroga del sistema fino al 31.12.2014. Con decreto del 4 febbraio 2015, il sistema venne adottato in via definitiva. Il bilancio complessivo è altamente positivo, in quanto sono stati ridotti gli adempimenti delle notifiche, con aggravio delle incombenze da parte dei vari uffici.

Si applica al SNT la disciplina sulla sicurezza dei supporti informatici

8. Richiesta di atti per scopi di informazione giuridica

Le "Linee-guida in materia di trattamento di dati personali nella riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica" (in G.U. 4 gennaio 2011, n. 2; [doc. web n. 1774813]) prevedono che l'anonimizzazione del provvedimento giudiziario in caso di riproduzione per finalità di informazione giuridica, mediante oscuramento delle generalità e di ogni altro elemento in grado di identificare l'interessato, può essere disposta dal giudice anche d'ufficio, nei casi in cui la diffusione di informazioni particolarmente delicate possa arrecare conseguenze negative alla vita di relazione o sociale dell'interessato (ad es., in ambito familiare o lavorativo). Perciò si avrà cura, da parte dei soggetti richiesti, di adeguare il rilascio delle copie di atti per scopi di informazione giuridica, a tali principi.

9. Cronaca giudiziaria e trattamento dati

L'Autorità Garante ha risposto a diversi reclami e segnalazioni richiamando il principio, ormai consolidato, secondo cui la pubblicazione di dati personali relativi a procedimenti penali è ammessa anche senza il consenso dell'interessato, nei limiti dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico (art. 137, comma 3, del Codice; artt. 5, 6 e 12 del codice di deontologia). La valutazione deve essere fatta caso per caso, in prima battuta dal giornalista, nel quadro anche delle disposizioni che disciplinano il segreto delle indagini e il regime di

pubblicazione degli atti processuali (artt. 114 e 329 c.p.p. e art. 684 c.p.). Perciò si avrà cura da parte dei magistrati, operatori amministrativi e di polizia giudiziaria di osservare rigorosamente tali limitazioni, nel contesto della disciplina che impone che i rapporti con la stampa devono essere tenuti dal procuratore capo della Repubblica.

10. Tabulati telefonici

Il Garante ha stabilito che i dati relativi al traffico telefonico non più necessari ai fini della trasmissione della comunicazione elettronica sono cancellati o resi anonimi dal fornitore del servizio, al quale è consentito il trattamento a fini di fatturazione per un periodo non superiore a sei mesi, salva l'ulteriore conservazione necessaria per effetto di una contestazione anche in sede giudiziale. Al di fuori di tali ipotesi, i dati relativi al traffico telefonico sono conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, solo per finalità di accertamento e repressione di reati (art. 132 del Codice, commi 1 e 3), non per richieste formulate nell'ambito di una controversia civile, amministrativa e contabile (v. provvedimento generale sulla sicurezza dei dati di traffico telefonico e telematico del 17 gennaio 2008).

Mentre l'ostensione di tali dati in sede civile è ammessa solo in controversie attinenti alla fatturazione del servizio (nota 31 ottobre 2012).

11. Verbali di commissioni di invalidità

In sede di decisione su ricorso, per conoscere le corrette modalità di comportamento in caso di richieste della polizia giudiziaria, finalizzate alla prosecuzione delle indagini, di accesso ai dati personali contenuti nei verbali di invalidità civile contenenti l'indicazione delle patologie, il Garante ha ricordato che tale ipotesi è regolata dall'art. 25, comma 2, del Codice -applicabile anche ai trattamenti effettuati dai soggetti pubblici, in base al rinvio di cui all'art. 18, comma 5, del Codice stesso- che, tra l'altro, consente la comunicazione di dati richiesti, in conformità alla legge, dalle forze di polizia per finalità di prevenzione, accertamento o repressione di reati (nota 21 novembre 2012).

12. Accorgimenti adottati per l'Ufficio Ricezione Atti

L'Ufficio Ricezione Atti, posto al IV° piano, tratta le istanze inerenti alle varie certificazioni fra cui quelle riguardanti i carichi pendenti, si è disposto per garantire la massima riservatezza, che l'utenza anziché dire a voce il nominativo richiesto, compili un modulo prestampato e che i soggetti che attendono in fila siano distanziati rispetto al bancone con vetrata della ricezione.

TRATTAMENTO DI DATI AFFIDATI ALL'ESTERNO

Nel momento in cui i dati da trattare sono affidati all'esterno gli incaricati avranno cura di assicurare:

1. Il trattamento dei dati verrà effettuato ai soli fini dell'espletamento dell'incarico ricevuto;

2. Il rispetto delle istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o integrazione delle procedure già in essere;
3. L'impegno a relazionare periodicamente sulle misure di sicurezza adottate, anche mediante eventuali questionari e liste di controllo, e ad informare immediatamente il titolare del trattamento in caso di situazioni anomale o di emergenze;
4. All'atto del conferimento dell'incarico il consulente tecnico del p.m. e gli ausiliari del p.m. devono impegnarsi, con dichiarazione messa a verbale, ad adottare le misure di sicurezza idonee a preservare i dati da eventi pericolosi, quali gli accessi e le utilizzazioni indebite. Il consulente, altresì, si impegna a consegnare per il deposito agli atti del procedimento la propria relazione unitamente alla documentazione versategli per il compimento del mandato. Qualora il trattamento dei dati sensibili o giudiziari sia effettuato con l'ausilio di strumenti elettronici, nell'ambito delle misure minime, deve essere redatto il documento programmatico sulla sicurezza.

Il consulente, inoltre, al momento del deposito della perizia dovrà dichiarare che non ha conservato, in originale o in copia, in formato elettronico o su supporto cartaceo, informazioni personali acquisite nel corso dell'incarico concernenti i soggetti, persone fisiche e giuridiche, nei cui confronti ho svolto accertamenti.

L'ufficio darà atto che il consulente ha dichiarato di aver nel corso delle operazioni peritali curato personalmente sia "le misure idonee e preventive" cui fa riferimento l'art. 31 del codice della privacy, sia le misure "minime" specificamente indicate negli articoli da 33 a 35 e nel

disciplinare tecnico, allegato B) al medesimo codice, e che, poiché il trattamento dei dati sensibili o giudiziari è stato effettuato con l'ausilio di strumenti elettronici il consulente ha redatto il documento programmatico sulla sicurezza con le modalità e i contenuto previsti dal disciplinare tecnico.

INTERVENTI FORMATIVI DEGLI INCARICATI DEL TRATTAMENTO

Nell' impossibilità di finanziare autonomamente regolari corsi periodici di informazione e di formazione, sarà garantita la partecipazione del personale alle iniziative didattiche organizzate dalle strutture ministeriali oltre ad agevolare e favorire scambi di esperienze e conversazioni con l'ausilio di esperti volontari (se reperiti e disponibili).

Sono autorizzate periodiche riunioni, preferibilmente con frequenza mensile, tra gli incaricati (magistrati e personale amministrativo che opera con strumenti elettronici) per lo scambio di informazioni sullo stato del servizio - a cominciare dall'esame del D.P.S. - sulla evoluzione delle tecniche di protezione dei dati e sulle misure per migliorare il coefficiente di riservatezza del trattamento dei dati personali.

Le riunioni saranno indette e coordinate dal magistrato addetto all'informatica, dal dirigente amministrativo e dal Responsabile del S.I.C.P..

Brevi e informali relazioni sull'esito delle riunioni costituiranno per la dirigenza utile strumento di riflessione e di miglioramento delle misure di salvaguardia dei dati personali.

MONITORAGGIO E VIGILANZA SUL RISPETTO DELLE PRESCRIZIONI CONTENUTE NEL PRESENTE DOCUMENTO

I Responsabili dei vari servizi sono tenuti a monitorare l'osservanza delle prescrizioni e a segnalare al Procuratore Capo eventuali violazioni ai sensi degli artt. 162 e segg. Codice privacy e succ. modifiche.

AGGIORNAMENTO PERIODICO DEL D.P.S.

Come previsto dal punto 4.8 della Direttiva 11 febbraio 2005 del Dipartimento della Funzione Pubblica e dal punto 19 dell'Allegato B del codice sulla privacy, il D.P.S. va aggiornato entro il 31 marzo di ogni anno.

INDICE

Siracusa, 25 Febbraio 2016

IL PROCURATORE DELLA REPUBBLICA
Francesco Paolo Giordano