



**ISTITUTO ROMANO DI SAN MICHELE**  
**Istituzione Pubblica di Assistenza e Beneficenza**

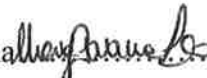
Legge 17.7.1890 n. 6972 – R.D. 7.6.1928 n. 1353  
00147 ROMA - Piazzale Antonio Tosti n. 4  
TEL. 06/51858205 – FAX 06/5120986

**DECRETO del Commissario Straordinario N. 109 del 8 giugno 2018**

**OGGETTO:** Attribuzione deleghe di funzioni per la protezione dei dati personali dell'Istituto Romano di San Michele.

Ufficio proponente: Ufficio Presidenziale

Estensore dell'atto  
Dott.ssa Maria Giovanna Leo

firma  addì 08/06/2018

Il Responsabile del Procedimento sotto riportato, a seguito dell'istruttoria, con la sottoscrizione del presente atto attesta che l'atto è legittimo nella forma e nella sostanza ed è utile per il servizio pubblico

Il Responsabile del Procedimento:

Il Responsabile dell'Ufficio Bilancio con la firma del presente atto attesta che i costi di cui al presente atto sono da imputare sui seguenti capitoli e articoli di bilancio

- ☐ non comporta impegno di spesa
- ☐ da imputare al cap. art. del bilancio di esercizio finanziario 2018

Il Responsabile dell'Ufficio Bilancio: Dott.ssa Roberta Valli

firma..... addì \_\_\_/\_\_\_/\_\_\_

Parere

FAVOREVOLE ☒ NON FAVOREVOLE ☐ (per le motivazioni riportate in allegato al presente atto)

Il Segretario Generale  
Dott. Claudio Panella

firma  addì 08/06/2018



## **Il Commissario Straordinario**

**Visto** il decreto del Presidente della Regione Lazio n. T00200 del 7 novembre 2017 – pubblicato sul BURL n.91 del 14 novembre 2017 - con il quale è stato nominato Commissario Straordinario dell'IPAB Istituto Romano di San Michele il Dott. Domenico Alessio dalla data di pubblicazione fino al 31 dicembre 2017 *“al fine di garantire l'ordinaria e straordinaria amministrazione”*;

**Preso atto** dell'effettivo insediamento del Dott. Domenico Alessio in data 14 novembre 2017 nelle funzioni di Commissario Straordinario;

**Visto** il decreto n. 390 del 5.12.2017 di attribuzione delle funzioni sostitutive del Segretario Generale al Funzionario del Personale così come indicato dalla Direzione Generale Attività di Controllo e Coordinamento delle funzioni di vigilanza;

**Preso atto** della deliberazione di Giunta Regionale n. 911 del 21/12/2017 di proroga del Commissariamento fino al 30/10/2018 - pubblicato sul BURL n. 2 del 4 gennaio 2018;

**Preso atto**, altresì, del Decreto del Presidente della Regione Lazio n. T00049 del 5 febbraio 2018 pubblicato sul BURL n. 11 del 6 febbraio 2018 di nomina del Dott. Domenico Alessio, quale Commissario Straordinario dell'Istituto Romano di San Michele fino al 30 ottobre 2018;

**Preso atto** del Decreto del Commissario Straordinario n. 57 del 14.03.2018 con il quale è stato affidato l'incarico triennale di Segretario Generale al Dott. Claudio Panella;

**Visto** il “Trattato sul funzionamento dell'Unione Europea” (TFUE) stipulato a Roma il 25 marzo 1957, e successive modificazioni e integrazioni;

### **Visti i Decreti Legislativi:**

- 30 giugno 2003, n. 196, “Codice in materia di protezione dei dati personali”;
- 22 gennaio 2004, n. 42, “Codice dei beni culturali e del paesaggio [...]”, per la parte inerente la documentazione sanitaria;
- 7 marzo 2005, n. 82, “Codice dell'Amministrazione Digitale” (CAD), così come modificato dal D.Lgs. 4 aprile 2006, n. 159; dalla L. 24 dicembre 2007, n. 244; dalla L. 28 gennaio 2009, n. 2; dalla L. 18 giugno 2009, n. 69; dalla L. 3 agosto 2009, n. 102; dal D.Lgs. 30 dicembre 2010, n. 235; dal D.L. 18 ottobre 2012, n. 179, convertito dalla L. 17 dicembre 2012, n. 221; dal D.L. 21 giugno 2013, n. 69, convertito dalla L. 9 agosto 2013, n. 98; dal D.Lgs. 26 agosto 2016, n. 179; e, per ultimo, dal D.Lgs. 13 dicembre 2017, n. 217;

**Visto** il D.Lgs. 30 maggio 2008, n. 109, “Attuazione della direttiva 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione [...]”;

**Visto** il D.Lgs. 14 marzo 2013, n. 33, “Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni”;

**Vista** la L. 20 novembre 2017, n. 167, recante “Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea - Legge europea 2017”

### **Visti i Regolamenti adottati dal Parlamento europeo e dal Consiglio:**

- UE/2014/910 del 23 luglio 2014 “in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno” (Regolamento eIDAS);



- UE/2016/679 del 27 aprile 2016 relativo alla “protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati [...]” (GDPR);
- VISTO il “Codice di deontologia medica” approvato dalla FNOMCeO il 18 maggio 2014 e smi, e, in particolare, gli artt. 10-12; l’art. 20; gli artt. da 25-26; gli artt. da 33-38; l’art. 78 e il relativo allegato “indirizzi applicativi” riguardanti le tecnologie informatiche;

**Visti** i Codici di deontologia e di buona condotta adottati dal Garante per la protezione dei dati personali, riguardanti i trattamenti di dati personali:

“a scopi statistici e di ricerca scientifica effettuati nell’ambito del Sistema statistico nazionale”, Provvedimento 31 luglio 2002, n. 13;

“per scopi statistici e scientifici”, Provvedimento 14 agosto 2004, n. 190;

**Visti** i Provvedimenti del Garante per la protezione dei dati personali e, in modo particolare ma non esclusivo:

- “Dati sanitari. Provvedimento generale sui diritti di “pari rango”, adottato con Provvedimento in data 9 luglio 2003;
- “Linee guida per posta elettronica e internet”, adottate con Deliberazione 1° marzo 2007, n. 13;
- “Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico”, adottate con Deliberazione 14 giugno 2007, n. 23;

**Vista** la Direttiva UE/2016/1148 adottata dal Parlamento europeo e dal Consiglio in data 6 luglio 2016 “recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell’Unione”;

**Vista** la Direttiva PCM 1° agosto 2015 con la quale sono state emanate disposizioni riguardanti la sicurezza informatica nazionale;

**Vista** la Circolare AgID 18 aprile 2017, n. 2, “Misure minime di sicurezza ICT per le pubbliche amministrazioni”;

**Considerato** quanto previsto dall’art. 4 del GDPR UE/2016/679 in ordine alla figura e al ruolo del:

- “Titolare del trattamento”, quale persona fisica o giuridica che determina le finalità e i mezzi del trattamento di dati personali [ c. 1, n. 7 ];
- “Responsabile del trattamento”, quale persona fisica o giuridica che tratta dati personali per conto del Titolare del trattamento [ c. 1, n. 8 ];
- “Terzo”, quale persona fisica o giuridica autorizzata al trattamento dei dati personali sotto l’autorità diretta del Titolare o del Responsabile [ c. 1, n. 10 ];

**Tenuto conto** dell’indirizzo espresso dal Garante in ordine alla figura dell’Incaricato introdotta dall’art. 30 e preso atto che nella “Guida all’applicazione del Regolamento europeo in materia di protezione dei dati personali” il Garante afferma che, pur non essendo espressamente prevista la figura dell’“Incaricato”, il Regolamento individua quale funzione operativa del trattamento le persone “autorizzate dal Titolare”. Tale definizione non contrasta quindi con le previsioni dell’art. 30 del Codice, anzi le rafforza su scala europea;

**Considerato** che con il Regolamento europeo cessano di avere efficacia i principi della normativa nazionale in contrasto con il GDPR senza tuttavia che sia abrogato il Codice nel suo complesso;

**Considerato** che il criterio di “autorizzazione preventiva” del personale al quale è consentita l’esecuzione dei processi organizzativi e dei conseguenti trattamenti di dati non contrasta, anzi coincide, con gli obblighi già previsti dall’art. 30 del D.Lgs. 196/03, e che pertanto permane l’obbligo di individuare



preventivamente e di autorizzare specificamente il personale incaricato dell'attuazione dei processi organizzativi definiti dal Titolare attraverso i relativi trattamenti;

**Considerato** infine che la figura del "Responsabile del trattamento" definita dall'art. 4, c. 1, par. 8, del GDPR si riferisce a soggetti esterni [ fornitori di servizi, associazioni di volontariato, etc. ] che trattano dati in esecuzione di un contratto o di altro atto giuridico che disciplina i processi, le procedure, gli strumenti e gli obblighi di qualità e di vigilanza ] GDPR, art. 28, c. 3 ] contratti con il Titolare;

**Considerato** che l'art. 28, c. 2, del GDPR prevede che il Responsabile del trattamento non possa ricorrere ad altro Responsabile [ subaffidamento ] senza previa autorizzazione scritta specifica del Titolare del trattamento;

**Considerato** che tale prescrizione si coordina con l'art. 105 del D.Lgs. 50/2016, "Codice degli appalti" che disciplina le forme, le modalità e i limiti del ricorso al subappalto;

**Considerata** l'articolazione organizzativa dell'Istituto;

**Ravvisata** la necessità di definire un sistema di delega di funzioni che risponda alle specifiche necessità operative dei servizi e all'esigenza di disporre di una rete di indirizzo e di governo più prossima alle strutture produttive così da rendere più tempestiva ed efficace l'individuazione del personale autorizzato e incaricato, l'informazione, la formazione, l'individuazione dei processi, delle procedure e degli strumenti autorizzati per ciascun trattamento, la vigilanza sulle procedure e sui trattamenti, alla protezione dei dati e la tempestiva segnalazione al Titolare di eventuali violazioni [data breach];

**Ritenuto** utile per queste ragioni e rispondente al pubblico interesse definire un sistema di delega di funzioni in materia di trattamento e protezione dei dati secondo la seguente articolazione:

- a) Segretario Generale;
- b) Responsabile del Servizio Prevenzione e Protezione;

**Considerata** comunque la nuova regolamentazione introdotta dal Regolamento a partire dal 25 maggio p.v. simultaneamente in tutti i Paesi aderenti all'Unione e considerato che i Regolamenti UE, per loro natura, non necessitano di specifiche norme nazionali di recepimento;

**Nelle more** del decreto legislativo di coordinamento e di integrazione del quadro normativo nazionale rispetto Regolamento UE/2016/679;

**Vista** la legge 17.7.1890 n. 6972 e successive modificazioni;

**Visto** lo Statuto dell'Istituto Romano di San Michele;

**Visto** l'art. 21 del D. Lgs.vo n. 207 del 4 maggio 2001;

## DECRETA

*le premesse formano parte integrante e sostanziale del presente Decreto*

1) A decorrere dalla data della presente deliberazione, nell'ambito delle rispettive funzioni di istituto, sono attribuite le seguenti deleghe di funzioni riguardanti la protezione dei dati personali dell'Istituto Romano S. Michele:

- Segretario Generale;
- Responsabile del Servizio Prevenzione e Protezione;



2) Ciascun “Delegato per la protezione dei dati” è tenuto ad assicurare quanto necessario per un adeguato indirizzo, organizzazione e vigilanza sulle strutture e sui soggetti che a qualsiasi titolo vi operano, in attuazione del GDPR UE/2016/679, del D.Lgs. 196/03, delle norme, dei regolamenti e dei Provvedimenti del Garante richiamati in premessa e delle specifiche istruzioni fornite dal “Titolare del Trattamento”.

3) Ciascun “Delegato per la protezione dei dati” è tenuto ad eseguire direttamente, nell’ambito delle istruzioni fornite dal “Titolare del trattamento”, quanto di seguito specificato:

- 3.1 autorizzazione del personale dipendente assegnato alla struttura mediante atto individuale:
  - a) che specifichi il ruolo operativo assegnato all’interno dell’organizzazione;
  - b) contenente specifiche istruzioni rapportate alla funzione operativa, alle procedure, agli strumenti autorizzati per ciascun incaricato ed al relativo profilo applicativo, ove i trattamenti debbano essere effettuati con sistemi informatici;
  - c) acquisito al protocollo dell’Istituto;
  - d) notificato individualmente;
  - e) che vincoli espressamente l’operatore autorizzato a un pari obbligo di riservatezza e di rispetto del segreto professionale già prescritto dai Codici deontologici delle professioni;
- 3.2 verifica che il livello di conoscenza e di consapevolezza dei dipendenti autorizzati ad effettuare trattamenti di dati sia adeguato a quello necessario per la loro effettuazione;
- 3.3 formazione e aggiornamento periodico del personale dipendente con condivisione dei processi, delle misure organizzative, delle procedure e degli strumenti autorizzati;
- 3.4 verifica che il livello di conoscenza e di consapevolezza degli addetti di eventuali fornitori di servizi o delle associazioni di volontariato operanti nell’Istituto in esecuzione di un contratto, di una convenzione o di altro atto giuridico, sia adeguato a quello necessario per l’effettuazione dei trattamenti di dati che si svolgono nella struttura. Ove sia carente, deve essere data comunicazione tempestiva al Titolare e al RUP affinché prescrivano al rispettivo Responsabile un’adeguata formazione e aggiornamento del personale;
- 3.5 presa d’atto dei dipendenti di fornitori di servizi o di associazioni di volontariato autorizzati ad operare nella struttura in virtù di un contratto, di una convenzione o di altro atto giuridico, assegnando loro per scritto uno specifico ruolo operativo all’interno dell’organizzazione e autorizzando il rilascio delle conseguenti credenziali per l’accesso ai sistemi IT dell’Istituto con indicazione dello specifico profilo applicativo, ove siano necessarie per l’esecuzione del contratto;
- 3.6 verifica che il Titolare del trattamento dei fornitori di servizi o delle associazioni di volontariato abbia provveduto preventivamente:
  - a) alla loro autorizzazione [ Incarico ] erogando le specifiche istruzioni necessarie;
  - b) alla loro formazione e aggiornamento riguardo il trattamento e la protezione dei dati, le procedure, i vincoli, le responsabilità e i rischi;
- 3.7 adozione di misure organizzative e operative adeguate al soddisfacimento dei requisiti previsti a garanzia della tutela dei diritti dell’interessato, modellate sulle specifiche esigenze operative dell’Istituto;
- 3.8 affissione in tutti i locali dell’Istituto degli appositi avvisi riguardanti il trattamento e la protezione dei dati da parte dell’Istituto;
- 3.9 vigilanza sull’idoneità dell’informativa resa all’interessato preliminarmente rispetto al trattamento di dati e adozione di eventuali ulteriori misure, necessarie per elevare la qualità e la comprensibilità della comunicazione;
- 3.10 vigilanza sull’attestazione del consenso/dissenso informato per il trattamento dei dati reso nelle forme e con gli strumenti previsti dall’Istituto;
- 3.11 vigilanza sull’espressione del consenso/dissenso informato per il trattamento dei dati per fini di gestione amministrativa, contabile, tecnica o logistica, reso dall’interessato nelle forme e con gli strumenti previsti dall’Istituto, avendo cura di verificare che questo sia sempre riposto tra la documentazione riguardante la posizione del dipendente, il contratto di fornitura o la convenzione;



- 3.12 vigilanza sull'accesso e sull'utilizzazione dei dati per fini statistici o di ricerca nel rispetto dei vincoli definiti dagli specifici Regolamenti UE di settore e Linee guida del Garante;
- 3.13 segnalazione al "Titolare del trattamento" di eventuali violazioni dei dati avvenute nel corso di trattamenti con sistemi automatici e non [ data-breach ] entro il limite massimo di dodici ore dal momento in cui il Delegato ne è venuto a conoscenza affinché il "Titolare", sentito anche il DPO, valuti la probabilità che da tale violazione derivino rischi per i diritti e le libertà delle persone e, in caso affermativo, proceda ad informarne l'Autorità di controllo [ Garante ] e gli interessati [ GDPR, artt. 33 e 34 ];
- 3.14 partecipazione alla redazione e all'aggiornamento continuo nel tempo del "Registro dei trattamenti" [ GDPR, art. 30 ] anche mettendo a disposizione del Titolare e del DPO valutazioni e contributi riguardanti la struttura per la quale si esercita la delega;
- 3.15 partecipazione alla realizzazione della "Valutazione di impatto sui dati" preliminare all'avvio di eventuali nuovi trattamenti di dati nella struttura per la quale si esercita la delega;
- 3.16 collaborazione con il Titolare per l'esercizio dei diritti dell'interessato [ GDPR, art. 12, 13 e 14 ];
- 3.17 valutazione dei rischi per i dati derivanti dai processi, dalle procedure, dall'organizzazione, dagli strumenti autorizzati o dal livello di consapevolezza, formazione e aggiornamento di ciascun Incaricato operante nella struttura per la quale si esercita la delega, adozione di misure volte al superamento di criticità, proposta di interventi correttivi riguardanti i processi o le procedure;
- 3.18 collaborazione con il "Responsabile della protezione dei dati" [ DPO - GDPR, artt. 37 e 39 ] al fine dell'individuazione dei trattamenti eseguiti nella struttura, della loro verifica in termini di conformità, dell'informazione e consulenza del Titolare o di eventuali Responsabili;
- 3.19 vigilanza sull'utilizzazione degli strumenti informatici e delle tecnologie autorizzate rese disponibili dal Titolare;
- 3.20 vigilanza sul divieto di:
  - a) utilizzare strumenti o sistemi informatici non preliminarmente valutati, approvati e autorizzati dal Titolare;
  - b) costituzione autonoma di basi di dati contenenti dati identificativi degli interessati;
  - c) utilizzazione di sistemi di public cloud o di social media per condividere dati e immagini degli interessati, indipendentemente se identificati o identificabili attraverso codici;
- 3.21 vigilanza affinché nessun soggetto privo di atto di incarico o di autorizzazione con specifiche istruzioni:
  - a) operi nell'Istituto;
  - b) acceda ai dati a questo conferiti;
  - c) effettui trattamenti;
- 3.22 individuazione di eventuali "Contitolari del trattamento" [ GDPR, art. 26 ] qualora il trattamento sia effettuato in ottemperanza di norme regionali/nazionali, con predisposizione degli specifici atti necessari per individuare i distinti ruoli e responsabilità, e definire le specifiche istruzioni riguardanti i processi, le procedure, gli strumenti ed i trattamenti autorizzati;
- 3.23 accreditamento di tutti coloro che sono stati autorizzati a trattare dati utilizzando sistemi informatici e procedure automatiche per i quali sono richieste le credenziali personali di autenticazione per l'accesso ai sistemi informatici dell'Istituto.

4) Nell'ambito della delega di funzioni è inoltre richiesto ai RUP:

- di prevedere, nell'ambito dei capitolati di gara, le specifiche disposizioni necessarie per l'adempimento delle prescrizioni introdotte dal GDPR, compresi i vincoli riguardanti:
  - a) il subappalto e la responsabilità solidale del fornitore di servizi in veste di Responsabile del trattamento [ GDPR, art. 28, c. 2 ];
  - b) l'obbligo di riservatezza e il vincolo al segreto professionale;
- di predisporre gli specifici atti necessari per l'aggiornamento dei contratti in essere con le prescrizioni e le responsabilità previste dal GDPR [ GDPR, art. 28, c. 3 ];
- di comprendere nei rispettivi atti:



- a) la descrizione puntuale dei processi, delle procedure, degli strumenti e delle prescrizioni alle quali l'aggiudicatario [ Responsabile del trattamento ] è soggetto;
- b) i vincoli riguardanti l'eventuale subappalto;
- c) l'obbligo di notifica preventiva al Titolare di un eventuale subappalto;
- d) l'obbligo di procedervi solamente dopo aver acquisito l'accettazione esplicita del Titolare;
- e) la responsabilità solidale del Responsabile del trattamento nei confronti del Titolare , compresa quella riguardante la liceità dei trattamenti effettuati da eventuali sub-Responsabili [ GDPR, art. 28, c. 2 ];
- f) l'obbligo di riservatezza e il vincolo al segreto professionale indipendentemente dall'appartenenza e dal ruolo del singolo operatore.

5) Con successiva nota del Commissario Straordinario sarà notificato a ciascun soggetto di cui al precedente articolo 1 l'atto individuale di delega comprendente le istruzioni del Titolare.

6) La presente deliberazione non prevede costi aggiuntivi a carico del bilancio dell'Istituto.

7) La presente deliberazione è inviata al Responsabile del Settore Patrimonio e Informatico perché provveda alla sua pubblicazione nella sezione Amministrazione trasparente del portale internet istituzionale dell'Istituto.



IL COMMISSARIO STRAORDINARIO  
(Dott. Domenico Alessio)



ISTITUTO ROMANO DI SAN MICHELE

## PUBBLICAZIONE

**Decreto del Commissario Straordinario n.109 del 08.06.2018**

**Si attesta che il Decreto del Commissario Straordinario n.109 del 08.06.2018  
ai sensi e per gli effetti dell'art. 32 della L.18.06.2017 n. 69 e ss.mm.ii. è stato pubblicato  
sul sito istituzionale dell'Istituto Romano di San Michele in data 08.06.2018**

**L'Istruttore Direttivo Amministrativo  
(Dott.ssa Antonietta Antenucci)**