

50122 Firenze, Italia
Piazza SS. Annunziata, 12
centralino tel. 055.20371
fax 055.241663

info@istitutodeglinnocenti.it
www.istitutodeglinnocenti.it
C.F: 80016790489
P.I. 00509010484

**Istituto
degli
Innocenti**



Allegato A) Le modifiche sono evidenziate in neretto e sottolineate

Regolamento sul trattamento dei dati personali effettuato dall'Istituto degli Innocenti

(approvato con delibera del Consiglio di Amministrazione n. 15 del 14 marzo 2019)

Sommario

Art. 1. Premessa e finalità

Art. 2. Definizioni

Art. 3. Campo d'applicazione

Art. 4. Titolare, Responsabili e Incaricati del trattamento dei dati e Amministratore di sistema

Art. 5. Il Responsabile della protezione dei dati personali (Data Protection Officer)

Art. 6. Circolazione dei dati nell'ambito dell'Istituto

Art. 7. Circolazione dei dati fuori dell'ambito dell'Istituto

Art. 8. Trattamento di categorie particolari di dati

Art. 9. Responsabilità

Art. 10. Modalità di raccolta e requisiti dei dati personali

Art. 11. Comunicazione e censimento degli archivi automatizzati e cartacei

Art. 12. Diritti dell'interessato

Art. 13. Modifiche e rinvio

Art. 1. Premessa e finalità

1. Il presente regolamento, adottato in attuazione del Regolamento UE 2016/679 del Parlamento e del Consiglio Europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito GDPR EU 2016/679), disciplina il sistema di gestione dei dati personali all'interno della A.S.P. Istituto degli Innocenti, nel seguito per brevità "*Istituto*".
2. La finalità del presente Regolamento è assicurare che il trattamento dei dati personali avvenga nel rispetto della vigente normativa e dei diritti, con particolare riguardo alla riservatezza e all'identità personale degli utenti e di tutti coloro che hanno rapporti con l'Istituto.

Art. 2. Definizioni

1. Ai fini del presente regolamento, si adottano le definizioni contenute nel GDPR EU 2016/679 e pertanto si intende:
 - a) “dato personale”: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
 - b) “trattamento”: 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;
 - c) “limitazione di trattamento”: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
 - d) “profilazione”: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
 - e) “pseudonimizzazione”: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e

organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

- f) “comunicazione”: dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal Rappresentante del Titolare nel territorio dello Stato, dal Responsabile e dagli Incaricati e dall'Amministratore di sistema in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- g) “diffusione: dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- h) “archivio”: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- i) “Titolare del trattamento”: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- j) “Responsabile del trattamento”: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento;
- k) “Incaricati”: le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile;
- l) “interessato”: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
- m) “destinatario”: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
- n) “terzo”: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il Titolare del trattamento, il Responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile;
- o) “consenso dell'interessato”: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

- p) “violazione dei dati personali”: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- q) “dati genetici”: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- r) “dati biometrici”: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- s) “dati relativi alla salute”: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- t) “Rappresentante”: la persona fisica o giuridica che, designata dal Titolare del trattamento o dal Responsabile del trattamento per iscritto, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;
- u) “autorità di controllo”: l'autorità pubblica indipendente istituita da uno Stato membro dell'UE;

Art. 3. Campo d'applicazione

1. Il presente regolamento si applica al trattamento dei dati personali effettuato con qualsiasi modalità dall'Istituto, dai suoi Responsabili (interni ed esterni), Incaricati (interni ed esterni) e Amministratori di sistema ai fini dell'esatto adempimento dei compiti assegnati nell'ambito delle proprie funzioni e, in ogni caso, nella misura a ciò strettamente necessaria.

Art. 4. Titolare, Responsabili, Incaricati del trattamento dei dati e Amministratore di sistema

1. Il Titolare del trattamento dell'Istituto, è l'Ente nel suo complesso rappresentato dal Presidente *pro tempore* che delega le funzioni relative al Direttore Generale *pro tempore* quale “Delegato del Titolare”.
2. Il Delegato del Titolare è investito del potere di pianificare ed attuare le linee strategiche ed organizzative dell'Ente.
3. Rientrano tra i principali compiti in capo al Titolare, e quindi al suo Delegato, quelli di:

- a) nominare i Responsabili e gli Incaricati interni ed esterni del trattamento e gli Amministratori di Sistema e provvedere agli aggiornamenti in caso di dimissioni o cambiamenti degli stessi;
- b) emanare e approvare le procedure per garantire la corretta applicazione della normativa privacy all'interno dell'Istituto e da parte di tutti coloro che, a diverso titolo, abbiano conoscenza dei dati la cui titolarità appartiene all'Istituto;
- c) garantire il corretto svolgimento dell'attività di vigilanza e controllo in conformità a quanto disposto dall'art. 32 del GDPR R EU 2016/ 679;
- d) garantire la sicurezza nel trattamento dei dati fin dalla progettazione e protezione per impostazione predefinita in conformità a quanto disposto dall'art. 25 del GDPR EU 2016/679;
- e) vigilare sulla puntuale osservanza delle disposizioni in materia di trattamento e delle istruzioni fornite.

4. Il Titolare del Trattamento può designare Responsabili interni del trattamento i Dirigenti e/o i Responsabili di Posizione Organizzativa

5. I Responsabili Esterni sono le persone giuridiche o fisiche terze (outsourcers) che, nell'espletamento delle mansioni affidate, trattano dati di cui l'Istituto è Titolare.
6. Rientrano tra i principali compiti in capo al Responsabile quelli di:
 - a) effettuare il trattamento attendendosi ai compiti e istruzioni ricevute dal Titolare;
 - b) garantire che la protezione dei dati, all'interno della struttura di propria competenza, sia realizzata in base alle misure di sicurezza disposte dall'Istituto e previste dalla legge;
 - c) assicurare il pieno rispetto degli adempimenti formali nei modi e nei tempi previsti dal GDPR EU 2016/679;
 - d) collaborare nelle verifiche predisposte dal Titolare.

7. Il Titolare del Trattamento, o il Responsabile ove nominato, designa il personale dipendente dell'Istituto "Incaricato del trattamento".

8. Rientrano tra i principali compiti in capo all'Incaricato quelli di:
 - a) utilizzare esclusivamente i dati necessari per svolgere le attività operative cui è preposto l'Ufficio di appartenenza;
 - b) osservare le istruzioni operative impartite dal Titolare/Responsabile;
 - c) informare prontamente il proprio Responsabile del trattamento di ogni questione rilevante ai fini della legge, così da poter individuare, con il supporto delle strutture competenti, le azioni necessarie per garantire la corretta applicazione delle disposizioni legislative;

- d) se Incaricati esterni, svolgere le attività assegnate con gli stessi accorgimenti previsti per l'Incaricato interno ed operare sotto la diretta autorità del Responsabile secondo istruzioni formalizzate.
9. Una particolare categoria di Incaricati sono gli Amministratori di sistema, ovvero le figure professionali dedicate alla gestione e alla manutenzione di sistemi informatici con cui vengono effettuati trattamenti di dati personali; gli stessi sono designati dal Titolare o dal Responsabile con atto formale.

Art. 5. Il Responsabile della protezione dei dati personali (Data Protection Officer)

1. Il Titolare, ai sensi dell'art. 37 del GDPR EU 2016/679, designa con atto ufficiale il Responsabile della Protezione dei dati personali (Data Protection Officer) allo scopo di collaborare alla gestione degli adempimenti privacy.
2. In particolare, il Responsabile della Protezione dei Dati personali (Data Protection Officer) è preposto a:
 - a) informare e fornire consulenza al Titolare del trattamento o al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni nazionali, dell'Unione o degli Stati membri relative alla protezione dei dati;
 - b) sorvegliare sull'osservanza del Regolamento EU 2016/679, di altre disposizioni nazionali, dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare del trattamento o del Responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
 - c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
 - d) cooperare con l'autorità di controllo;
 - e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.
3. L'Istituto, in qualità di Titolare del trattamento, ai sensi dell'art. 38, paragrafo 6 del GDPR EU 2016/679, garantisce che i compiti e le funzioni assegnati al Responsabile della Protezione dei Dati personali (Data Protection Officer) non diano adito a conflitto di interessi.

Art. 6. Circolazione dei dati nell'ambito dell'Istituto



1. L'accesso ai dati personali da parte di strutture e/o di dipendenti dell'Istituto, che sia strettamente connesso allo svolgimento dell'attività del richiedente, deve essere soddisfatto in via diretta e senza alcuna formalità, nella misura strettamente necessaria, pertinente e non eccedente al perseguimento dell'interesse istituzionale.
2. Laddove l'accesso sia finalizzato ad un utilizzo ulteriore e/o diverso dei dati, i soggetti - di cui al primo comma - devono presentare richiesta scritta e motivata al Titolare o Responsabile che potrà concedere l'autorizzazione solo dopo aver valutato la compatibilità della richiesta con i fini istituzionali dell'Istituto e il consenso dell'interessato.
3. Per tutto quanto non espressamente disposto, si rinvia alle prescrizioni di cui alla L. 7 agosto 1990 n. 241 *Nuove norme sul procedimento amministrativo* e del Decreto legislativo 14 marzo 2013, n. 33 *Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*.

Art. 7. Circolazione dei dati fuori dell'ambito dell'Istituto

1. La comunicazione ed il **trasferimento** dei dati personali da parte dell'Istituto sono permesse qualora:
 - a) siano previste da norme di legge, di regolamento o dalla normativa comunitaria;
 - b) siano necessarie per finalità di ricerca scientifica o di statistica e si tratti di dati anonimi;
 - c) siano richieste da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati, con l'osservanza delle norme che regolano la materia;
 - d) siano state espressamente autorizzate dagli interessati.
2. Al di fuori dei casi sopra esposti, l'eventuale richiesta rivolta all'Istituto e finalizzata a ottenere il trattamento, la comunicazione o la diffusione dei dati personali, dovrà essere formulata per iscritto, adeguatamente motivata e contenere le seguenti informazioni:
 3. il nome, la denominazione o la ragione sociale del richiedente;
 - a) i dati cui la domanda si riferisce e le finalità nonché le modalità di utilizzo degli stessi;
 - b) l'eventuale ambito di comunicazione e diffusione dei dati richiesti;
 - c) la dichiarazione che il richiedente si impegna ad utilizzare i dati ricevuti esclusivamente per le finalità e nell'ambito delle modalità per cui sono stati richiesti.

3. Il Titolare o il Responsabile competente, dopo aver valutato che il trattamento, la comunicazione o la diffusione dei dati sono compatibili con i fini istituzionali dell'Istituto, provvede - nel rispetto delle norme stabilite dal GDPR EU 2016/679 in materia di comunicazione e diffusione dei dati personali - alla trasmissione degli stessi nella misura e secondo le modalità strettamente necessarie a soddisfare la richiesta.

Art. 8. Trattamento di categorie particolari di dati

1. È vietato trattare dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, come pure trattare dati relativi alla salute e alla vita sessuale.
2. Il comma 1 non si applica quando:
 - a) l'interessato ha dato il proprio consenso esplicito a tale trattamento;
 - b) il trattamento risulta necessario per salvaguardare un interesse vitale dell'interessato, di un terzo o della collettività, qualora l'interessato si trovi nell'incapacità fisica o giuridica di dare il proprio consenso;
 - c) il trattamento riguarda dati resi manifestamente pubblici dall'interessato o è necessario per accertare, esercitare o difendere un diritto in via giudiziale;
 - d) in tutte le ipotesi espressamente previste dalla vigente normativa.
3. Il comma 1 non si applica quando il trattamento dei dati è necessario in ambito medico per finalità di prevenzione, diagnosi, assistenza sanitaria o terapia ovvero gestione di centri di cura, e quando il trattamento dei medesimi dati è effettuato da un professionista della sanità vincolato al segreto professionale o da un'altra persona soggetta a un equivalente obbligo di segretezza.

Art. 9. Responsabilità

1. Il soggetto che, nell'adempimento delle proprie mansioni, richiede, riceve, tratta, o semplicemente ha notizia di dati è vincolato al rispetto del segreto d'ufficio.
2. Nell'ambito delle responsabilità connesse con la posizione ricoperta e le funzioni svolte, si richiama la responsabilità relativa alla mancata vigilanza sull'attività degli Incaricati al trattamento dei dati.
3. La responsabilità, espressamente prevista dal GDPR EU 2016/679 per un eventuale uso non corretto dei dati personali, è a carico della singola persona, Titolare, Responsabile (interno ed esterno), Amministratore di sistema cui l'uso illegittimo sia riferibile.

Art. 10. Modalità di raccolta e requisiti dei dati personali

1. I dati personali oggetto di trattamento devono essere:

- a) trattati in modo lecito e secondo correttezza;
 - b) raccolti per finalità determinate, esplicite e legittime, e utilizzati in altre operazioni del trattamento in termini non incompatibili con tali finalità;
 - c) esatti e, se necessario, aggiornati;
 - d) adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono raccolti o successivamente trattati;
 - e) conservati in modo da consentire l'identificazione degli interessati per un arco di tempo non superiore a quello necessario per il conseguimento delle finalità per le quali sono raccolti o successivamente trattati.
2. Il trattamento dei dati personali ai fini di ricerca scientifica o storica o a fini statistici è effettuato nel rispetto di adeguate garanzie per i diritti e le libertà dell'interessato, in conformità alle norme previste dall'art. 89 del GDPR EU 2016/679.

Art. 11. Comunicazione e censimento degli archivi automatizzati e cartacei

1. Chi intraprende un nuovo trattamento di dati o cessa un trattamento già esistente nell'ambito delle strutture dell'Istituto, o per conto dello stesso, deve comunicarlo al Titolare o al Responsabile.
2. Nella comunicazione dovranno essere indicate:
 - a) le finalità e le modalità del trattamento;
 - b) la natura dei dati, il luogo dove vengono custoditi, le categorie di interessati cui i dati si riferiscono nonché la lista nominativa dei responsabili e degli Incaricati del trattamento autorizzati ad operare sui dati medesimi;
 - c) l'ambito di comunicazione e diffusione dei dati;
 - d) gli eventuali trasferimenti di dati previsti verso Paesi non appartenenti all'Unione Europea o, qualora si tratti di dati relativi alla salute e di dati relativi ai provvedimenti di cui all'art. 686 c.p.p., fuori dal territorio nazionale;
 - e) una descrizione delle misure di sicurezza adottate;
 - f) l'eventuale connessione con altri trattamenti o banche dati.

Art. 12. Diritti dell'interessato

1. All'interessato, i cui dati siano in possesso dell'Istituto, spettano i diritti di cui agli artt. 15, 16, 17, 18, e 21 del GDPR EU 2016/679, ovvero di ottenere, a cura del Titolare o del Responsabile, senza ritardo:
 - a) la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati e la comunicazione in forma intelligibile dei medesimi dati, della

loro origine, della finalità e modalità del trattamento, della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici, degli estremi identificativi del Titolare, dei Responsabili e dei soggetti o delle categorie ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di Responsabili o Incaricati; la richiesta può essere rinnovata, salva l'esistenza di giustificati motivi, con intervallo non minore di novanta giorni;

- b) la cancellazione dei dati e/o la limitazione del trattamento dei dati qualora ricorrano i presupposti previsti dal GDPR EU 2016/679;
 - c) l'aggiornamento, la rettificazione ovvero, qualora vi abbia interesse, l'integrazione dei dati;
 - d) l'attestazione che le operazioni di cui alle lettere b) e c) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si riveli impossibile o comporti un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato;
 - e) di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
 - f) di opporsi, in tutto o in parte, al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.
2. Per le richieste volte ad ottenere la conferma dell'esistenza o meno di dati personali relativi all'interessato, alla loro origine, alle finalità e modalità del trattamento o alla logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici, può essere chiesto all'interessato stesso, ove non risulti confermata l'esistenza di dati che lo riguardano, un contributo spese, non superiore ai costi effettivamente sopportati per la ricerca effettuata nel caso specifico.
3. L'interessato può esercitare tali diritti con una richiesta indirizzata senza formalità al Titolare o al Responsabile, anche per il tramite di un Incaricato, alla quale deve essere fornito un idoneo riscontro senza ritardo. La richiesta sarà ritenuta valida anche se effettuata da persone terze, enti, associazioni od organismi muniti di delega o procura scritta dell'interessato.

Art. 13. Modifiche e rinvio

- 1. Eventuali modifiche o integrazioni al presente regolamento, nel rispetto della normativa vigente in materia, vengono deliberate dal Consiglio di Amministrazione dell'Istituto.
- 2. Per tutto quanto non espressamente disciplinato nel presente regolamento, si rinvia alla vigente legislazione nazionale e comunitaria.

