REGOLAMENTO PER LA PROTEZIONE DEI DATI PERSONALI

Approvato dal Consiglio di Amministrazione con delibera n. 25 del 19 settembre 2019

1. Introduzione

1. Il presente Regolamento disciplina le modalità di protezione dei dati personali da parte della Fondazione Patrimonio Ca' Granda (la "Fondazione" o "Fondazione Patrimonio"), in conformità al Regolamento UE n. 679/2016 (di seguito il "Regolamento UE") e alla normativa nazionale quale il d. lgs. n. 196/2016 come modificato dal d. lgs. 101/2018.
2. Il presente Regolamento non preclude l'attuazione del diritto di accesso come disciplinato dal *Regolamento sull'accesso agli atti* della Fondazione.

2. Definizioni

- *Trattamento dei dati personali*: 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.
- *Dati personali*: 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.
- *Categorie particolari di dati personali*: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
- *Interessato*: la persona fisica i cui dati personali sono oggetto di trattamento, identificata o identificabile.
- *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.
- *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.
- *Incaricato del trattamento*: persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile
- *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.
- *Garante*: il Garante è l'autorità di controllo designata anche ai fini dell'attuazione del Regolamento UE ai sensi del d. lgs. 10 agosto 2018, n. 101.

3. Principi

1. Il Trattamento di dati personali deve avvenire nel rispetto dei principi fissati dall'art. 5 del Regolamento UE, di seguito sinteticamente richiamati:
   a) liceità, correttezza e trasparenza;
   b) limitazione della finalità;

c) minimizzazione dei dati;
d) esattezza;
e) limitazione della conservazione;
f) integrità e riservatezza.

2. Il Trattamento dei dati personali è ammesso quando ricorre una delle condizioni previste dall'art. 6 del Regolamento UE, di seguito sinteticamente richiamate:
   a) l'Interessato ha espresso il consenso al Trattamento dei propri dati personali per una o più specifiche finalità;
   b) il Trattamento è necessario all'esecuzione di un contratto di cui l'Interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
   c) il Trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento;
   d) il Trattamento è necessario per la salvaguardia degli interessi vitali dell'Interessato o di un'altra persona fisica;
   e) il Trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
   f) il Trattamento è necessario per il perseguimento del legittimo interesse del Titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'Interessato che richiedono la protezione dei dati personali, in particolare se l'Interessato è un minore.
3. Il Consenso di cui alla lett. a) del precedente paragrafo deve essere espresso mediante un atto positivo inequivocabile, con il quale l'Interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il Trattamento dei dati personali che lo riguardano. Pertanto, il Consenso dell'Interessato è valido solo nel caso in cui:
   a) sia stato espresso dall'Interessato liberamente e in modo inequivocabile;
   b) sia stata resa all'Interessato l'informazione sul Trattamento dei dati personali;
   c) sia stato espresso dall'Interessato specificamente a ciascuna finalità, qualora il Trattamento ne preveda più d'una.
4. Il Consenso è ammesso solo in forma scritta, ritenuta l'unica modalità idonea a configurare l'inequivocabilità del consenso e il relativo carattere esplicito, ed è pertanto vietata ogni forma tacita o presunta, ad esempio, attraverso l'utilizzo di moduli precompilati.
5. Qualora il Trattamento dei dati personali avvenga per finalità diverse da quelle per le quali erano stati inizialmente raccolti, la Fondazione lo comunica tempestivamente all'Interessato che può avvalersi, tra l'altro, del diritto di opposizione. In ogni caso, prima di procedere al nuovo Trattamento, la Fondazione verifica la sussistenza di una condizione di legittimità.
6. Il Trattamento di Categorie particolari di dati personali è ammesso quando ricorre una delle condizioni previste dall'art. 9 del Regolamento UE, di seguito sinteticamente richiamate:
   a) l'Interessato ha prestato il proprio consenso esplicito;
   b) il Trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del Titolare del trattamento o dell'Interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;
   c) il Trattamento è necessario per tutelare un interesse vitale dell'Interessato o di un'altra persona fisica qualora l'Interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
   d) il Trattamento è effettuato da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il Trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti

con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'Interessato;

e) il Trattamento riguarda dati personali resi manifestamente pubblici dall'Interessato;
f) il Trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
g) il Trattamento è necessario per motivi di interesse pubblico rilevante;
h) il Trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali;
i) il Trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica;
j) il Trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1.

7. Il Trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza può avvenire solo se autorizzato dalla legge o sotto il controllo dell'autorità pubblica, ai sensi dell'art. 10 del Regolamento UE.

4. I Diritti dell'Interessato

1. Sono diritti dell'Interessato:
   a) l'accesso, la rettifica e la cancellazione dei propri dati personali;
   b) la limitazione del Trattamento;
   c) la portabilità dei dati;
   d) il diritto di opposizione.
2. L'Interessato ha diritto a ricevere una risposta alla propria richiesta, che deve essere resa: in forma scritta, anche attraverso strumenti elettronici; in modo intelligibile, conciso, trasparente e facilmente accessibile; utilizzando un linguaggio semplice e chiaro; entro il termine di 30 giorni, estendibile fino a 90 giorni in casi di particolare complessità, previo preliminare riscontro entro 30 giorni; motivando l'eventuale mancato accoglimento della richiesta.
3. L'Interessato ha il diritto di ottenere gratuitamente quanto richiesto alla Fondazione, fatto salvo il caso in cui:
   a) l'Interessato richieda più di una copia dei dati personali, in forma cartacea o elettronica;
   b) la Fondazione dimostri il carattere infondato e/o eccessivo e/o ripetitivo della richiesta.

   L'entità del contributo viene determinato dalla Fondazione secondo un criterio di ragionevolezza ed appropriatezza.
4. L'Interessato ha il diritto di ottenere la cancellazione dei dati personali che lo riguardano quando ricorre una delle condizioni previste dall'art. 17 del Regolamento UE, di seguito sinteticamente richiamate:
   a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
   b) l'Interessato revoca il consenso su cui si basa il Trattamento conformemente all'art. 6, par. 1, lett. a), o all'art. 9, par. 2, lett. a) del Regolamento UE, e se non sussiste altro fondamento giuridico per il Trattamento;
   c) l'Interessato si oppone al Trattamento ai sensi dell'art. 21, par. 1 Regolamento UE, e non sussiste alcun motivo legittimo prevalente per procedere al Trattamento, oppure si oppone al Trattamento ai sensi dell'art. 21, par. 2 del Regolamento UE;
   d) i dati personali sono stati trattati illecitamente;

e) i dati personali devono essere cancellati per adempiere un obbligo giuridico previsto dalla legge, cui è soggetto il Titolare del trattamento;
f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'art. 8, par. 1 del Regolamento UE.

Verificata la sussistenza di una delle condizioni di legge, la Fondazione provvede alla cancellazione dei dati su qualsiasi supporto archiviati e, se del caso, informa della richiesta pervenuta gli altri Titolari cui ha trasmesso i dati, invitandoli a rimuovere ogni copia degli stessi.

5. L'Interessato ha il diritto di ottenere la limitazione del Trattamento quando ricorre una delle condizioni previste dall'art. 18 del Regolamento UE, di seguito sinteticamente richiamate:
   a) l'Interessato contesta l'esattezza dei dati personali, per il periodo necessario al Titolare del trattamento per verificare l'esattezza di tali dati personali;
   b) il Trattamento è illecito e l'Interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
   c) il Titolare del trattamento non ha più bisogno i dati personali ai fini del Trattamento, ma sono necessari all'Interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
   d) l'Interessato si è opposto al Trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del Titolare del trattamento rispetto a quelli dell'Interessato.

5. L'Informativa

1. La Fondazione procede al Trattamento dei dati solo dopo aver fornito apposita Informativa all'Interessato che va resa entro i seguenti termini:
   a) quando i dati sono raccolti presso l'Interessato, contestualmente alla loro acquisizione;
   b) quando i dati non sono raccolti presso l'Interessato, entro 30 giorni; oppure, nel caso siano destinati alla comunicazione con l'Interessato, al momento della prima comunicazione; oppure, nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.
2. L'Informativa fornita deve riportare le seguenti informazioni:
   a) l'identità ed i dati di contatto del Titolare del trattamento;
   b) le finalità e la base giuridica del Trattamento;
   c) gli eventuali destinatari dei dati;
   d) il periodo di conservazione;
   e) i diritti riconosciuti all'Interessato dalla normativa vigente.

6. La conservazione dei dati

1. I dati personali sono conservati presso gli uffici della Fondazione in archivi dedicati, di tipo elettronico e/o cartacei, il cui accesso è disciplinato da specifiche misure di sicurezza finalizzati alla protezione dei dati.
2. Gli archivi elettronici sono costituiti da cartelle digitali create sul server, il cui accesso può avvenire esclusivamente mediante password individuale che deve soddisfare determinati criteri di complessità, la cui validità è di 90 giorni e non può essere riutilizzata. L'accesso agli archivi cartacei è protetto da serratura.
3. L'assegnazione dei titoli di accesso agli archivi ai singoli Incaricati del trattamento (password e/o chiave) è autorizzata dal Titolare del trattamento. L'accesso agli archivi da parte di soggetti diversi dagli Incaricati del trattamento deve essere debitamente autorizzato dal Titolare del trattamento.
4. I tempi di conservazione dei dati sono determinati tenendo conto, tra gli altri, dei seguenti criteri:
   a) finalità di utilizzo;

b) interesse legittimo e/o diritto del Titolare del trattamento o di un terzo;
c) interesse legittimo e/o diritto dell'Interessato;
d) tipologia e/o entità del servizio/attività offerta all'Interessato.

5. I termini di conservazione, definiti sulla base dei criteri sopra elencati, sono riportati nel Registro dei Trattamenti e individuati in ciascun modello di informativa.

7. Titolare, Incaricato e Responsabile del trattamento

1. Il Titolare del trattamento è la Fondazione, cui spetta l'obbligo di garantire e dimostrare che il Trattamento viene effettuato in conformità al Regolamento UE attraverso misure tecniche e organizzative proposte dal Direttore generale e attuate dall'Incaricato del trattamento.
2. L'Incaricato del trattamento è ogni dipendente la cui mansione organizzativa richiede la gestione di dati personali: le relative modalità di Trattamento sono disciplinate nell'atto di nomina, in conformità al presente Regolamento.
3. Il Responsabile del trattamento è ogni fornitore di beni e servizi che svolge l'attività di Trattamento per conto della Fondazione. Il Responsabile del trattamento deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del Regolamento UE. L'esecuzione del Trattamento da parte del Responsabile del trattamento è disciplinata da un atto di nomina in cui siano indicati: la materia disciplinata; la durata, la natura e le finalità del Trattamento; il tipo di dati personali; le categorie di Interessati; gli obblighi e i diritti del Titolare del trattamento.

8. L'amministratore di sistema

1. L'amministratore di sistema è la figura professionale cui compete la gestione del sistema informatico e chiunque abbia la possibilità di accedere in modo privilegiato a risorse del sistema informativo e a dati personali cui non si è legittimati ad accedere rispetto ai profili di autorizzazione attribuiti.
2. L'Amministratore di sistema è identificato da specifico atto di nomina che disciplina gli obblighi in materia di protezione di dati personali.

9. Il registro dei trattamenti

1. La Fondazione istituisce un Registro delle attività di Trattamento svolte sotto la propria responsabilità che, in conformità al modello pubblicato dal Garante, contiene le seguenti informazioni:
   a) il nome e i dati di contatto del Titolare del trattamento;
   b) le finalità del Trattamento;
   c) le categorie dei soggetti interessati e le categorie dei dati personali trattati;
   d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
   e) i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
   f) una descrizione generale delle misure di sicurezza tecniche e organizzative;
   g) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale.

10. La valutazione d'impatto della protezione dei dati

1. Nel caso in cui si tratti una tipologia di dati che, consideratane la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, è obbligatorio effettuare, prima di procedere al trattamento, una valutazione d'impatto privacy (DPIA). Il suddetto rischio deve essere misurato con criteri oggettivi che permettano di individuare i trattamenti a rischio nonché quelli a rischio elevato, in termini di probabilità e gravità le cui grandezze

devono essere determinate con attenzione a natura, ambito di applicazione, contesto e finalità di trattamento.

2. In assenza di indicazioni normative o regolamentari circa la metodologia da adottare per la misurazione del rischio, la Fondazione definisce un processo di valutazione e gestione del rischio privacy sulla base di quanto previsto: dai *Considerando* del GDPR; dalle *Linee Guida WP248rev.1* adottate in materia dal Gruppo WP29; dall'Allegato 1 al *Provvedimento n. 467 dell'11 ottobre 2018* del Garante privacy italiano.
3. Il processo per la valutazione d'impatto viene disciplinato e attuato dal Direttore generale, tenuto conto delle proposte tecniche elaborate dagli uffici preposti.

11. Violazione dei dati personali

1. La violazione dei dati personali o *data breach* consiste in una violazione degli standard di sicurezza adottati per la protezione dei dati personali tale da comportare la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trattati.
2. Nel caso in cui il Titolare del trattamento ritenga che ne derivino rischi per i diritti e le libertà degli interessati, la Fondazione procede alla notifica della violazione al Garante entro 72 ore dal momento in cui ne è stata presa conoscenza nonché alla comunicazione all'Interessato con indicata la natura della violazione e le raccomandazioni finalizzate ad attenuare i potenziali effetti negativi.
3. La Fondazione documenta ogni violazione subita, anche nel caso non siano causa di rischi per i diritti e le libertà degli interessati, specificando circostanze, conseguenze e provvedimenti adottati, segnalando l'evento nel Registro dei trattamenti.

12. La formazione in materia di Privacy

1. La Fondazione prevede la formazione continua e obbligatoria del personale nominato Incaricato del trattamento finalizzata a una corretta e tempestiva attuazione delle misure tecniche e organizzative previste per la protezione dei dati personali nonché delle disposizioni previste dal presente Regolamento.

13. Disposizioni finali

Il presente Regolamento entra in vigore il giorno successivo alla sua approvazione da parte del Consiglio di Amministrazione ed è pubblicato sul sito internet della Fondazione.