MODELLO DI ORGANIZZAZIONE PRIVACY

Approvato dal Consiglio di amministrazione con delibera n. 115 del 06.04.2023

Indice:

PREMESSA

Il presente Modello di Organizzazione Privacy ("MOP") è il documento utilizzato dalla Fondazione Patrimonio Ca' Granda (di seguito anche "Fondazione" o "Titolare") per descrivere le misure tecniche e organizzative adottate al fine di garantire un livello di sicurezza adeguato al rischio connesso al trattamento dei dati effettuato dal Titolare ai sensi dell'art. 32 del Regolamento Europeo n. 679/2016 (di seguito anche "GDPR" o "Regolamento").

Il presente Documento è finalizzato a recepire in un unico testo gli adempimenti richiesti da tutta la normativa in materia di protezione dei dati personali (il Regolamento, le Linee guida del Garante italiano per la protezione dei dati personali - di seguito "Garante Privacy" - e dei Garanti Europei, nonché la normativa nazionale in materia di protezione dei dati personali).

Il MOP contiene, altresì, specifiche indicazioni relative alla produzione, gestione, conservazione e trasmissione dei dati personali, con peculiare attenzione a quelli di tipo elettronico/informatico, che per loro natura risultano particolarmente critici.

Il MOP è un documento in continua evoluzione che deve essere aggiornato laddove intervengano modifiche normative in materia di protezione dei dati personali, cambiamenti organizzativi interni alla Fondazione che comportino modifiche alle procedure e istruzioni contenute nel Modello o all'Organigramma Privacy, nonché nei casi in cui la Fondazione modifichi le proprie misure di sicurezza tecniche e organizzative.

Il MOP è inoltre sottoposto ad aggiornamento periodico, al fine di perseguire costantemente la piena conformità dello stesso alla normativa vigente, alle pronunce giurisprudenziali e alle pronunce del Garante Privacy.

PARTE GENERALE

1. RIFERIMENTI NORMATIVI E DOCUMENTALI

Il Modello di Organizzazione Privacy di Fondazione Patrimonio Ca' Granda è stato redatto in modo da garantire la puntuale applicazione:

- del Regolamento Europeo n. 679/2016 (di seguito anche "GDPR");
- delle Linee Guida adottate dal Gruppo WP29 in relazione alla corretta applicazione del Regolamento Europeo n. 679/2016;
- del Codice in materia di protezione dei dati personali, Decreto legislativo 30 giugno 2003, n. 196 (anche, di seguito, "Codice Privacy"), come modificato dal D. Lgs. 101 del 2018;
- dei successivi provvedimenti emanati dal Garante per la protezione dei dati personali, tra cui in particolare:
    - Provvedimento del Garante Privacy del 23 novembre 2006 in materia di trattamento dei dati personali dei lavoratori con riferimento alla gestione del rapporto di lavoro;
    - Provvedimento del Garante Privacy del 27 novembre 2008 e successive modificazioni relativamente agli Amministratori di Sistema;
    - Provvedimento del Garante Privacy del 29 aprile 2010 in materia di videosorveglianza;
- delle linee guida emanate dall'*European Data Protection Board* e delle decisioni della Commissione Europea, quali, ad esempio:
    - Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video;
    - Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data adottate il 18 giugno 2021;
    - Decisione di esecuzione (UE) 2021/914 della Commissione del 4 giugno 2021 relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio;
    - Decisione di esecuzione (UE) 2021/915 della Commissione del 4 giugno 2021 relativa alle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento a norma dell'articolo 28, paragrafo 7, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio e dell'articolo 29, paragrafo 7, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio.

2. PRINCIPI CHE REGOLANO IL TRATTAMENTI DEI DATI

Nello svolgimento di ogni attività di trattamento dei dati, la Fondazione opera in conformità ai seguenti principi sanciti dalla normativa nazionale e comunitaria.

- Liceità, correttezza e trasparenza

ARTICOLO 5, PAR. 1, LETT. A) REG. UE/679/2016

❖ Cfr. Considerando 39, 40, 44 Reg. UE/679/2016

"I dati personali sono … trattati in modo lecito, corretto e trasparente nei confronti dell'interessato".

La Fondazione si impegna ad eseguire esclusivamente trattamenti leciti ai sensi della normativa nazionale ed europea. Pertanto, il Titolare tratta dati personali esclusivamente previa raccolta del consenso da parte dell'Interessato del trattamento o, in alternativa, a seconda dei casi, in forza delle diverse basi giuridiche previste dagli artt. 6 e 9 GDPR.

La Fondazione assicura, inoltre, la trasparenza dei trattamenti eseguiti, con particolare riferimento alle finalità e modalità del trattamento, attraverso la diffusione di informative facilmente accessibili, comprensibili e redatte con linguaggio chiaro e semplice.

- Limitazione della finalità

ARTICOLO 5, PARAGRAFO 1, LETT. B), REG. UE/679/2016

❖ Cfr. Considerando 28, 50 e articolo 6, par. 1, lett. b) Reg. UE/679/2016

"I dati personali sono … raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali".

La Fondazione predefinisce le finalità di ogni trattamento eseguito e le esplicita, fin dal momento della raccolta del dato, all'interno dell'informativa consegnata all'Interessato e nella sezione dedicata del Registro. In ogni caso, il Titolare raccoglie dati personali solo se strettamente necessari al perseguimento di tali finalità.

Inoltre, nel caso di nuova finalità, la Fondazione valuta in modo sostanziale e non meramente formale la compatibilità del fine ulteriore rispetto a quello per cui i dati sono stati raccolti, sulla base di parametri quali i) la ragionevole aspettativa dell'Interessato rispetto ai trattamenti futuri, anche considerando la relazione tra questo e il Titolare, ii) la sede di raccolta dei dati, iii) le garanzie disponibili al fine di ridurre l'impatto dell'ulteriore trattamento sulla sfera privata dell'Interessato

- Minimizzazione dei dati

ARTICOLO 5, PARAGRAFO 1, LETT. C), REG. UE/679/2016

❖ Cfr. articolo 25, paragrafo 2, Reg. UE/679/2016

"I dati personali sono … adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati".

La Fondazione raccoglie i dati funzionali ed essenziali al perseguimento delle finalità per cui il dato è trattato. Il trattamento non è eseguito in tutti i casi in cui le medesime finalità sono realizzabili mediante dati anonimi o altre modalità che rendano non determinabile l'identità dell'Interessato.

Inoltre, la Fondazione ha definito e formalizzato diversi livelli autorizzativi per ogni funzione aziendale. Pertanto, ogni soggetto autorizzato al trattamento dei dati può accedere esclusivamente alle categorie di dati essenziali per lo svolgimento della propria mansione lavorativa.

- Esattezza dei dati

ARTICOLO 5, PARAGRAFO 1, LETT. D), REG. UE/679/2016

"I dati personali sono … esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto allefinalità per le quali sono trattati".

La Fondazione effettua specifiche verifiche atte ad accertare l'esattezza dei dati dalla raccolta del dato fin alla sua cancellazione, e riconosce ad ogni Interessato la possibilità di esercitare in modo immediato il proprio diritto di rettifica ed aggiornamento. A tal fine, durante il trattamento dei dati, il Titolare effettua verifiche periodiche atte ad accertare la correttezza dei dati originariamente raccolti.

- Limitazione della conservazione

ARTICOLO 5, PARAGRAFO 1, LETT. E), REG. UE/679/2016

❖ Cfr. Considerando 39 e articolo 89 Reg. UE/679/2016

"I dati personali sono … conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato".

La Fondazione ha definito i tempi di conservazione di ogni tipologia di dato personale trattato. I tempi di conservazione sono stati definiti in base alla finalità per cui il dato è trattato, coerentemente ai vigenti obblighi contrattuali e normativi.

- Integrità e riservatezza

ARTICOLO 5, PARAGRAFO 1, LETT. F), REG. UE/679/2016

❖ Cfr. Considerando 39 Reg. UE/679/2016

"I dati personali sono … trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali".

La Fondazione ha adottato tutte le misure, tecniche e organizzative, ritenute idonee a salvaguardare la correttezza del processo di raccolta e gestione dei dati, la loro sicurezza e protezione in caso di intrusioni e alterazioni non autorizzate.

- Principio di *Accountability*

ARTICOLO 24, REG. UE/679/2016

❖ Cfr. Considerando 74 Reg. UE/679/2016

"Il Titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed esserein grado di dimostrare la conformità delle attività di trattamento al Regolamento, compresa l'efficacia delle misure".

La Fondazione ha implementato un sistema di gestione del rischio privacy, individuando i rischi connessi al trattamento, valutando tali rischi in termini di origine, natura, probabilità e gravità, nonché individuando le migliori prassi per attenuare il rischio.

- *Privacy by design* e *by default*

ARTICOLO 25, REG. UE/679/2016

❖ Cfr. Considerando 78 Reg. UE/679/2016

"Il Titolare del trattamento, al fine di dimostrare la conformità con il presente regolamento, dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei datifin dalla progettazione e della protezione dei dati di default".

La Fondazione ha implementato un sistema di gestione privacy atto a perseguire la piena tutela dei dati trattati fin dal momento precedente all'avvio del trattamento.

A tal fine, il Titolare – al momento di definizione dei mezzi del trattamento – valuta lo stato dell'arte, i costi di attuazione, la natura, l'ambito di applicazione, il contesto e le finalità del trattamento, i possibili rischi ad esso connessi e le correlate gravità e probabilità, nonché ogni altro elemento ritenuto utile, al fine di condurre un'analisi appropriata ed adottare scelte operative che siano idonee a garantire la tutela dei dati trattati.

Tali misure saranno aggiornate ogniqualvolta si renda necessario adottare un nuovo processo organizzativo o nuovo sistema informatico nonché nel caso di utilizzo di nuove tecnologie.

Ancora, attraverso la loro applicazione ed il loro periodico aggiornamento, la Fondazione si impegna affinché per impostazione predefinita saranno oggetto di trattamento solo i dati personali necessari in relazione a ciascuna finalità specifica e che la quantità dei dati raccolti e la durata della loro conservazione non eccedano il minimo necessario per le finalità perseguite.

3. I SOGGETTI COINVOLTI NEL TRATTAMENTO DEI DATI

Il GDPR delinea un sistema composto da più figure, ognuna caratterizzata da una diversa ampiezza di poteri e responsabilità, modulati in relazione al ruolo assegnato e alle attività concretamente svolte con riferimento al trattamento delle categorie di dati personali.

La corretta individuazione di tali figure assume, infatti, un ruolo cruciale per la tenuta e l'efficienza del sistema privacy della Fondazione.

Il **Titolare del trattamento** (art. 24 Regolamento) è la Fondazione – considerata nel suo complesso quale persona giuridica – che determina le finalità e modalità del trattamento dei dati, nonché misure tecniche ed organizzative da adottare con riferimento a tutte le operazioni di trattamento eseguite.

Fondazione Patrimonio Ca' Granda – tramite le proprie risorse – in quanto Titolare del trattamento provvede a:

- definire le modalità e finalità dei trattamenti eseguiti e le categorie di dati trattati;
- adottare tutte le misure tecniche ed organizzative necessarie per garantire la sicurezza dei dati trattati;
- verificare ed aggiornare periodicamente le misure tecniche ed organizzative adottate;
- scegliere consapevolmente i soggetti coinvolti nel trattamento dei dati ed istruirli adeguatamente;
- in caso di violazioni, attuare contro-misure tempestive ed effettive ed effettuare le comunicazioni dovute ai sensi di legge.

Con riferimento a specifici trattamenti, la Fondazione condivide la decisione in merito alle finalità ed ai mezzi del trattamento con altri soggetti che operano quali autonomi Titolari del trattamento, assumendo così la posizione di **Contitolari del trattamento**.

Tutte le situazioni di contitolarità sono formalmente disciplinate attraverso appositi accordi, in cui trovano puntuale esplicazione e definizione i ruoli reciproci e il riparto degli obblighi.

La Fondazione, ove ne ricorrano i presupposti, provvede ad informare gli Interessati sul contenuto di tale accordo: la dichiarazione del rapporto di contitolarità e le informazioni essenziali sullo stesso sono fornite con l'informativa resa al momento di avvio del trattamento, informazioni più approfondite sul contenuto dell'accordo sono rese su richiesta dell'Interessato.

In ogni caso, gli enti coinvolti provvedono ad informare tempestivamente l'Interessato nel caso di modifiche all'accordo che ne riguardino il contenuto essenziale o che incidano su aspetti della sfera giuridica dell'Interessato stesso.

L'elenco delle contitolarità in cui la Fondazione è coinvolta e gli accordi di contitolarità stipulati sono conservati in apposito *database* digitale a cura del Responsabile dell'Ufficio Affari Legali e *Compliance*.

La Fondazione ha formalmente individuato nel Responsabile dell'Ufficio Affari Legali e *Compliance* il proprio **Referente Privacy.**

Il Referente ha il compito di:

- informare e fornire supporto al Titolare del trattamento, nonché ai dipendenti che eseguono il trattamento, in merito agli obblighi derivanti dal GDPR, nonché da altre disposizioni nazionali o dell'Unione relative alla protezione dei dati;
- sorvegliare l'osservanza del GDPR, di altre disposizioni nazionali o dell'Unione relative alla protezione dei dati nonché delle politiche del Titolare 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;
- comunicare tempestivamente al Titolare ogni inadeguatezza del sistema privacy aziendale di cui abbia conoscenza, nonché ogni comportamento od evento che possa determinare una violazione della normativa legislativa ed aziendale vigente ed ogni circostanza idonea a determinare – anche solo potenzialmente – una violazione dei dati personali trattati dalla Fondazione;
- curare le attività di valutazione dei rischi correlati ai trattamenti di dati eseguiti dal Titolare e, ove necessario, lo svolgimento della valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35 GDPR;
- supportare il Titolare nelle relazioni con il Garante per la protezione dei dati personali;
- segnalare al Titolare la necessità di avvalersi di un supporto di tipo tecnico, anche di natura esterno, nell'ambito dello svolgimento dei compiti assegnati;
- supportare il Titolare nella compilazione e nell'aggiornamento dei Registri dei trattamenti ex art. 30 GDPR;
- suggerire al Titolare l'adozione, in piena autonomia, di tutte le iniziative e degli interventi idonei a garantire il rispetto delle statuizioni della normativa vigente in materia di protezione dei dati personali, garantendo che il trattamento sia strettamente connesso con il perseguimento degli obiettivi aziendali e di quanto comunicato all'interessato al momento della raccolta dei dati;
- supportare il Titolare nelle attività di nomina di eventuali Responsabili interni nonché nell'individuazione e nella nomina dei soggetti incaricati del trattamento ex art. 29 GDPR;
- fornire supporto ad ogni soggetto incaricato del trattamento per l'analisi e la risoluzione di dubbi/difficoltà connesse al trattamento dei dati;
- coordinarsi e fornire supporto alle funzioni aziendali per tutte le iniziative, prese o da prendere, per garantire un livello adeguato di protezione dei dati personali e tutelare i diritti degli interessati.

Il Titolare, con il supporto del Referente Privacy, ha altresì individuato nei Responsabili di Funzione i cd. **Responsabili Interni**, i quali agiscono come *focal point* per tutte le questioni inerenti alla tematica privacy all'interno della propria area di competenza e responsabilità.

I compiti del Responsabili Interni sono i seguenti:

- fornire supporto ad ogni soggetto autorizzato al trattamento per l'analisi e la risoluzione di dubbi/difficoltà connesse al trattamento dei dati;
- sensibilizzare i soggetti autorizzati della propria funzione sulla rilevanza del tema privacy nelle attività quotidiane;
- verificare che le istruzioni impartite dal Titolare – e comunicate attraverso qualsiasi strumento – siano effettivamente conosciute dai soggetti autorizzati;
- fungere da punto di contatto tra il Referente Privacy ed i soggetti autorizzati ex art. 29 GDPR appartenenti all'area di sua competenza;
- valutare l'adeguatezza delle misure di protezione, tecniche e organizzative, adottate nell'ambito dell'area di competenza;
- fornire supporto al Referente Privacy nella corretta tenuta del Registro delle attività di trattamento (art. 30 GDPR) effettuate nell'ambito dell'area di sua competenza;
- coinvolgere il Referente Privacy, fin dalla fase di progettazione, in caso di nuovo processo/progetto/utilizzo di nuova tecnologia che coinvolga dati personali al fine di mettere in atto misure tecniche e organizzative adeguate e per garantire che siano trattati per impostazione predefinita solo i dati necessari per ogni specifica finalità del trattamento (Privacy by design e Privacy by default);
- supportare il Referente Privacy nell'analisi dei rischi privacy e nell'eventuale valutazione di impatto sulla protezione dei dati (DPIA);
- proporre al Titolare del Trattamento, in collaborazione con il Referente Privacy, la nomina di soggetti esterni quali Responsabili del trattamento ex art. 28 GDPR, in relazione all'affidamento agli stessi di determinate attività;
- coordinare la raccolta delle informazioni necessarie a rispondere ad eventuali richieste pervenute dall'Autorità Garante Privacy o dagli Interessati;
- segnalare eventuali "incidenti" inerenti al trattamento dei dati personali (*data breach*);
- segnalare eventuali anomalie nella corretta applicazione delle misure di sicurezza, delle procedure e delle istruzioni per la gestione dei dati personali.

A ciascun Responsabile compete anche la supervisione sullo svolgimento delle operazioni di trattamento all'interno della propria area al fine di verificare che lo stesso sia eseguito in maniera corretta.

L'elenco dei nominativi dei Responsabili interni è costantemente aggiornato e conservato a cura del Responsabile dell'Ufficio Affari Legali e *Compliance* in apposito *database* digitale.

La Fondazione ha altresì individuato, autorizzato e formato i propri **soggetti autorizzati**.

I soggetti autorizzati al trattamento (Art. 29 GDPR) sono coloro che per lo svolgimento della propria attività lavorativa hanno accesso ai dati personali forniti dal Titolare e che ricevono dallo stesso istruzioni per il trattamento.

Ogni persona autorizzata al trattamento è pertanto opportunamente informata/formata sull'ambito di estensione delle proprie mansioni e competenze.

Al riguardo, il Titolare, in applicazione dell'art. 2 *quaterdecies* del D. Lgs. 196 del 2003, che ha introdotto la figura del soggetto formalmente designato, al momento di assunzione, fornisce a ciascuno dei soggetti in parola una specifica lettera di attribuzione dell'incarico in cui è ampiamente descritto il ruolo e i compiti loro attribuiti nel trattamento dei dati e la tipologia di dati al cui accesso sono autorizzati.

L'elenco dei nominativi dei soggetti autorizzati è costantemente aggiornato e conservato a cura del Responsabile dell'Ufficio Affari Legali e *Compliance* in apposito *database* digitale.

Da ultimo, la Fondazione ha individuato e nominato i propri **Responsabili esterni del trattamento**.

Il Responsabile del trattamento (art. 28 GDPR) è la persona, fisica o giuridica, autorità pubblica od altro organismo che materialmente effettua il trattamento per conto del Titolare ed è dallo stesso formalmente nominato e istruito.

Ai sensi dell'art. 28 del Regolamento, la Fondazione, quale Titolare del trattamento, qualora si avvalga di soggetti esterni per lo svolgimento di servizi nell'ambito dei quali sia necessario svolgere un trattamento dei dati, nomina il prescelto quale Responsabile del Trattamento.

Tale soggetto deve essere dotato delle necessarie competenze e conoscenze; l'incarico, affidato tramite contratto o altro atto giuridico vincolante, contiene tassativamente gli elementi elencati all'art. 28 GDPR, tra cui natura, durata e finalità del trattamento, il tipo di dati oggetto del trattamento e le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento.

La Fondazione prima di procedere alla nomina verifica che tale soggetto sia dotato delle necessarie competenze e conoscenze, che presenti garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'Interessato.

L'elenco dei nominativi dei Responsabili esterni è costantemente aggiornato e conservato a cura del Responsabile dell'Ufficio Affari Legali e *Compliance* in apposito *database* digitale.

4. FLUSSI INFORMATIVI

L'effettiva applicazione del Modello di Organizzazione Privacy si basa su costanti flussi di comunicazione tra le diverse figure organizzative, descritte nel precedente paragrafo.

- **Comunicazioni dei Responsabili interni nei confronti del Referente Privacy**

Il Referente Privacy, nello svolgimento delle proprie attività, è tenuto al segreto e alla riservatezza e deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

Ogni Responsabile Interno è tenuto a comunicare al Referente Privacy:

- le variazioni apportate ai livelli di accesso alle informazioni contenenti dati personali consentiti, per ragioni di sicurezza;
- la necessità di modificare il Registro dei trattamenti attraverso l'inserimento di un nuovo processo operativo/un nuovo sistema informativo e/o l'interruzione di un processo/un sistema informativo già in corso;
- ogni eventuale difficoltà riscontrata nell'esercizio della propria mansione;
- ogni carenza e/o inadeguatezza delle misure di protezione adottate dal Titolare del trattamento nelle aree di propria competenza;
- eventuali ispezioni in materia di protezione dei dati personali o richieste di informazioni e documentazione da parte del Garante della privacy o di altre Autorità;
- ogni comportamento od evento che possa determinare una violazione del Modello di Organizzazione Privacy o che, più in generale, sia rilevante ai fini della normativa in materia di protezione dei dati personali;
- ogni circostanza idonea a determinare potenzialmente una violazione dei dati (es. dispersione, distruzione, accesso non autorizzato e comunque trattamenti non consentiti) deve essere comunicata al Referente Privacy nel rispetto della Procedura di *Data Breach*.

- **Comunicazioni del Referente Privacy verso il Titolare del trattamento**

Il Referente Privacy riferisce direttamente al Titolare del trattamento in merito all'efficacia e osservanza del MOP e di ogni altra procedura in materia di privacy, all'emersione di eventuali aspetti critici, alla necessità di interventi modificativi.

A tal fine, il Referente Privacy predispone:

- con cadenza annuale, una relazione informativa, relativa all'attività svolta da presentare al Direttore Generale;
- immediatamente, al verificarsi di violazioni di dati, una comunicazione da presentare al Direttore Generale.

5. RAPPORTI CON L'AUTORITÀ DI CONTROLLO

Ogni Stato membro istituisce una o più autorità pubbliche indipendenti con il compito di "sorvegliare l'applicazione del presente regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione" (art. 51 GPDR).

L'Autorità di Controllo italiana è il Garante della Privacy ed esso è competente a conoscere eventuali violazioni di dati personali (*Data Breach*) e ad accogliere, nonché decidere su eventuali reclami presentati dagli Interessati.

Ai sensi dell'art. 56 del Regolamento l'autorità di controllo di riferimento di Fondazione Patrimonio Ca' Granda è il Garante della Privacy Italiano.

In caso di ispezioni in materia di protezione dei dati personali o di richieste di informazioni e documentazione da parte del Garante della Privacy o di altre Autorità, ogni soggetto autorizzato è tenuto a informare tempestivamente il Referente Privacy, che si coordina con il Titolare del trattamento.

6. L'INTERESSATO ED I SUOI DIRITTI

La Fondazione, al fine di tutelare pienamente gli Interessati dai trattamenti eseguiti, ha istituto un apposito canale per la ricezione delle istanze relative all'esercizio dei diritti riconosciuti all'Interessato dal GDPR.

In particolare, ogni Interessato, contattando il Titolare, potrà esercitare (nei limiti definiti dal GDPR), i seguenti diritti:

- **Diritto di Accesso (art. 15 GDPR):** l'Interessato ha il diritto di chiedere e ricevere una copia dei suoi dati personali oggetto di trattamento.
  Il Titolare è tenuto a fornire gratuitamente una copia dei dati, in forma cartacea o elettronica, potendo addebitare il costo di eventuali ulteriori copie in capo all'Interessato.
  Nelle ipotesi in cui il trattamento comporti una notevole quantità di informazioni, il Referente Privacy potrà chiedere all'Interessato di specificare le informazioni a cui la richiesta si riferisce.

- **Diritto di rettifica (art. 16 GDPR):** ogni Interessato ha il diritto di ottenere la correzione di eventuali inesattezze, nonché la correzione di informazioni non complete.
  L'inesattezza potrà in ogni caso essere inerente esclusivamente a dati di valore oggettivo. Di conseguenza, l'Interessato potrà chiedere la rettifica esclusivamente di dati fattuali e non invece di valutazioni soggettive e personali.
  Se non richiede uno sforzo sproporzionato, il Titolare comunicherà le richieste ricevute e le rettifiche/integrazioni effettuate ai soggetti cui i dati sono stati eventualmente comunicati.

- **Diritto di cancellazione (diritto all'oblio) (art.17 GDPR):** nel caso di espressa richiesta dell'Interessato, il Titolare ha l'obbligo di cancellare i dati dello stesso, su qualsiasi supporto archiviati. Inoltre, se tali dati sono stati diffusi (es. pubblicazione su un sito web), il Titolare deve informare della richiesta di cancellazione gli altri Titolari che trattano i dati personali oggetto della richiesta di cancellazione, invitandoli a rimuovere ogni copia degli stessi.
  In ogni caso, si precisa che la richiesta di cancellazione deve essere accolta solo al ricorrere di una delle ipotesi previste dal GDPR:
  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'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;
  c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;
  d) i dati personali sono stati trattati illecitamente;

e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro 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'articolo 8, paragrafo 1.
In ogni caso, la richiesta sarà respinta in tutte le ipotesi in cui ricorra una delle fattispecie derogatorie previste dagli artt. 2-*undecies* e 2-*duodecies* del Codice Privacy.
Si segnala altresì che in forza dello specifico interesse connesso ai dati oggetto della richiesta, il Titolare del trattamento potrà optare per la loro cancellazione o anonimizzazione.

- **Diritto di limitazione del trattamento (art. 18 GDPR):** l'Interessato può chiedere al Titolare di limitare il trattamento dei propri dati solo con riferimento ad alcune specifiche finalità unicamente nelle quattro ipotesi tassativamente elencate all'art. 18 GDPR, ovvero,
a) in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi),
b) nel caso in cui l'Interessato chieda la rettifica dei dati (in attesa di tale rettifica da parte del titolare),
c) si opponga al loro trattamento ai sensi dell'art. 21 del Regolamento (in attesa della valutazione da parte del titolare),
d) nelle ipotesi in cui i dati non siano più necessari al Titolare per il perseguimento delle proprie finalità ma divengano necessari per l'esercizio o la difesa di un diritto dell'interessato in sede giudiziaria.
Le tempistiche di limitazione sono strettamente connesse alla ragione posta a fondamento della richiesta. Infatti, nel caso in cui la limitazione sia richiesta per consentire la verifica della correttezza dei dati, per l'esercizio del diritto di opposizione o per l'esercizio di un diritto giudiziario dell'Interessato i dati potranno essere nuovamente resi disponibili in seguito all'accertamento; nel caso di trattamento illegittimo e conseguente richiesta di limitazione dell'Interessato, la limitazione potrà proseguire fino alla cancellazione dei dati o all'eventuale richiesta di portabilità dell'Interessato.
In ogni caso, la richiesta sarà respinta in tutte le ipotesi in cui ricorra una delle fattispecie derogatorie previste dagli artt. 2-*undecies* e 2-*duodecies* del Codice Privacy.

- **Diritto alla portabilità dei dati (art. 20 GDPR):** il diritto alla portabilità dei dati consente all'Interessato a) di ottenere, su richiesta, la restituzione dei propri dati personali da parte del titolare del trattamento e b) la loro trasmissione ad un nuovo Titolare.
La richiesta di portabilità può essere accolta solo al ricorrere di determinati presupposti:
1) sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato e
2) solo i dati che siano stati "forniti" dall'Interessato al Titolare, inoltre
3) il diritto alla portabilità può essere soddisfatto solo se non lesivo di diritti e libertà altrui.
Quando accolta, la richiesta di opposizione obbliga il Titolare ad interrompere il trattamento in modo definitivo e permanente.

Si precisa che la portabilità non comporta la cancellazione automatica dei dati conservati nei sistemi del Titolare.

- **Diritto di opposizione (art. 21 GDPR):** l'Interessato può chiedere l'interruzione, in modo permanente, del trattamento dei suoi dati personali.
  La richiesta di opposizione sarà accolta esclusivamente al ricorrere delle ipotesi previste dall'art. 21 par. 1 GDPR.
  Quando accolta, la richiesta di opposizione obbliga il Titolare ad interrompere il trattamento in modo definitivo e permanente.

Infine, l'Interessato ha sempre il diritto di proporre reclamo al Garante privacy ai sensi dell'art. 77 del GDPR qualora ritenga che i diritti di cui gode a norma della disciplina vigente sono stati violati a seguito di un trattamento.

Nelle informative rese agli Interessati al momento della raccolta dei dati, ogni Titolare comunica la possibilità di esercitare i diritti di cui al GDPR.
Da ultimo, le informative contengono esplicito riferimento alla possibilità per gli Interessati di proporre reclamo all'autorità di controllo ai sensi dell'art. 77 del Regolamento.

7. IL REGISTRO DEI TRATTAMENTI

La Fondazione ha adottato un proprio Registro dei Trattamenti che fornisce un quadro aggiornato dei trattamenti in essere all'interno dell'Ente.

Il Registro dei trattamenti della Fondazione è un file Excel formato da molteplici righe di lavoro, ciascuna dedicata ad uno specifico trattamento come di seguito meglio specificato.

Fondazione Patrimonio si è dotata di un proprio Registro dei trattamenti, non solo al fine di adempiere all'obbligo normativo previsto dall'art. 30 GDPR, ma anche e soprattutto al fine di dotarsi di uno strumento attraverso cui svolgere un'analisi accurata dei dati trattati, una mappatura approfondita dei trattamenti ed una ricognizione puntuale delle finalità perseguite.

Il Registro è continuamente aggiornato dal Referente Privacy con il supporto dei Responsabili Interni. Nel caso in cui si determini la necessità di procedere all'aggiornamento di una o più parti del Registro, il Referente Privacy provvede alla creazione di un nuovo foglio Excel, il quale sarà denominato con la data di redazione, ed al suo invio – via e-mail – al Titolare del trattamento al fine di attribuirvi data certa.

I fogli recanti le versioni obsolete del Registro saranno convertite in pdf e non saranno più modificabili.

Il Referente Privacy aggiorna il Registro:

- ogni volta che vengono modificate le aree di trattamento già registrate o vengono introdotte nuove aree di trattamento;
- in ogni caso, almeno una volta all'anno.

7.1 ASSEGNAZIONE DELLE BASI GIURIDICHE

Come specificato nel Capitolo 2, la Fondazione esegue il trattamento esclusivamente in forza di una delle basi giuridiche previste dagli artt. 6, 9 e 10 GDPR.

La Fondazione ricorre alla base giuridica del legittimo interesse solo in casi eccezionali e residuali. In tal caso, il Titolare si impegna a svolgere preventivamente un bilanciamento tra l'interesse proprio o di terzi e degli interessi, diritti e libertà fondamentali dell'Interessato.

Tale bilanciamento sarà eseguito a cura del Referente Privacy con il supporto del Responsabile Interno coinvolto.

Il bilanciamento dovrà dare evidenza delle ragioni a sostegno della prevalenza dell'interesse legittimo del Titolare sui diritti dell'Interessato.

Nelle ipotesi in cui il bilanciamento attesti la prevalenza dell'interesse del Titolare o di terzi, il trattamento è legittimamente avviato e traccia scritta del bilanciamento con correlato esito è archiviata a cura del Referente Privacy.

Nei casi in cui prevalgano gli interessi, le libertà e i diritti dell'Interessato, il trattamento non è avviato per carenza di un'idonea base giuridica.

7.2 TEMPI DI CONSERVAZIONE

Il Titolare del trattamento ha definito i tempi di conservazione di ogni categoria di dati in base alla finalità di impiego dei medesimi.

In particolare, nel Registro dei trattamenti è indicato il termine massimo di conservazione oltre il quale il Titolare si impegna a cancellare i dati o ad adottare procedure che li anonimizzino.

I dati personali trattati dai soggetti che il Titolare ha nominato Responsabili ex art. 28 GDPR saranno cancellati oppure restituiti al Titolare al termine del rapporto contrattuale che ha legittimato l'utilizzo di tali dati da parte del Responsabile.

7.3 MISURE TECNICHE ED ORGANIZZATIVE

Ai sensi dell'art. 32 GDPR, il Titolare, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio.

Le **misure tecniche** adottate dal Titolare per garantire un adeguato livello di rischio sono, tra le altre:

- controllo accessi (sistemi di autenticazione, sistemi di autorizzazione);
- credenziali unipersonali;
- definizione di livelli di accesso differenziati in relazione alla mansione;
- sistemi di protezione IT (antivirus, firewall);
- backup.

Le misure **organizzative** adottate dal Titolare per garantire un adeguato livello di rischio sono, tra le altre:

- definizione di un organigramma privacy con dettaglio di ruoli e responsabilità;
- nomina per iscritto del personale contenente puntuali istruzioni per il trattamento;
- organizzazione di corsi di formazione e di campagne di sensibilizzazione in materia di protezione dei dati personali;
- definizione di un Modello di Organizzazione Privacy;
- definizione di procedure e *policies* di sicurezza logiche e fisiche;
- archiviazione dei documenti cartacei in locali con accesso limitato;
- individuazione dei soggetti terzi che hanno accesso ai dati della Fondazione nomina di tali soggetti quali Responsabili esterni e previsione di verifiche periodiche sul rispetto

del GDPR da parte di tali soggetti;

- minimizzazione dell'utilizzo dei dati.

8 VALUTAZIONE DEI RISCHI CONNESSI AI TRATTAMENTI

Ai sensi dell'art. 35 del GDPR il Titolare del trattamento, nel caso in cui 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 tenuto ad effettuare, prima di procedere al trattamento, una valutazione d'impatto privacy (di seguito "DPIA" o "*Data Protection Impact Assessment*").

La DPIA è pertanto obbligatoria solo per i trattamenti che presentano un rischio elevato per i diritti e le libertà delle persone fisiche (cfr. Considerando 75 GDPR).

Il GDPR (Considerando 75 e 76) precisa che il suddetto rischio deve essere misurato con criteri oggettivi che permettano di individuare trattamenti a rischio e a rischio elevato in termini di probabilità e gravità e che tali grandezze debbano essere determinate con attenzione a natura, ambito di applicazione, contesto e finalità di trattamento.

In assenza di ulteriori indicazioni inerenti alla metodologia attraverso cui l'adempimento deve essere condotto, la Fondazione ha costruito un processo di valutazione e gestione del rischio privacy seguendo le indicazioni contenute nei Considerando del GDPR, nelle Linee Guida WP248 rev.1 adottate in materia dal Gruppo WP29 e nell'Allegato 1 al provvedimento n. 467 dell'11 ottobre 2018 del Garante Privacy italiano.

In particolare, il processo così costruito prevede che, al fine di adempiere alle prescrizioni normative, la Fondazione:

- esegua un'analisi preliminare di ogni trattamento posto in essere, sulla base di quanto riportato nel Registro dei trattamenti, per verificare la sussistenza delle condizioni per procedere al DPIA (*valutazione rischio astratto*);
- solo per i trattamenti per cui risulta in essere un rischio astratto elevato, esegua una valutazione d'impatto (DPIA), verificando l'incidenza delle misure tecniche e organizzative nell'attenuazione e gestione del rischio (*valutazione rischio residuo*);
- nei casi in cui il DPIA restituisce come esito un rischio elevato, proceda alla consultazione preventiva del Garante per la protezione dei dati personali ai sensi dell'art. 36 GDPR.

La Fondazione utilizza l'espressione "rischio" per indicare *uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità» per i diritti e le libertà e l'espressione "rischio astratto" per indicare il rischio associato al verificarsi di un possibile evento che possa comportare un impatto sui diritti e le libertà degli Interessati, senza tenere in considerazione le misure di sicurezza interne.*

Il rischio astratto è quindi identificato nel rischio intrinseco che l'Interessato corre nel momento in cui suoi dati sono oggetto di trattamento.

La fase di "Analisi Preliminare" si compone di due sottofasi:

i) verifica della ricorrenza di una delle ipotesi indicate dall'Autorità Garante nell'Allegato 1 al provvedimento n. 467 dell'11 ottobre 2018;
ii) individuazione e misurazione del rischio astratto correlato ai trattamenti posti in essere.

Con riferimento al punto i), la Fondazione confronta ogni trattamento effettuato con l'elenco delle 12 tipologie di trattamento da sottoporre a necessaria valutazione d'impatto pubblicato dall'Autorità Garante e nei casi di corrispondenza procede all'esecuzione della DPIA.

Con riferimento al punto ii), la Fondazione sottopone a valutazione specifica del rischio astratto ogni trattamento che non trovi corrispondenza nell'elenco di cui sopra (stante la sua natura esemplificativa e non tassativa).

Nello specifico, il "*Rischio astratto*" è calcolato attraverso il rapporto tra la "probabilità" (P) che si verifichi un evento lesivo per gli Interessati nell'ambito del singolo trattamento e la "gravità" (G) potenziale di tale impatto.

La "probabilità" (P) è definita attraverso il prodotto di due parametri:

- il tipo di trattamento (T): il cui valore è dato dal ricorrere di una o più delle attività indicate dalle citate Linee Guida del Gruppo WP29 come caratterizzate da un "rischio elevato" in quanto potenzialmente lesive dei diritti e delle libertà delle persone fisiche se ricorrenti congiuntamente.
  Pertanto, il valore del fatto probabilità cresce al crescere delle ipotesi ricorrenti, seguendo il seguente schema:

Categoria	Descrizione	Valore attribuito
Trascurabile	Il dato non rientra in alcuna delle categorie	1
Basso	Il dato rientra in 1 categoria	2
Medio	Il dato rientra in 2 categorie	3
Elevato	Il dato rientra in più di 2 categorie	4

- il numero di interessati coinvolti (Q): la cui incidenza è valutata sulla base dei seguenti 4 parametri:

Categoria	Quantità interessati	Valore attribuito
Trascurabile	Da 1 a 10	1
Basso	Da 11 a 100	2
Medio	Da 101 a 10.000	3
Elevato	Oltre 10.000	4

Correlando gli indicatori relativi al tipo di trattamento (T) e al numero di interessati coinvolti (Q), secondo la matrice $\boldsymbol{P = T \; x \; Q}$, è definito il valore della Probabilità:

			Tipologia trattamento (T)			
			Trascurabile	Bassa	Media	Alta
			1	**2**	**3**	**4**
Quantità di interessati	Trascurabile	**1**	1	1	2	2
	Bassa	**2**	1	2	3	3
	Media	**3**	2	3	3	4
	Alta	**4**	2	3	4	4

L'attribuzione del valore della probabilità avviene secondo i seguenti 4 livelli:

Probabilità	Valore attribuito
Improbabile	1
Poco Probabile	2
Mediamente probabile	3
Altamente probabile	4

Il fattore Gravità, ovvero gli effetti causati sui diritti e le libertà dell'Interessato da un determinato evento, è determinato in base all'incidenza sul dato in termini di disponibilità, integrità e riservatezza.

In particolare, la valutazione è effettuata con l'ausilio dei criteri riportati nella tabella sottostante:

Livello Gravità	**Riservatezza (divulgazione e accesso illegittimo)**	**Integrità (alterazione illegittima)**	**Disponibilità (distruzione illegittima, indisponibilità, perdita dei dati)**
1 - Trascurabile	La mancanza di riservatezza, di integrità o di disponibilità ha impatti lievi (es. fastidio) sulla vita sociale o personale degli interessati. Ad esempio, perdita di tempo nel dover ripetere le procedure o di aspettarle, riutilizzo dei dati da parte di terzi per scopi pubblicitari, senso di violazione della privacy senza danno reale.		
2 - Basso	La mancanza di riservatezza, integrità e disponibilità ha impatti, non critici e che creano piccole difficoltà (es. costi, paura, incomprensioni, stress, malanni minori) a causa degli effetti sulla vita sociale o personale degli interessati.		
3 - Medio	La mancanza di riservatezza, integrità e disponibilità ha un elevato impatto che può essere superato con difficoltà sulla vita sociale o personale degli interessati. Ad esempio, fondi non disponibili, blocco da parte di enti economici, danni alla proprietà, perdita del posto di lavoro, denunce, peggioramento della salute, appropriazione indebita di denaro, guadagni persi, perdita di lavoro, vittima di ricatti, cyberbullismo, molestie morali.		
4 - Elevato	La mancanza di riservatezza, integrità e disponibilità ha impatti non reversibili sulla vita sociale o personale, e comporta: - perdita di autonomia; - esclusione (p.e. inabilità a lavorare); - sanzioni penali e perdita di libertà; - danni fisici (p.e. danni fisici o mentali a lungo termine o morte); - impossibilità di azione legale; - squilibrio di potere; - perdita di fiducia; - perdita economica.		

In base alle valutazioni condotte ad ogni trattamento è attribuito uno dei seguenti quattro livelli di gravità:

Entità/Gravità impatto	Valore attribuito
Trascurabile	1
Basso	2
Medio	3
Elevato	4

Il Rischio Astratto (RA) è pertanto calcolato secondo la seguente tabella:

			Entità e gravità dell'impatto			
			trascurabile	***Bassa***	***Media***	***Alta***
			1	**2**	**3**	**4**
Probabilità	***Improbabi***	**1**	**1**	**2**	**3**	**4**
	poco	**2**	**2**	**4**	**6**	**8**
	Probabile	**3**	**3**	**6**	**9**	**12**
	altamente	**4**	**4**	**8**	**12**	**16**

Indice di Rischio	Descrizione
Trascurabile	$R \leq 2$
Basso	$2 < R \leq 4$
Medio	$4 < R \leq 6$
Alto	$6 < R \leq 9$
Elevato	$R > 9$

Per i soli trattamenti in cui il Rischio Astratto sia stato valutato elevato, la Fondazione esegue la valutazione d'impatto ai sensi dell'art. 35 GDPR ed individua il Rischio Residuo (RR), tenendo conto delle misure di sicurezza adottate che consentono, quindi, di arginare l'incidenza del rischio astratto.

Nello svolgimento di tale valutazione sono prese in considerazione le misure di sicurezza che si distinguono in:

- ❖ in misure tecniche:
  - Controllo accessi (Sistemi di autenticazione, sistemi di autorizzazione)
  - *Data storage*
  - *Vulnerability management*
  - Protezione da malware
  - *Key management*
  - Archiviazione e gestione dei Log
  - *Continuity management*: sistema in *Disaster Recovery*, sistema di *backup*
  - *Firewell*
  - Cifratura dei dati
  - *Intrusion detection*
  - *Vulnerability assessment/penetration test*
  - Tracciamento operazioni

- ❖ in misure fisiche:
  - vigilanza della sede
  - sistemi di videosorveglianza
  - ingresso controllato nei locali ove ha luogo il trattamento
  - sistemi di allarme e/o di sorveglianza antintrusione
  - registrazione degli accessi
  - autenticazione degli accessi
  - custodia in armadi blindati e/o ignifughi
  - dispositivi antincendio
  - continuità dell'alimentazione elettrica
  - controllo sull'operato degli addetti alla manutenzione
  - verifica della leggibilità dei supporti
  - monitoraggio parametri ambientali locali macchine

- ❖ in misure di organizzazione:
  - creazione di un organigramma privacy e definizione di ruoli e responsabilità
  - istruzioni
  - formazione
  - elaborazione di un Modello Organizzativo Privacy
  - procedure e *policies* di sicurezza logiche e fisiche
  - *audit*
  - strumenti di controllo per gli interessati
  - separazione dei dati
  - controllo accessi amministratori

- misure di sicurezza per terze parti
- minimizzazione dei dati
- anonimizzazione dei dati
- conservazione adeguata

La valutazione delle misure di sicurezza è effettuata sulla base dei criteri riportati nella tabella sottostante, i quali danno una corrispondenza in termini di 3 livelli di adeguatezza delle suddette misure:

Livello	Linee guida per la valutazione	Valutazione rischio residuo
1- Inadeguato	Il controllo non è previsto o è assente nella pratica.	Tale livello comporta il mantenimento della classe di rischio individuata per il rischio astratto.
2- Parzialmente adeguato	Le misure sono state adottate, tuttavia sono state rilevate delle mancanze che non ne garantiscono la totale efficacia oppure il controllo è stato implementato, ma è sporadicamente applicato.	Tale livello comporta il passaggio ad una classe di inferiore rischio.
3- Adeguato	Le misure di sicurezza sono adeguate e sistematicamente applicate.	Tale livello comporta il passaggio a due classi inferiori di rischio.

Se all'esito della valutazione d'impatto il rischio rimane elevato, la Fondazione procederà con la consultazione preventiva all'autorità Garante della Privacy ex art. 36 GDPR.

9 GESTIONE DEI DATA BREACH

Data breach: perdita accidentale (smarrimento di una chiavetta USB contenente dati riservati), furto (furto di un notebook contenente dati confidenziali), infedeltà aziendale (copia dei dati distribuita in ambiente pubblico da un dipendente), accesso abusivo (accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite).

Nel caso in cui si verifichi una violazione dei dati personali (*Data Breach*), ogni soggetto incaricato al trattamento che ne abbia per primo conoscenza dovrà darne comunicazione al Referente Privacy, così da consentire al Titolare di adempiere agli obblighi di notifica previsti dall'art. 33 GDPR entro i tempi definiti dalla norma.

La comunicazione deve essere inviata in forma scritta tramite e-mail al soggetto sopra indicato e deve contenere una prima breve descrizione dell'evento e del suo impatto sui dati personali.

Successivamente, ove ritenuta meritevole di approfondimento, il Referente Privacy, con il supporto del Responsabile interno eventualmente competente, provvede a richiedere ulteriori indagini al soggetto che ne ha avuto per primo conoscenza.

In base alle informazioni così raccolte, il Referente Privacy esegue la valutazione dei fatti e definisce il livello di rischio per i diritti e le libertà degli Interessati connesso alla violazione, al fine di valutare la necessità di notifica della violazione all'Autorità di controllo e agli Interessati.

Indipendentemente dall'esito della valutazione, il Referente Privacy predispone un *report* sulle caratteristiche, circostanze e conseguenze della violazione, nonché sui provvedimenti di prevenzione e mitigazione del rischio adottati.

Nei casi in cui la valutazione induca a ritenere improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, la procedura si interrompe.

Nel caso in cui gli accertamenti eseguiti rilevino un probabile rischio per i diritti e le libertà degli Interessati, il Titolare, per il tramite del Referente Privacy, notifica la violazione all'Autorità di Controllo, entro 72 ore dall'evento ove possibile, in caso contrario corredando la notifica con i motivi del ritardo.

Ove la violazione dei dati presenti un rischio elevato per i diritti e le libertà delle persone fisiche, il Referente Privacy provvede a dare comunicazione della violazione anche agli interessati, senza ingiustificato ritardo.

10 CONTROLLO E SANZIONI

Un primo livello di controllo è posto in carico ai Responsabili Interni di riferimento, i quali dovranno verificare che le istruzioni fornite agli autorizzati con il presente Modello e con specifici atti di nomina siano effettivamente rispettate e applicate.

Un secondo livello di controllo è invece in carico al Referente Privacy, il quale ha la facoltà di, mediante la definizione di un Piano di attività periodico effettuare specifici *assessment* e verifiche a campione, finalizzate a monitorare la corretta applicazione del Modello, delle procedure e delle istruzioni fornite, nonché effettua verifiche su tutto il sistema privacy del Titolare.

Nel caso in cui i soggetti autorizzati al trattamento violino, eludano o applichino parzialmente o non correttamente il Modello e i documenti allo stesso allegati, saranno sanzionati ai sensi della disciplina relativa ai contratti di lavoro, con particolare riferimento agli illeciti disciplinari, e la sanzione sarà modulata rispetto al livello di responsabilità ed autonomia del dipendente, all'intenzionalità del comportamento e alla gravità del medesimo rispetto agli effetti a cui il Titolare può ragionevolmente ritenersi esposto.

In caso di violazione della disciplina prevista dal Regolamento UE, ai sensi dell'articolo 83 GDPR e dell'art. 166 del D. Lgs. n. 196/2003, l'Autorità di controllo provvede ad infliggere sanzioni amministrative pecuniarie.

In particolare, in base alla tipologia di violazione le sanzioni possono ammontare fino a 10 milioni di euro, o fino al 2% del fatturato mondiale annuo della società se superiore, ovvero fino a 20 milioni di euro, o fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente se superiore.

Ancora, il Titolare del trattamento ovvero il Responsabile del trattamento devono, ai sensi dell'articolo 82 GDPR, risarcire il danno all'Interessato che abbia subito un danno materiale o immateriale causato dalla violazione e che ne faccia richiesta.

Inoltre, le Autorità di controllo possono limitare, sospendere ovvero anche bloccare un trattamento di dati.

Il GDPR non prevede direttamente delle sanzioni penali in materia di protezione dei dati personali; tuttavia, nel Considerando 149 stabilisce che gli Stati membri dovrebbero poter stabilire disposizioni relative a sanzioni penali per violazioni del GDPR.

PARTE SPECIALE

1. GESTIONE DELLE ATTIVITÀ DI SELEZIONE E GESTIONE DEL PERSONALE

La Fondazione al fine di svolgere le attività di selezione, assunzione e gestione del personale dipendente è tenuta ad effettuare il trattamento di alcuni loro dati personali.

Tali attività si svolgono come di seguito descritto:

i. redazione dell'avviso di selezione a cura dell'Ufficio Servizi Generali e Risorse Umane, avendo cura 1) di non indicare tra le informazioni necessarie per la somministrazione della candidatura informazioni non necessarie in relazione le finalità perseguite e 2) di includere tra la documentazione di gara un'informativa ex art. 13 GDPR per i candidati;

ii. ricezione dei CV attraverso i canali specificatamente individuati nella documentazione di gara;

iii. verifica a cura della Commissione di preselezione dei contenuti del *Curriculum Vitae* di ciascun candidato: in caso di ricezione di CV contenenti dati particolari (quali ad esempio malattie, opinioni politiche o convinzioni religiose), fatte salve le ipotesi in cui il dato sia necessario per proseguire la valutazione, il Presidente di Commissione provvede all'oscuramento dell'informazione o alla richiesta al candidato di inviare nuovamente il CV eliminando tali dati;

iv. assegnazione a ciascun candidato di un codice identificativo alfanumerico che ne consenta l'individuazione univoca e che ne tuteli la riservatezza;

v. individuazione del candidato prescelto e pubblicazione della graduatoria – in forma esclusivamente anonima (i.e. tramite codice alfanumerico) – sul sito Internet della Fondazione a cura dell'Ufficio Servizi Generali e Risorse Umane;

vi. archiviazione della documentazione prodotta durante i diversi *step* di valutazione a cura dell'Ufficio Servizi Generali e Risorse Umane, con modalità idonee a garantire riservatezza e disponibilità;

vii. sottoscrizione della lettera di assunzione ad opera del Direttore Generale, nonché del neoassunto per accettazione, e consegna di informativa ex art. 13 GDPR nonché di specifica lettera di autorizzazione al trattamento dei dati personali;

viii. al momento dell'assunzione della nuova risorsa, è acquisita copia della documentazione necessaria per gli adempimenti amministrativo-contabili correlati alla nuova assunzione. - ogni informazione acquisita in tale sede è conservata in un fascicolo individuale, avente forma cartacea ed elettronica, conservato in archivi riservati ed accessibili esclusivamente al personale dell'Ufficio competente per la sua implementazione;

ix. con particolare riferimento alle informazioni idonee a rilevare lo stato di salute del dipendente, il Titolare del trattamento assumerà esclusivamente informazioni relative al generale stato di salute del dipendente e non, invece, informazioni specifiche.
Invero:

a. con riferimento agli accertamenti condotti dal Medico competente tramite visite periodiche nell'espletamento dei compiti previsti dal D. Lgs. 81/08 e dalle altre disposizioni in materia di igiene e sicurezza nei luoghi di lavoro, il Titolare del trattamento avrà conoscenza dell'esito della visita condotta esclusivamente quale

giudizio di idoneità/inidoneità lavorativa con riferimento alla specifica mansione del dipendente;

b. nel caso di lavoratore assente per malattia, la Fondazione riceverà esclusivamente un certificato senza diagnosi contenente la sola indicazione dell'inizio e della durata dell'infermità;

x. con riferimento alle informazioni idonee a rilevare l'appartenenza sindacale, l'orientamento politico e religioso del dipendente, il Titolare del trattamento si impegna a raccogliere le informazioni strettamente necessarie per garantire i diritti costituzionali riconosciuti in materia. Pertanto, ad esempio, la Fondazione accetterà permessi sindacali o politici solo se privi di ogni indicazione circa l'associazione sindacale o il partito politico di appartenenza;

xi. con riferimento alle informazioni relative la composizione del nucleo familiare del dipendente, il Titolare del trattamento si impegna ad acquisire esclusivamente le informazioni necessarie per la determinazione ed applicazione dei benefici fiscali. Inoltre, le stesse saranno rese note esclusivamente ai dipendenti specificamente autorizzati e deputati alla loro raccolta ed archiviazione;

xii. con riferimento alle informazioni inerenti a condanne o misure di sicurezza, la Fondazione si impegna ad acquisire tali tipologie di dati solo ed esclusivamente ove necessario per l'adempimento ad un obbligo di legge, secondo le modalità da questo definite;

xiii. il dipendente è informato dell'esistenza e del contenuto delle norme comportamentali da seguire, anche in materia di privacy, ed è tenuto a sottoscrivere la presa visione del Modello di Organizzazione Privacy adottato dalla Fondazione nonché della normativa interna in materia di protezione dei dati personali;

xiv. il monitoraggio delle presenze e degli orari di lavoro giornalieri per il personale operativo è effettuato tramite sistemi di monitoraggio informatico, idonei a garantire alti livelli di segregazione e integrità;

i. il Consulente del Lavoro deputato alla gestione degli aspetti contabili opera in qualità di Titolare autonomo, conformemente alla normativa vigente in materia di protezione dei dati personali;

ii. la prestazione lavorativa in modalità *smart working* è regolata attraverso regolamenti interni, che definiscono – tra l'altro – le misure di sicurezza organizzative e tecniche da attuare.

2. GESTIONE DI PROCEDURE E BANDI DI GARA FINALIZZATI ALL'ACQUISTO DI BENI E SERVIZI

Il GDPR ed il Codice Privacy prescrivono un particolare regime di tutela per i dati personali relativi a condanne penali e a reati o alle connesse misure di sicurezza.

Ai sensi dell'art. 2-*octies* del Codice Privacy, il trattamento dei dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza può essere effettuato solo se autorizzato da norma di legge o, nei casi previsti dalla legge, di regolamento, e purché i provvedimenti in parola prevedano garanzie appropriate per i diritti e le libertà degli Interessati.

La Fondazione tratta dati riconducibili alla categoria di cui all'art. 10 GDPR dei propri fornitori in adempimento di specifici obblighi di legge strettamente correlati alla peculiare natura giuridica.

Nell'eseguire le suddette attività, la Fondazione attua le misure di sicurezza di seguito dettagliate:

- il trattamento viene eseguito attraverso soggetti interni ed esterni specificatamente individuati, nominati e formati;
- il trattamento è effettuato unicamente con operazioni, nonché con logiche e mediante forme di organizzazione dei dati, proporzionate e necessarie in rapporto agli obblighi ed alle finalità per i quali il trattamento è effettuato;
- il trattamento è effettuato unicamente per realizzare le finalità perseguite;
- il Titolare verifica periodicamente l'esattezza e l'aggiornamento dei dati raccolti, nonché la loro adeguatezza, pertinenza e necessità rispetto alle finalità perseguite nei singoli casi;
- il Titolare cura la cancellazione dei dati che, anche a seguito delle verifiche, risultino non adeguati, non pertinenti o non necessari, salva l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene.

Le attività di raccolta e trattamento dei suddetti dati consistono in:

- identificazione della necessità di raccolta di un "dato giudiziario" a cura dell'Ufficio Affari Legali e *Compliance;*
- verifica della sussistenza di un'adeguata base giuridica a cura del Referente Privacy;
- raccolta del dato tramite consegna spontanea da parte dell'Interessato o, in alternativa, raccolta del dato tramite richiesta alla competente Autorità;
- custodia del dato a cura dell'Ufficio Affari Legali e *Compliance* in buste, individuali, chiuse ed opportunamente sigillate, nonché tramite database adeguatamente segregato;
- impiego del dato per il fine per cui è stato raccolto a cura dell'Ufficio competente;
- conservazione del dato per il tempo strettamente necessario in buste, individuali, chiuse ed opportunamente sigillate, collocate in cassaforte site in locale ad accesso controllato, nonché tramite database adeguatamente segregato;
- distruzione del documento al decorrere del tempo di conservazione definito.

3. GESTIONE DELL'AFFIDAMENTO DEI CONTRATTI DI LOCAZIONE E/O AFFITTO

Il processo di gestione dell'affidamento dei contratti di locazione e/o di affitto dei beni immobili si articola nelle seguenti macro-attività:

i. esecuzione delle attività propedeutiche all'individuazione del conduttore, in fase di rinnovo del contratto di affitto (i.e. conduttore uscente o, in successione, conduttore contiguo o quello limitrofo) o in fase di nuova stipula (a seguito di pubblicazione di apposito avviso/indizione di una gara);

ii. indipendentemente dalla modalità di individuazione del conduttore, l'Ufficio Gestione Locazioni con il supporto l'Ufficio Affari Legali e *Compliance* predispone la documentazione di gara avendo cura di includere anche una specifica informativa ex art. 13 GDPR, finalizzata ad informare ciascun potenziale conduttore delle modalità e finalità del trattamento dei suoi dati durante l'iter di selezione e valutazione;

iii. individuato il conduttore, l'Ufficio competente in relazione alla procedura esperita, in fase di sottoscrizione del contratto di locazione/affitto, consegna al conduttore apposita informativa ex art. 13 GDPR.

4. GESTIONE DELLE ATTIVITÀ DI COMUNICAZIONE E PROMOZIONE

La gestione delle comunicazioni istituzionali e delle attività di promozione dell'immagine della Fondazione sono disciplinate dalle seguenti regole operative:

i. le attività di comunicazione e promozione sono gestite dal Responsabile dell'Ufficio Comunicazione, con il supporto degli uffici della Fondazione di volta in volta interessati in relazione all'oggetto della comunicazione;

ii. il Responsabile dell'Ufficio Comunicazione individua gli eventi/le attività da portare a conoscenza del pubblico e raccoglie le informazioni necessarie per la redazione della comunicazione;

iii. il Responsabile dell'Ufficio Comunicazione redige la bozza di documento/comunicato;

iv. con riferimento alle ipotesi in cui, per la predisposizione del materiale, il Responsabile dell'Ufficio Comunicazione intervista i referenti di progetto o i partecipanti al progetto, lo stesso ha cura di acquisire una registrazione audio/video in cui l'Interessato manifesta il proprio consenso all'utilizzo dei propri dati. La registrazione è sottoposta al Referente Privacy per la verifica di legittimità;

v. ove il testo del documento prodotto sia corredato da immagini/foto atte a ritrarre – direttamente e/o indirettamente – persone fisiche, la bozza del documento /comunicato è sottoposta al Referente Privacy per la verifica di legittimità. Il Referente Privacy, verificato se la persona fisica è ritratta con modalità idonee a consentirne il riconoscimento, ne autorizza la pubblicazione solo ove l'interessato abbia manifestato il suo libero consenso tramite liberatoria/presa visione dell'Informativa privacy; il Referente Privacy autorizza la pubblicazione anche in assenza di specifico consenso, nelle ipotesi in cui il soggetto sia ritratto di spalle o con altre modalità idonee ad evitarne il riconoscimento o nelle ipotesi in cui il volto raffigurato, anche soltanto in parte, sia puntualmente anonimizzato;

vi. con riferimento al servizio di *newsletter* avente ad oggetto comunicazioni inerenti ad eventi organizzati dalla Fondazione (es. Accademia Ca' Granda) o da terzi, il Responsabile dell'Ufficio Comunicazione utilizza esclusivamente i dati di contatto di utenti che hanno manifestato il proprio interesse, tramite iscrizione in apposito *form online*, e che non hanno revocato il medesimo tramite apposito meccanismo di *flag out*.

5. GESTIONE DEI FORNITORI – RESPONSABILI EX ART. 28 GDPR

La qualifica di Responsabile ("esterno") del trattamento ex art. 28 GDPR è attribuita ad una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che tratta dati personali per conto del Titolare (art. 4, pf. 8 GDPR).

I criteri fondamentali per l'individuazione del Responsabile, pertanto, sono i seguenti:

- che sia un'entità distinta e separata rispetto al Titolare del trattamento;
- che tratti dati personali per conto del Titolare del trattamento e su sua documentata istruzione (fermo restando che le istruzioni del Titolare del trattamento possono lasciare un certo grado di discrezionalità consentendo al responsabile del trattamento di scegliere la soluzione tecnica e organizzativa più adatta al caso concreto).

La circostanza per cui il Responsabile ("esterno") sia tenuto a trattare dati per conto del Titolare implica necessariamente che il medesimo entri a far parte del "Sistema privacy" della Fondazione e, di conseguenza, sia tenuto a trattare i dati secondo le istruzioni del Titolare (soggetto che determina finalità e mezzi del trattamento).

Per tale ragione, il Titolare deve preliminarmente verificare, in una fase precedente alla sottoscrizione di un contratto con un fornitore, se la controparte, al fine di eseguire il contratto, necessiti di trattare i dati personali di titolarità della Fondazione. In caso affermativo, al Titolare è richiesto di accertare che la controparte possa mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti di cui al GDPR e garantisca la tutela dei diritti dell'interessato (art. 28, par. 1 del GDPR).

Le attività di nomina dei Responsabili esterni si svolgono pertanto come di seguito descritto:

i. al momento del conferimento dell'incarico, il Responsabile di funzione competente in relazione alla procedura di acquisto – con il supporto del Referente Privacy – verifica se l'attività affidata al fornitore/consulente comporta il trattamento di dati personali;
ii. ove la verifica dia esito positivo, il Responsabile di funzione competente in relazione alla procedura di acquisto si adopera a somministrare al fornitore apposite richieste documentali e non finalizzate a verificare il livello di conformità alla normativa privacy;
iii. il Responsabile dell'Ufficio Servizi Generali e Risorse Umane trasmette al fornitore apposita lettera di incarico ex art. 28 GDPR con richiesta di siglarla per accettazione del contenuto;
iv. il riscontro documentale e non del fornitore deve essere inviato dal richiedente al Referente Privacy per la valutazione delle misure di sicurezza del fornitore;
v. superata con esito positivo la valutazione del fornitore/Responsabile, il Referente Privacy informa il soggetto richiedente che procede con la definizione della nomina a Responsabile del trattamento;
vi. il Referente Privacy tiene traccia di tutti i fornitori nominati Responsabili del trattamento in apposito Registro, annotando anche il giorno di sottoscrizione della nomina a Responsabile del trattamento ed eventuali verifiche svolte sul Responsabile, e dando atto del Sub-Responsabile eventualmente nominato e del trasferimento di dati extra-UE, se realizzato.