fondazione
innovazione urbana

PROCEDURE IN MATERIA DI TRATTAMENTO DEI DATI PERSONALI

1. Scopo

Lo scopo del presente documento è di definire:le modalità operative per la corretta applicazione del Regolamento Generale sulla Protezione dei Dati (Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27/4/16, di seguito GDPR) e del Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" con riferimento:

- alla gestione delle richieste di esercizio dei diritti degli interessati;
- alla gestione della violazione dei dati personali (c.d. *data breach*).

2. Campo di applicazione

Le disposizioni contenute nel presente documento si applicano al trattamento di dati personali, secondo la definizione datane dall'art. 4, paragrafo 1, n. 1), del GDPR, effettuato dalla Fondazione sia in qualità di Titolare del trattamento sia in qualità di Responsabile del trattamento.

3. Soggetti coinvolti

3.1. Titolare del trattamento

Ai sensi dell'art. 4, paragrafo 1, n. 7), il Titolare del trattamento è 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.

Al momento, la Fondazione è Titolare del trattamento dei dati personali dei propri dipendenti e dei propri collaboratori, dati che vengono raccolti direttamente presso gli Interessati, ma anche di familiari di propri dipendenti, per adempimento di obblighi di legge relativi al rapporto di lavoro, che non vengono raccolti presso gli Interessati.

3.2. Contitolare del trattamento

Ai sensi dell'art. 26 del GDPR, si ha una situazione di "Contitolarità" allorché due o più Titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento.

In tale caso, i Contitolari del trattamento debbono determinare, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR, con particolare riguardo all'esercizio dei diritti degli Interessati, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del GDPR (informative). Il contenuto di tale accordo è messo a disposizione degli Interessati.

Gli Interessati possono in ogni caso esercitare i loro diritti nei confronti di e contro ciascuno dei Titolari-Contitolari del trattamento, indipendentemente da quanto dai medesimi stabilito nel loro accordo interno.

3.3. Responsabile del trattamento

Ai sensi dell'art. 4, paragrafo 1, n. 8), il Responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento.

Secondo le indicazioni del GDPR, il Responsabile del trattamento è un soggetto esterno alla struttura del Titolare del trattamento.

Il soggetto designato in qualità di Responsabile del trattamento deve fornire garanzie sufficienti ad assicurare il rispetto degli obblighi previsti dal GDPR e, in particolare, l'attuazione di misure tecniche e organizzative adeguate a far sì che il trattamento soddisfi pienamente le disposizioni del GDPR e garantisca la tutela dei diritti degli Interessati.

La designazione in qualità di Responsabile del trattamento deve essere effettuata mediante apposito atto scritto, redatto in conformità all'art. 28 del GDPR.

In attuazione di quanto sopra, la Fondazione nomina in qualità di Responsabili del trattamento tutti i soggetti esterni che trattano, per suo conto, dati personali di cui è Titolare del trattamento.

La Fondazione si trova altresì a svolgere, per conto di soggetti terzi, attività che implicano il trattamento di dati personali di cui detti soggetti terzi sono Titolari.

In tali casi, la Fondazione agisce in veste di Responsabile del trattamento, in virtù di appositi atti di nomina in tale qualità, attenendosi alle istruzioni impartite dal Titolare del trattamento avendo cura di segnalare eventuali istruzioni non conformi al GDPR.

3.4. Sub-Responsabile

Ai sensi dell'art. 28 del GDPR, i Responsabili del trattamento che, per lo svolgimento delle attività loro affidate dal Titolare del trattamento, si avvalgono di ulteriori soggetti esterni possono designare questi ultimi in qualità di altri Responsabili del trattamento (c.d. Sub-Responsabili) disciplinando i rapporti mediante apposito atto scritto. Tale atto, redatto in conformità all'art. 28 del GDPR, deve prevedere tutti i contenuti e gli obblighi che legano il Responsabile del trattamento al Titolare del trattamento e deve essere preceduto dalla verifica che i Sub-Responsabili presentino garanzie idonee ad assicurare il rispetto degli obblighi previsti dal GDPR e, in particolare, l'attuazione di misure tecniche e organizzative adeguate a far sì che il trattamento soddisfi pienamente le disposizioni del GDPR e garantisca la tutela dei diritti degli Interessati.

In ragione di quanto sopra, laddove agisce in qualità di Titolare del trattamento, la Fondazione chiede espressamente ai Responsabili del trattamento via via designati di dare conto degli eventuali Sub-Responsabili indicando: la denominazione, le attività affidate, i dati personali oggetto di trattamento

e le categorie di Interessati, l'avvenuta verifica circa le garanzie presentate, l'avvenuta formalizzazione per iscritto dei rapporti in essere tra Responsabile e Sub-Responsabile.

Laddove agisce invece in qualità di Responsabile del trattamento, la Fondazione, previa autorizzazione del Titolare del trattamento, ricorre unicamente a Sub-Responsabili che forniscano garanzie sufficienti ad assicurare il rispetto degli obblighi previsti dal GDPR e, in particolare, l'attuazione di misure tecniche e organizzative adeguate a far sì che il trattamento soddisfi pienamente le disposizioni del GDPR e garantisca la tutela dei diritti degli Interessati e formalizza i rapporti in essere mediante atti scritti aventi contenuto conforme agli atti stipulati con il Titolare del trattamento.

3.5. Destinatario

Ai sensi dell'art. 4, paragrafo 1, n. 9), del GDPR, il Destinatario è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che riceve comunicazione di dati personali, sia esso o meno un soggetto terzo.

I dipendenti e i collaboratori che agiscono sotto la diretta autorità della Fondazione sono autorizzati al trattamento dei dati personali di cui la stessa è Titolare ovvero Responsabile mediante apposite lettere di incarico e relative Istruzioni.

I soggetti esterni che svolgono, per conto della Fondazione, attività che implicano il trattamento di dati personali di cui la stessa è Titolare ovvero Responsabile sono designati in qualità di Responsabili ovvero di Sub-Responsabili del trattamento.

3.6. Persone autorizzate al trattamento di dati personali sotto l'autorità diretta del Titolare o del Responsabile del trattamento

Come già precisato nel precedente paragrafo 3.5, le persone che effettuano per conto della Fondazione attività che implicano il trattamento di dati personali di cui la stessa è Titolare o Responsabile e che agiscono sotto la diretta autorità della Fondazione sono a ciò espressamente autorizzati mediante apposite lettere di incarico e ricevono specifiche istruzioni di comportamento formalizzate per iscritto.

La Fondazione cura altresì che tali persone ricevano una adeguata formazione/informazione sul GDPR, sulle altre normative dell'Unione Europea e nazionali in materia di protezione dei dati personali e sulle misure tecniche e organizzative adottate dalla Fondazione al fine di garantire che i trattamenti di dati personali avvengano nel pieno rispetto di dette normative e garantiscano la tutela dei diritti degli Interessati.

3.7. Responsabile della Protezione dei Dati (RPD) ovvero Data Protection Officer (DPO)

Ai sensi dell'art. 39 del GDPR, il Responsabile della Protezione dei Dati (RPD), più noto come *Data Protection Officer (DPO)*, è il soggetto - persona fisica - appositamente nominato dal Titolare ovvero dal Responsabile del trattamento e svolge i seguenti compiti:

a) informa e fornisce consulenza al Titolare o al Responsabile del trattamento, nonché ai dipendenti che eseguono il trattamento, in merito agli obblighi derivanti dal GDPR e da altre disposizioni di legge vigenti nell'Unione Europea e/o negli Stati membri in materia di protezione dei dati personali;
b) sorveglia l'osservanza, all'interno dell'ente che lo ha nominato, del GDPR e delle altre disposizioni di legge vigenti nell'Unione Europea e/o negli Stati membri in materia di protezione dei dati personali, nonché delle politiche adottate dal Titolare o dal 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) fornisce, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati di ogni trattamento che presenti un rischio elevato per i diritti e le libertà delle persone fisiche;
d) coopera con l'Autorità di controllo, in Italia, con il Garante per la Protezione dei Dati Personali, e fungere da punto di contatto per tale Autorità. Il nominativo del Responsabile della Protezione dei Dati deve infatti essere comunicato direttamente al Garante, il quale per ogni verifica o acquisizione di dati/informazioni farà direttamente riferimento al Responsabile della Protezione dei Dati, che fungerà da interfaccia.

Nello svolgimento dei suoi compiti il Responsabile della Protezione dei Dati considera debitamente i rischi inerenti a ciascun trattamento, che debbono pertanto essere adeguatamente conosciuti e valutati.

In ragione di quanto sopra, il Responsabile della Protezione dei Dati viene tempestivamente ed adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

Il Titolare del trattamento fornisce al Responsabile della Protezione dei Dati le risorse (economiche e di supporto) necessarie per assolvere ai suoi compiti.

Gli Incaricati del trattamento possono rivolgersi direttamente al Responsabile della Protezione dei Dati al fine di essere supportati nello svolgimento delle loro attività di trattamento.

Gli Interessati possono contattare direttamente il Responsabile della Protezione dei Dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei diritti loro derivanti dalla applicazione del GDPR e dalle altre normative vigenti in materia.

Il Responsabile della Protezione dei Dati può essere un dipendente del Titolare o del Responsabile del trattamento ovvero un soggetto esterno. La Fondazione ha provveduto ad affidare l'incarico di Responsabile della Protezione dei Dati a un soggetto esterno. Il nominativo e i recapiti del Responsabile della Protezione dei Dati sono pubblicati sul sito istituzionale della Fondazione.

3.8. Terzo

Ai sensi dell'art. 4, paragrafo 1, n. 10), del GDPR, il "Terzo" è 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 ovvero una persona autorizzata al trattamento, ovvero un altro dei soggetti sopra indicati.

4. Altre definizioni

Ai fini della corretta applicazione della presente procedura da parte di tutte le figure a vario titolo coinvolte, risulta opportuno dare conto di altre definizioni contenute del GDPR.

4.1. Dato personale

Qualsiasi informazione riguardante una persona fisica identificata o identificabile; 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.

4.2. Categorie particolari di dati personali

Ai sensi dell'art. 9 del GDPR rientrano in tali categorie (sostanzialmente coincidenti con i "dati sensibili" di cui all'art. 4, lettera d, D.Lgs. 196/2003) i dati personali:

- che rivelano l'origine razziale o etnica;
- che rivelano le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale;
- genetici;
- biometrici;
- relativi allo stato di salute;
- relativi alla vita sessuale o all'orientamento sessuale.

4.3. Dati generici

Sono 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.

4.4. Dati biometrici

Sono 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.

4.5. Dati relativi allo stato di salute

Sono 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.

4.6. Interessato

Si tratta della persona fisica cui si riferiscono i dati personali.

4.7. Trattamento dei dati personali

Si intende 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.

- Raccolta: L'acquisizione dei dati personali direttamente presso l'Interessato o presso terzi.
- Registrazione: l'inserimento dei dati personali in supporti, informatici e/o cartacei, al fine di rendere i dati disponibili per i successivi trattamenti.
- Organizzazione: il processo di trattamento dei dati personali che ne favorisce la fruibilità attraverso l'aggregazione o la disaggregazione, l'accorpamento, la catalogazione, ecc.
- Strutturazione: l'operazione di trattamento che consiste nell'inserimento dei dati personali all'interno di un sistema secondo un preciso ordine.
- Conservazione: l'operazione di trattamento che consiste nella custodia dei dati personali.
- Adattamento e Modifica: le operazione di trattamento mediante le quali i dati personali registrati vengono adattati/modificati in relazione a successive variazioni dei medesimi.
- Estrazione: l'operazione mediante la quale da un complesso di dati personali viene appunto estratto un dato personale per compiere ulteriori operazioni di trattamento.
- Consultazione: l'operazione di trattamento che consiste nella possibilità di avere accesso ai dati personali disponibili.
- Uso: le operazioni di trattamento volte a realizzare lo scopo per cui si è provveduto alla raccolta
- Comunicazione: l'operazione di trattamento che consiste nel portare i dati personali dell'Interessato a conoscenza di uno o più soggetti determinati, diversi da quest'ultimo, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
- Diffusione: l'operazione di trattamento che consiste nel portare i dati personali dell'Interessato a conoscenza di soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
- Raffronto: l'operazione mediante la quale diversi dati personali vengono messi a confronto.
- Interconnessione: l'operazione mediante la quale si mettono in relazione banche dati diverse e distinte tra loro al fine di compiere ulteriori processi di elaborazione, selezione, estrazione o raffronto.
- Limitazione: l'operazione volta a limitare l'uso futuro dei dati personali.
- Elaborazione dei dati: le operazioni che attribuiscono significatività ai dati in relazione allo scopo per il quale essi sono stati raccolti.
- Cancellazione e Distruzione: le operazioni di trattamento che consistono nella eliminazione del dato personale registrato.

5. Diritti dell'interessato e gestione delle richieste di esercizio

Il Titolare fornisce agli Interessati, distinti in ragione delle categoria di appartenenza, le informazioni di cui all'art. 13 con le modalità ed utilizzando la modulistica meglio specificate nel precedente paragrafo 10.

Relativamente ai dati personali trattati dalla Fondazione in qualità di Titolare del trattamento, gli Interessati potranno esercitare in qualunque momento i seguenti diritti:

- chiedere alla Fondazione, in persona del Direttore, la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano, l'accesso a tali dati e le seguenti informazioni:
    - finalità del trattamento;
    - categorie di dati personali in questione;
    - i destinatari o le categorie di destinatari a cui i dati sono stati o saranno comunicati, in particolare se destinatari di Paesi terzi o organizzazioni internazionali;
    - quando possibile, il periodo di conservazione previsto oppure, se ciò non è possibile, i criteri utilizzati per determinare tale periodo;
    - l'esistenza del diritto dell'interessato di chiedere al Titolare del trattamento la rettifica dei dati inesatti o l'integrazione di quelli mancanti o la loro cancellazione, al verificarsi di una delle condizioni di cui all'art. 17, paragrafo 1, del GDPR e nel rispetto delle eccezioni previste dal paragrafo 3 dello stesso articolo, o la limitazione del loro trattamento, al ricorrere di una delle ipotesi indicate nell'art. 18, paragrafo 1, del GDPR, o di opporsi al loro trattamento nei casi previsti dall'art. 21 del GDPR, paragrafo 1, del GDPR;
    - l'esistenza del diritto di proporre reclamo all'Autorità Garante per la protezione dei dati personali – www.garanteprivacy.it;
    - qualora i dati non siano stati raccolti presso l'Interessato, tutte le informazioni disponibili sulla loro origine;
    - l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'art. 22, paragrafi 1 e 4, del GDPR e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste da tale trattamento per l'Interessato;
    - qualora i dati personali siano trasferiti a un Paese terzo o a un'organizzazione internazionale, le informazioni relative all'esistenza di garanzie adeguate ai sensi dell'art. 46 relative al trasferimento;
- chiedere e ottenere, nei casi in cui la base giuridica del trattamento è costituita da un contratto o dal consenso e il trattamento viene effettuato con mezzi automatizzati, i loro dati personali in un formato strutturato e leggibile da dispositivo automatico, anche al fine di comunicare tali dati ad un altro Titolare del trattamento (c.d. diritto alla portabilità dei dati);
- revocare il loro consenso al trattamento dei suoi dati personali in qualsiasi momento, limitatamente alle ipotesi in cui il trattamento sia basato sul loro consenso per una o più specifiche finalità. Il trattamento basato sul consenso ed effettuato antecedentemente alla revoca dello stesso conserva comunque la sua liceità.

Le suddette informazioni in ordine ai diritti esercitabili sono riportate in tutti i modelli di informativa privacy rivolte alle varie categorie di Interessati.

I diritti di cui sopra potranno essere esercitati mediante comunicazione scritta da inviarsi alla Fondazione, in persona del Direttore, a mezzo raccomandata a/r presso la sede legale della Fondazione ovvero a mezzo pec presso il domicilio digitale della Fondazione.

Il Titolare del trattamento fornisce all'Interessato le informazioni relative all'azione intrapresa senza ingiustificato ritardo e comunque, al più tardi, entro un mese dal ricevimento della richiesta. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. In tal caso, il Titolare informa l'Interessato della proroga e dei motivi del ritardo entro un mese dal ricevimento della richiesta.

Se l'Interessato ha presentato la richiesta mediante mezzi elettronici, le informazioni vengono fornite, ove possibile, con mezzi elettronici, salva diversa indicazione dell'Interessato stesso. Il Titolare del trattamento fornisce all'Interessato una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'Interessato, il Titolare valuterà se addebitare un contributo spese ragionevole, quantificato tenendo conto dei costi amministrativi. Il Titolare valuterà le modalità da adottare affinché il rilascio della copia all'Interessato non leda i diritti e le libertà altrui.

Se non ottempera alla richiesta dell'Interessato, il Titolare del trattamento lo informa senza ritardo e comunque, al più tardi, entro un mese dal ricevimento della richiesta dei motivi dell'inottemperanza e della possibilità di proporre reclamo all'Autorità Garante per la protezione dei dati personali e di proporre ricorso giurisdizionale.

Le informazioni di cui agli artt. 13 e 14 del GDPR e le eventuali comunicazioni e azioni intraprese ai sensi degli articoli da 15 a 22 e dell'art. 34 del GDPR vengono fornite gratuitamente.

Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il Titolare valuterà se:

- addebitare un contributo spese ragionevole, quantificato tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta;

oppure:

- rifiutare di soddisfare la richiesta, qualora ritenga di poter dimostrare il carattere manifestamente infondato o eccessivo della richiesta, incombendo il capo al medesimo l'onere della prova.

Ai sensi dell'art. 11, paragrafo 2, del GDPR, qualora le finalità per cui la Fondazione tratta i dati personali non richiedano o non richiedano più l'identificazione dell'Interessato e la stessa possa dimostrare di non essere in grado di identificare l'Interessato lo informa, se possibile. In tale caso gli articoli da 15 a 22 non si applicano, salvo che l'Interessato, al fine di esercitare i diritti di cui ai suddetti articoli, fornisca ulteriori informazioni che ne consentano l'identificazione.

Fatto salvo quanto sopra, qualora la Fondazione nutra ragionevoli dubbi circa l'identità della persona fisica che ha presentato la richiesta, valuterà se chiedere ulteriori informazioni al fine di confermarne l'identità.

Come già precisato nel precedente paragrafo 3.7, per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei diritti loro derivanti dalla applicazione del GDPR e dalle altre normative vigenti in materia, gli Interessati possono contattare direttamente il Responsabile della Protezione dei Dati della Fondazione a mezzo raccomandata a/r o pec.

Gli accordi di designazione stipulati tra la Fondazione, in qualità di Titolare del trattamento, e i vari Responsabili del trattamento prevedono espressamente, tra l'altro, in capo a tali soggetti l'obbligo di assistere la Fondazione con misure tecniche e organizzative adeguate, tenendo conto della natura del trattamento e nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo della stessa, in qualità di Titolare del trattamento, di dare seguito alle richieste per l'esercizio dei diritti degli interessati di cui al Capo III del GDPR.

6. Gestione della violazione dei dati personali (c.d. *data breach*)

L'art. 4, paragrafo 1, n. 12), del GDPR definisce la "violazione dei dati personali" (c.d. *data breach*) come 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.

Il considerando 85 del GDPR evidenzia che una violazione di dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali agli Interessati quali, a titolo esemplificativo: la perdita del controllo di dati personali che li riguardano o la limitazione di loro diritti, discriminazione, furto o usurpazione di identità, perdite finanziarie, decifratura non autorizzata della pseudomizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo. Il Garante per la Protezione dei Dati Personali precisa che una violazione dei dati personali può compromettere la riservatezza, l'integrità e/o la disponibilità dei dati personali e individua alcuni possibili esempi:

- l'accesso o l'acquisizione di dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni (virus, malware, ecc.);
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi incendio e altre calamità;
- la divulgazione non autorizzata dei dati personali.

Gli obblighi posti in capo al Titolare del trattamento qualora si verifica una violazione di dati personali sono previsti e disciplinati dagli artt. 33 e 34 del GDPR.

In particolare, in caso di data breach, il Titolare del trattamento è tenuto a:

- notificare la violazione all'Autorità Garante per la protezione dei dati personali senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per le libertà degli Interessati. In buona sostanza, anche in ragione delle indicazioni fornite dal Garante, devono essere notificate unicamente le violazioni di dati personali che possono avere effetti avversi significativi sugli Interessati, causando danni fisici, materiali o immateriali;
- la notifica al Garante effettuata oltre il termine delle 72 ore deve essere corredata dai motivi del ritardo;

- negli accordi di designazione sottoscritti dalla Fondazione in qualità di Titolare del trattamento, con i vari Responsabili del trattamento è espressamente previsto l'obbligo in capo a tali soggetti di informare, senza ingiustificato ritardo, il Titolare qualora si verifichi una violazione di dati personali. Eguale obbligo ha assunto la Fondazione nei confronti dei vari Titolari del trattamento laddove agisce in veste di Responsabile;
- la notifica al Garante deve, almeno:
    - descrivere la natura della violazione dei dati personali verificatasi compresi, ove possibile, le categorie e il numero approssimativo di Interessati nonché le categorie e il numero approssimativo di registrazioni dei dati personali in oggetto;
    - indicare il nome e i dati di contatto del RPD o di altro punto di contatto presso cui ottenere maggiori informazioni. Per tale ragione, la Fondazione informerà, nel più breve tempo possibile, il RPD dell'accaduto;
    - descrivere le probabili conseguenze della violazione dei dati personali;
    - descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.

Qualora la Fondazione non disponga, nell'immediato, di tutte le informazioni di cui sopra, ne darà atto nella notifica riservandosi di integrare le informazioni mancanti senza ingiustificato ritardo.

La notifica verrà effettuata utilizzando il modello allegato al Provvedimento del Garante del 30 luglio 2019 sulle notifiche delle violazioni dei dati personali (doc. web n. 9126951), da scaricare provvedendo successivamente alla sua compilazione.

La notifica verrà inviata al Garante tramite posta elettronica all'indirizzo protocollo@pec.gpdp.it e dovrà essere sottoscritta digitalmente (con firma elettronica qualificata/firma digitale) ovvero con firma autografa. In tale secondo caso la notifica dovrà essere presentata unitamente a copia del documento di identità del firmatario (ossia del Legale Rappresentante della Fondazione).

L'oggetto del messaggio dovrà obbligatoriamente contenere la dicitura "Notifica violazione dati personali" e (opzionalmente) la denominazione del Titolare del trattamento.

Anche qualora la Fondazione non dia corso alla notifica ritenendo a meno improbabile che la violazione dei dati personali presenti un rischio per le libertà degli Interessati, dovrà documentare tutte le violazioni verificatesi, dando conto di volta in volta nel Registro appositamente istituito, almeno:

- delle circostanze relative alla violazioni verificatasi;
- delle sue conseguenze;
- dei provvedimenti adottati per porvi rimedio.

Il Registro è conservato presso la sede della Fondazione e dovrà essere messo a disposizione del Garante e di eventuali altre Autorità di controllo.

Qualora la violazione dei dati comporti un rischio elevato per i diritti e le libertà degli Interessati, il Titolare del trattamento è tenuto a comunicare la violazione all'Interessato/agli Interessati senza ingiustificato ritardo.

La comunicazione di cui sopra deve:

- descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali;
- indicare il nome e i dati di contatto del RPD o di altro punto di contatto presso cui ottenere maggiori informazioni;
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.

La comunicazione all'Interessato/agli Interessati non è richiesta se è soddisfatta almeno una delle seguenti condizioni:

- il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà dell'Interessato/degli Interessati;
- qualora la comunicazione in oggetto richieda sforzi sproporzionati. In tal caso, il Titolare deve invece procedere a una comunicazione pubblica o a una misura simile, tramite la quale l'Interessato/gli Interessati vengano informati dell'accaduto con analoga efficacia.

Nel caso in cui il Titolare non abbia comunicato all'Interessato/agli Interessati l'avvenuta violazione dei dati personali, il Garante o altra Autorità di controllo può valutare la probabilità che la violazione presenti un rischio elevato e chiedere che vi provveda ovvero ritenere integrata almeno una delle condizioni di cui sopra.

Si evidenzia che il Garante può prescrivere misure correttive, ai sensi dell'art. 58, paragrafo 2, del GDPR qualora rilevi una violazione delle disposizioni del Regolamento, anche per quanto riguarda l'adeguatezza delle misure di sicurezza tecniche e organizzative applicate ai dati oggetto di violazione. Sono altresì previste sanzioni pecuniarie che possono arrivare fino a 10 milioni di euro o, nel caso di imprese, fino al 2% del fatturato totale annuo mondiale.