FONDAZIONE LIRICO SINFONICA
PETRUZZELLI E TEATRI DI BARI

REGOLAMENTO PER LA PROTEZIONE DEI DATI PERSONALI

in attuazione del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati

Approvato con deliberazione del Consiglio di Indirizzo del 30 gennaio 2024

Indice

TITOLO I – DISPOSIZIONI GENERALI

Art.1 - Oggetto e finalità del regolamento

Il presente Regolamento disciplina, nel rispetto della vigente normativa comunitaria e nazionale, nonché delle Linee Guida in materia approvate dal Comitato Europeo per la Protezione dei Dati e del Garante per la protezione dei dati personali, le misure procedimentali e le regole di dettaglio inerenti la protezione delle persone fisiche, con riguardo al trattamento e alla libera circolazione dei predetti dati, laddove trattati dalla Fondazione Lirico Sinfonica Petruzzelli e Teatri di Bari (d'ora in poi "Fondazione") in qualità di titolare o di responsabile del trattamento.

In particolare, il Regolamento assicura che il trattamento dei dati avvenga unicamente per finalità istituzionali e nel rispetto dei diritti e della dignità delle persone, con particolare riferimento alla riservatezza, all'identità personale e alla protezione dei dati personali delle persone fisiche e giuridiche.

Per finalità istituzionali della Fondazione, ai fini del presente Regolamento, si intendono:

- funzioni proprie dell'Ente;
- funzioni e compiti delegati o conferiti al Fondazione da norme statali o regionali;
- funzioni svolte dal Fondazione a seguito di convenzioni, accordi, intese ed altri strumenti di collaborazione posti in essere al fine di realizzare gli interessi e corrispondere ai bisogni della comunità.

Art.2 - Definizioni

Ai sensi del presente Regolamento si intende per:

- ***Archivio***: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato o decentralizzato, ripartito in modo funzionale o geografico, disponibile su supporto analogico o digitale;
- ***Consenso dell'interessato***: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesti il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- ***Contitolari del trattamento***: due o più titolari del trattamento che determinino congiuntamente, mediante un accordo interno, le finalità e i mezzi del trattamento;
- ***Data Protection Impact Assessment (DPIA) – valutazione d'impatto sulla protezione dei dati***: processo volto a descrivere un trattamento di dati personali, valutarne la necessità e la proporzionalità, nonché gestirne gli eventuali rischi per i diritti e le libertà delle persone fisiche da esso derivanti, effettuando una valutazione del livello del rischio e determinando le misure idonee a mitigarlo;

- ***Dati biometrici***: dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentano o confermino l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- ***Dati genetici***: dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscano informazioni univoche sulla fisiologia o sulla salute di detta persona e che risultino in particolare dall'analisi di un campione biologico della medesima;
- ***Dati identificativi***: dati personali che permettono l'identificazione diretta dell'interessato;
- ***Dati personali***: 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 ad un identificativo come il nome, il 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;
- ***Particolari categorie di dati personali***: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
- ***Dati relativi alla salute***: dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelino informazioni relative al suo stato di salute;
- ***Destinatario***: persona fisica o giuridica, autorità pubblica, servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari. Il trattamento di tali dati da parte delle predette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
- ***Finalità scientifiche***: finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore;
- ***Finalità statistiche***: finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici;
- ***Finalità storiche***: finalità di studio, ricerca e documentazione di figure, fatti e circostanze del passato;
- ***Garante***: Autorità di controllo, ossia il Garante per la Protezione dei Dati Personali;
- ***Autorizzato al trattamento***: chiunque, soggetto che, agendo sotto l'autorità del Titolare del trattamento o del responsabile del trattamento, abbia accesso a dati personali, essendo stato autorizzato al loro trattamento;
- ***Interessato***: persona fisica cui si riferiscono i dai personali oggetto del trattamento;
- ***Limitazione di trattamento***: contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- ***Pseudonimizzazione***: trattamento dei dati personali in modo tale che gli stessi non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a

condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

- ***Profilazione***: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- ***Responsabile della protezione dei dati***: (RDP) persona fisica o giuridica, anche estranea all'organizzazione del Titolare o del Responsabile del trattamento, che svolga i compiti di cui all'art.39 del RGPD o ulteriori compiti affidatigli dal Titolare del trattamento;
- ***Responsabile della sicurezza informatica***: figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, nonché all'amministrazione di basi di dati, di reti e di apparati di sicurezza e di sistemi software complessi;
- ***Responsabile del trattamento***: persona fisica o giuridica, autorità pubblica, servizio o altro organismo che tratti dati personali per conto del Titolare del trattamento e distinto dal titolare stesso;
- ***RGPD***: Regolamento (UE) 2016/679 del parlamento europeo e del Consiglio del 27 aprile 2016 "*Regolamento generale sulla protezione dei dati*";
- ***Sub-responsabile del trattamento***: persona fisica o giuridica, autorità pubblica, servizio o altro organismo alla quale il responsabile del trattamento abbia affidato specifiche attività di trattamento per conto del medesimo titolare e previa autorizzazione dello stesso;
- ***Terzo***: persona fisica o giuridica, autorità pubblica, servizio o altro organismo che non sia l'interessato, il Titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile;
- ***Titolare del trattamento***: persona fisica o giuridica, autorità pubblica, servizio o altro organismo che, singolarmente o insieme ad altri, determini le finalità e i mezzi del trattamento di dati personali;
- ***Trattamento***: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- ***Violazione dei dati personali***: violazione di sicurezza che comporti 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.

Per le definizioni non riportate nel presente articolo, si rinvia all'elenco definizioni previsto dall'art.4 del RGPD.

Art.3 - Principi generali

Principi generali inerenti il trattamento dei dati:

- ***Principio di liceità, correttezza e trasparenza***: i dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- ***Principio di limitazione della finalità***: i dati devono essere 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'art.89, prf 1 del RGDP, considerato incompatibile con le finalità iniziali;
- ***Principio di minimizzazione dei dati***: i dati raccolti devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- ***Principio di esattezza***: i dati raccolti devono essere esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
- ***Principio di limitazione della conservazione***: i dati devono essere 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, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato;
- ***Principio di integrità e riservatezza***: i dati devono essere 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;
- ***Principio di responsabilizzazione***: il Titolare del trattamento è competente per il rispetto di tutti i principi suelencati e deve essere in grado di comprovare il predetto rispetto.

Nelle ipotesi in cui disposizioni legislative, regolamentari o statutarie prevedano pubblicazioni obbligatorie, il Titolare del trattamento adotta le opportune misure volte a garantire la riservatezza dei dati personali nel rispetto del quadro normativo e regolamentare vigente.

TITOLO II – SOGGETTI

Art.4 - Titolare del trattamento

La Fondazione è Il Titolare del trattamento dei dati personali raccolti in banche dati, automatizzate o cartacee, gestite dai suoi uffici per le finalità di cui all'articolo 1.

La Fondazione è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dal RGPD e richiamati nel precedente art. 3 del presente Regolamento. Pertanto, mette in atto misure tecniche ed organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al

RGPD. Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione strategica, di bilancio ed operativa, previa apposita analisi preventiva della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, la Fondazione effettua, con il parere del Responsabile della protezione dei dati di cui al successivo art. 8, se richiesto, una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell'art.35 del RGDP, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento.

Il Sovrintendente sentito il Responsabile della protezione dei dati, il Responsabile della sicurezza informatica e i Referenti, dirama le direttive necessarie per l'applicazione del presente Regolamento.

Art.5 – Contitolari del trattamento

Nel caso di esercizio associato di funzioni e servizi, nonché per le attività la cui gestione è affidata alla Fondazione, allorché due o più titolari determinano congiuntamente e in modo trasparente, mediante accordo interno, finalità e mezzi del trattamento si configura la fattispecie della contitolarità del trattamento, descritta nell'art.26 del RGPD. In questi casi, la Fondazione e il/i contitolare/i determinano in modo trasparente, mediante uno specifico accordo, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente Regolamento, con particolare riferimento all'esercizio dei diritti dell'interessato nonché i rispettivi ruoli nei confronti dell'interessato. Il contenuto essenziale dell'accordo è posto a disposizione dell'interessato che può esercitare i propri diritti, ai sensi del presente Regolamento, nei confronti e contro ciascun contitolare.

Art.6 – Referenti in materia di trattamento di dati personali

Il Sovrintendente, il Segretario Artistico, il Direttore Esecutivo, il Direttore Artistico, il Direttore Amministrativo, il Direttore di Produzione, il Direttore del Personale, il Responsabile del Personale, il Direttore Tecnico, il Responsabile Affari Generali e di Sovrintendenza ed il Responsabile della Prevenzione della Corruzione e della Trasparenza sono individuati quali Referenti in materia di trattamento dei dati personali (d'ora in poi Referenti). In tale ruolo e per i rispettivi ambiti di competenza funzionale, svolgeranno, senza la necessità di ulteriori provvedimenti di nomina, in nome della Fondazione, le attività previste dal presente Regolamento e, in particolare:

A) la modellazione dei processi di trattamento in conformità ai principi di cui all'articolo 5 del RGPD e nel rispetto dei diritti previsti dagli articoli dal 15 al 22 del RGPD;
B) la valutazione del rischio, eventualmente conforme agli articoli 35 e 36 del Reg. UE 2016/679, per ciascun processo di trattamento di dati personali e la conseguente adozione delle misure tecniche e organizzative opportune per garantire un livello di sicurezza adeguato al rischio previste dall'art. 32 del RGPD;

C) la verifica dell'applicazione delle misure tecniche e organizzative opportune per garantire un livello di sicurezza adeguato al rischio previste dall'art. 32 del RGPD;

D) l'approvazione delle eventuali modifiche o integrazioni ai processi di trattamento per il rispetto dei principi di protezione fin dalla progettazione e di protezione per impostazione predefinita di cui all'art. 25 del RGPD;

E) la definizione di idonee procedure per informare gli interessati e rispondere adeguatamente alle istanze di cui all'art. 12 del RGPD;

F) la verifica dell'attuazione delle procedure per informare gli interessati e rispondere adeguatamente alle istanze di cui all'art. 12 del RGPD;

G) la definizione delle modalità di informazione da fornire agli interessati secondo quanto previsto dagli articoli 13 e 14 del RGPD;

H) la definizione e la diffusione di idonee procedure per limitare l'impatto di eventuali violazioni di dati personali;

I) la verifica dell'attuazione delle procedure per limitare l'impatto delle violazioni di dati personali;

J) l'autorizzazione al trattamento dei dati personali e la successiva ed eventuale revoca per i dipendenti autorizzati al trattamento di dati personali;

K) la nomina, per i rispettivi ambiti di competenza funzionale e per conto della Fondazione, nel rispetto di quanto stabilito dal paragrafo 1 dell'art. 28 del RGPD, dei responsabili del trattamento dei dati personali nell'ambito di rapporti contrattuali con soggetti esterni;

L) l'elaborazione e comunicazione ai responsabili del trattamento dei dati personali, nell'ambito dei rapporti giuridici che li legano alla Fondazione delle istruzioni previste dal paragrafo 3 dell'art. 28 del RGPD;

M) l'elaborazione dell'accordo di contitolarità di cui al precedente articolo 5;

N) la comunicazione al Responsabile per la Protezione dei Dati della Fondazione di tutte le informazioni riguardanti i processi di trattamento dei dati personali per assicurare la conformità alla normativa vigente e per aggiornare il registro delle attività di trattamento previsto dall'art. 30 del RGPD;

O) la comunicazione al Responsabile per la Protezione dei Dati della Fondazione di tutte le informazioni necessarie all'autorità di controllo ed agli interessati in caso di violazione di dati personali di cui agli artt. 33 e 34 del RGPD.

Qualora un Referente del trattamento si assenti o sia impedito o sospeso per un periodo di tempo superiore a giorni 30 (trenta), il Sovrintendente provvede alla sostituzione temporanea.

Il Responsabile della protezione dei dati della Fondazione fornirà la necessaria consulenza tecnica per:

- assicurare il coordinamento delle attività svolte dai referenti, senza incidere sui diritti e sulle libertà degli interessati, con particolare riferimento alla coerenza dei processi di trattamento dei dati personali sviluppati in concorso tra i diversi servizi;
- garantire l'omogeneità dei rapporti con gli interessati in tutti i processi di trattamento dei dati personali sviluppati dalla Fondazione.

I referenti avranno cura di rispettare la posizione di indipendenza del Responsabile per la protezione dei dati della Fondazione e di fornire ogni supporto e informazione utile allo svolgimento dei compiti previsti dall'art. 39 del RGPD.

Art.7 – Responsabili del trattamento dei dati personali

Laddove se ne manifesti la necessità, è prevista l'individuazione di Responsabili del trattamento dei dati personali, ossia di persone fisiche o giuridiche esterne all'Ente, a cui siano affidati trattamenti di dati personali o singole operazioni di trattamento mediante convenzioni, contratti, incarichi professionali o altra forma giuridicamente equipollente.
In tali ipotesi, nella convenzione, contratto, incarico professionale o altro atto è prevista espressamente la designazione degli stessi soggetti affidatari quali Responsabili del trattamento dei dati personali ai sensi dell'art. 28 del RGPD e i predetti soggetti sono tenuti, preliminarmente, a fornire la descrizione delle misure tecniche e organizzative adeguate in modo tale che:

- il trattamento soddisfi i requisiti del RGPD;
- il trattamento garantisca la tutela dei diritti dell'interessato;
- il trattamento sia eseguito secondo specifiche indicazioni che i Referenti forniscono già in fase di avvio di procedura di scelta del contraente; allo scopo, di norma, i Referenti corredano la documentazione di gara con la personalizzazione delle Clausole Contrattuali Tipo di cui alle decisioni della Commissione UE n. 914/2021 e n. 915/2021.

La designazione dei Responsabili del trattamento avviene a cura dei Referenti conformemente a quanto previsto dall'articolo 6**.**

Art.8 – Responsabile della protezione dei dati personali

Il Responsabile della protezione dei dati personali dell'Ente (di seguito RDP) è, di regola, un dirigente ovvero un funzionario al quale potrà essere eventualmente conferito l'incarico di alta professionalità, dipendente della Fondazione che possegga i requisiti di cui all'art. 37 del RGPD.

In mancanza di un dipendente con le caratteristiche di cui al punto precedente, il RDP può essere un soggetto esterno, persona fisica e/o giuridica, affidatario di apposito contratto di servizi per il quale sia verificata l'assenza di conflitto di interessi ed il possesso di adeguata conoscenza della normativa e delle prassi di gestione dei dati personali, anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati, nonché della capacità di assolvere i compiti assegnati a tale figura dall'art.39 del RGPD.

Al momento dell'individuazione del Responsabile della protezione dei dati, il Sovrintendente provvede, tempestivamente alla pubblicazione dei dati identificativi e i contatti del RDP sul sito web istituzionale dell'Ente, rendendoli accessibili da un apposito link e alla comunicazione dei medesimi dati al Garante, ai componenti degli organi di governo, a tutti i dipendenti della Fondazione, nonché ai componenti degli organi di controllo interno.

Il RDP è tenuto al segreto e/o alla riservatezza in merito e supporta il Titolare del trattamento ed i Referenti, in ogni adempimento connesso al trattamento dei dati:

- ponendo in essere ogni attività preliminare, propedeutica e/o connessa al trattamento dei dati e finalizzata alla mappatura dei trattamenti, all'esito dell'eventuale valutazione d'impatto del trattamento dei dati ed alle modalità operative per il relativo trattamento;

- supportando i Referenti nella mappatura delle aree di attività e nella valutazione del grado di rischio in termini di protezione dei dati;
- informando e sensibilizzando il Titolare del trattamento ed i Referenti, nonché i dipendenti dell'Ente relativamente agli obblighi derivanti dal presente Regolamento e da altre disposizioni vigenti in tema di protezione dei dati;
- sorvegliando l'osservanza del Regolamento, di altre disposizioni dell'Unione o dello Stato relative alla protezione dei dati nonché delle politiche del Titolare del trattamento o dei Referenti, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità;
- collaborando con il Responsabile della sicurezza informatica in modo da assicurare l'effettività delle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti;
- cooperando con il Garante e fungere da punto di contatto con il medesimo su ogni questione connessa al trattamento dei dati.

Il RPD è tenuto a manifestare il proprio dissenso alle decisioni o ai provvedimenti o ai comportamenti incompatibili con il RGPD adottati o tenuti dai componenti degli organi di governo e di controllo, dai componenti degli organi di gestione, dai Responsabili del trattamento e dai dipendenti ogni qual volta ne venga a conoscenza, dandone comunicazione al Titolare del trattamento nonché ai Referenti interessati dai rilievi e, ove necessario, al Responsabile della sicurezza informatica. I Responsabili del trattamento, qualora non condividano i rilievi formulati dal RPD, comunicano a quest'ultimo e al Titolare del trattamento le proprie osservazioni. Il Titolare del trattamento dei dati, per il tramite del Sovrintendente e sulla base delle indicazioni fornite dal RPD, previa valutazione delle conclusioni del RDP e delle controdeduzioni dei Responsabili del trattamento, dirama le direttive utili a prevenire il ripetersi delle violazioni rilevate.

Al fine di consentire al Responsabile per la protezione dei dati di svolgere adeguatamente il proprio incarico, il Titolare del trattamento, i Referenti ed i Responsabili del trattamento garantiscono il suo tempestivo e adeguato coinvolgimento in ogni questione riguardante la protezione dei dati personali. In particolar modo, è necessario che il Responsabile per la protezione dei dati:

- svolga i propri compiti in maniera indipendente ed in assoluta autonomia;
- sia coinvolto in ogni situazione in cui debbano essere assunte decisioni che impattano sulla protezione dei dati;
- disponga tempestivamente di tutte le informazioni pertinenti, al fine di poter rendere idonea consulenza;
- sia consultato tempestivamente qualora si verifichi una violazione dei dati o altro incidente connesso alla gestione dei medesimi;
- possa accedere agli uffici dell'Ente al fine di fornire supporto e assicurare lo scambio di informazioni utili all'espletamento dell'incarico;
- riceva collaborazione attiva da parte dei Direttori di Area e dei dipendenti dell'Ente nell'espletamento dei propri adempimenti.

Art.9 – Responsabile della sicurezza informatica

Al fine di assicurare che il sistema informatico della Fondazione sia strutturato e gestito in modo da garantire le misure tecniche e organizzative adeguate per la necessaria protezione dei dati personali trattati attraverso lo stesso sistema, il Sovrintendente, con proprio provvedimento, nomina, nell'ambito dei servizi informatici della Fondazione, il Responsabile della sicurezza informatica, ossia l'Amministratore di sistema responsabile della sicurezza delle banche dati detenute con strumenti informatici nonché custode delle stesse.

Il Responsabile della sicurezza informatica, anche tramite affidamento ad un soggetto esterno all'Ente debitamente nominato Responsabile del trattamento, provvede a:

a) gestire l'*hardware* e i *software* dei *server* e delle postazioni di lavoro informatizzate;

b) impostare e gestire un sistema di autenticazione informatica per i trattamenti di dati personali effettuati con strumenti elettronici;

c) registrare gli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema;

d) impostare e gestire gli adeguati sistemi di profilazione per i componenti degli organi di governo e di controllo interno, per il Responsabile della protezione dei dati e per i Referenti effettuati con strumenti elettronici nonché per quanti siano autorizzati all'accesso ai dati personali contenuti nelle banche-dati informatizzati;

e) collaborare alla costante verifica che la Fondazione abbia adottato le misure tecniche adeguate alla garanzia di sicurezza dei dati personali, nel rispetto delle indicazioni in materia fornite dal RGPD;

f) suggerire ai Referenti l'adozione e l'aggiornamento delle misure di sicurezza adeguate per assicurare la sicurezza dei dati atte a che i dati personali oggetto di trattamento siano custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Ai fini dell'attuazione di quanto su descritto, il Responsabile della sicurezza informatica deve:

a) assegnare e gestire il sistema di autenticazione informatica nel rispetto delle indicazioni fornite nel RGPD e quindi, fra le altre, generare, sostituire ed invalidare, in relazione agli strumenti e alle applicazioni informatiche utilizzate, le parole chiave ed i Codici identificativi personali da assegnare ai soggetti autorizzati al trattamento svolgendo anche la funzione di custode delle copie delle credenziali. In particolare, deve:

   - custodire le parole chiave di natura amministrativa degli strumenti informatici in modo da evitare accidentali aperture della busta ed evitare di aprire tali buste;
   - nel caso in cui il Referente abbia la necessità indifferibile di accedere ad un elaboratore in caso di assenza o impedimento dell'incaricato che lo utilizza abitualmente, consentire al Referente, con una nuova parola chiave, l'accesso all'elaboratore sul quale egli possa intervenire unicamente per necessità di operatività e sicurezza del sistema informativo; informare il dipendente autorizzato al trattamento allorché rientri in servizio e consegnargli una nuova parola chiave diversa da quella consegnata al Referente durante la sua assenza;

b) procedere, più in particolare, alla disattivazione dei Codici identificativi personali, in caso di perdita della qualità che consentiva ai soggetti interessati l'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei Codici identificativi personali per oltre 6 (sei) mesi;

c) dotare e attivare nonché aggiornare adeguati programmi antivirus, firewall ed altri strumenti software o hardware atti a garantire la massima misura di sicurezza e protezione dei dati trattati attraverso gli elaboratori del sistema informativo contro il rischio di intrusione e contro l'azione dei virus informatici, ed utilizzando le conoscenze acquisite in base al progresso tecnico software e hardware, verificandone l'installazione, l'aggiornamento ed il funzionamento degli stessi;

d) aggiornare periodicamente, con frequenza almeno annuale (oppure semestrale se si trattano particolari categorie di dati personali o dati personali relativi a condanne penali e reati), i programmi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti, informandone con apposita relazione il rispettivo referente nonché il Responsabile della Protezione dei Dati Personali;

e) aggiornare, nell'ambito dei sistemi informativi della Fondazione, il profilo autorizzativo del soggetto autorizzato al trattamento in conformità al relativo incarico formalizzato e trasmesso dal rispettivo Referente;

f) curare l'adozione e l'aggiornamento delle predette misure di sicurezza;

g) impartire a tutti i soggetti che comunque svolgano trattamento dei dati istruzioni organizzative dirette al salvataggio quotidiano dei dati; assumere, pertanto, tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di back-up; assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro;

h) adottare procedure per la custodia delle copie di sicurezza dei dati e per il ripristino della disponibilità dei dati e dei sistemi;

i) predisporre un piano di controlli periodici, da eseguirsi con cadenza almeno annuale, dell'efficacia delle misure di sicurezza;

j) indicare al personale competente o provvedere direttamente alla distruzione e smaltimento dei supporti informatici di memorizzazione logica o alla cancellazione dei dati allorché si provveda al loro reimpiego.

Il Responsabile della sicurezza informatica:

a) è soggetto al tassativo divieto di leggere, copiare, stampare o visualizzare i documenti o i dati degli utenti memorizzati sul sistema a meno che questo sia strettamente indispensabile per le operazioni attinenti ai ruoli allo stesso assegnati; tale divieto vale anche nei confronti di quanti non siano stati autorizzati dal Titolare o dai Referenti a conoscere i dati personali oggetto di trattamento;

b) è obbligato a dare tempestiva comunicazione al Titolare e ai Referenti interessati nonché al Responsabile della protezione dei dati dei problemi di affidabilità sia dell'hardware che dei software eventualmente rilevati.

Art.10 - Soggetti autorizzati al trattamento dei dati

I Referenti nominano, con proprio provvedimento, per ogni processo di trattamento presente nella propria articolazione, i relativi soggetti autorizzati, che provvedono, a gestire i dati medesimi assicurando il rispetto integrale delle disposizioni vigenti in materia, nel rispetto delle direttive impartite dal rispettivo Referente.

La nomina di ogni singolo soggetto autorizzato deve avvenire per iscritto e deve individuare puntualmente l'ambito del trattamento consentito, atteso che ogni incaricato non può svolgere operazioni di trattamento dei dati che non gli siano stati espressamente assegnati.

Pertanto, nel provvedimento di nomina devono essere espressamente indicati:

- i processi e le attività per lo svolgimento dei quali è indispensabile il trattamento dei dati personali;
- le operazioni di trattamento eseguibili, con particolare riferimento alla comunicazione e alla diffusione di particolari categorie di dati personali e dati personali relativi a condanne penali e reati;
- gli eventuali limiti al trattamento;
- le misure di sicurezza da adottare da parte degli stessi autorizzati.

Il provvedimento di nomina deve essere notificato al dipendente interessato, il quale non può esimersi dalla sua accettazione e attuazione.

Gli incaricati del trattamento operano sotto l'autorità dei Referenti, garantendo la massima riservatezza e attenendosi alle istruzioni impartite per iscritto, con particolare riferimento alla custodia degli atti e documenti analogici e digitali contenenti particolari categorie di dati personali e dati personali relativi a condanne penali e reati e alle relative misure di sicurezza, provvedendo:

- al trattamento dei dati personali per lo svolgimento delle funzioni istituzionali della Fondazione, in conformità alle disposizioni del RGPD;
- alla raccolta e la registrazione per gli scopi inerenti all'attività istituzionale svolta da ciascuno;
- alla verifica in ordine alla loro pertinenza, completezza e non eccedenza delle finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal Referente;
- alla conservazione, rispettando le misure di sicurezza predisposte al riguardo.

Nel caso di allontanamento anche temporaneo dalla propria postazione di lavoro, il dipendente autorizzato verifica che non vi sia possibilità, per chiunque non sia autorizzato all'accesso ai dati, di accedere alle banche-dati e/o ai dati personali, anche su supporto cartaceo, per i quali è in corso un qualsiasi tipo di trattamento.

Il flusso di dati tra Titolare del trattamento, Referenti, soggetti autorizzati, Responsabile della sicurezza informatica, Responsabile della protezione dei dati, Sovrintendente, componenti degli organi di governo e di controllo interno non costituisce "comunicazione" in senso tecnico quale operazione di trattamento. Ne consegue che tale flusso non è soggetto ai limiti previsti per tale operazione di trattamento, ai sensi del successivo art.31 del presente Regolamento.

TITOLO III – DIRITTI DELL'INTERESSATO

Art.11 - Diritto alla comunicazione trasparente per l'esercizio dei propri diritti

In ogni comunicazione inerente il trattamento dei dati i Referenti adottano misure appropriate per fornire all'interessato tutte le informazioni in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

L'interessato ha diritto di ricevere le informazioni relative all'azione intrapresa riguardo a una richiesta relativa all'esercizio dei diritti di cui al presente Titolo senza ingiustificato ritardo e, comunque, al più tardi entro 30 (trenta) giorni dal ricevimento della richiesta stessa. Qualora, in considerazione della complessità e del numero delle richieste, si renda necessario prorogare il termine, il Referente informa tempestivamente l'interessato della necessità di proroga e dei motivi a base della stessa che, comunque, non può avere una durata superiore a 60 (sessanta) giorni. Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con gli stessi mezzi.

Qualora il Referente ritenga di non ottemperare alla richiesta dell'interessato, provvede ad informarlo tempestivamente dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale.

Le informazioni e/o comunicazioni di cui ai diritti elencati nel presente Titolo sono gratuite, tuttavia, se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il Referente può addebitare un contributo spese pari al tariffa prevista dalla Fondazione per il rilascio di copie di atti amministrativi, in ragione dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta, oltre ai costi per la spedizione postale della documentazione, ove tale modalità di trasmissione sia espressamente richiesta dall'interessato. Inoltre, nella medesima ipotesi e previa dimostrazione del carattere manifestamente infondato o eccessivo della richiesta, il Referente può rifiutare di soddisfare la richiesta medesima.

Salvo l'ipotesi di trattamenti che non richiedono l'identificazione dell'interessato, di cui all'art. 11 del RGPD, qualora il Referente nutra ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta per esercitare uno o più diritti di cui al presente Titolo, può richiedere ulteriori informazioni necessarie per confermarne l'identità.

Art.12 - Diritto di accesso

L'interessato ha il diritto di ottenere dal Referente la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalità del trattamento;

b) le categorie di dati personali in questione;

c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;

d) laddove possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

e) l'esistenza del diritto dell'interessato di chiedere alla Fondazione la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;

f) il diritto di proporre reclamo a un'autorità di controllo;

g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;

h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, del RGPD e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Il Referente provvede a soddisfare la richiesta dell'interessato nel più breve tempo possibile e comunque non oltre 30 (trenta) giorni.

Art.13 - Diritto di rettifica e di integrazione

L'interessato ha il diritto di ottenere dal Referente la rettifica dei suoi dati personali inesatti nonché, tenuto conto delle finalità del trattamento, l'integrazione dei suoi dati personali incompleti, anche fornendo una dichiarazione integrativa. L'istanza di rettifica o integrazione è formulata dall'interessato per iscritto e inviata anche tramite posta elettronica.

Alla rettifica ovvero all'integrazione dei dati richiesta dall'interessato provvede il Referente cui ineriscono i dati da rettificare o integrare, senza ritardo e, comunque, entro 5 (cinque) giorni lavorativi dalla data di arrivo della predetta istanza.

Dell'eseguita rettifica o integrazione ovvero della motivata inammissibilità è data tempestiva comunicazione all'interessato, con il medesimo mezzo mediante il quale è stata formulata l'istanza.

Il Referente dei dati oggetto della richiesta deve comunicare, con tempestività:

- a ciascuno dei destinatari cui sono stati trasmessi;
- alle strutture interne alla Fondazione che trattano i medesimi dati

la rettifica del trattamento effettuata, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato.

Art.14 - Diritto all'oblio

L'interessato ha il diritto di ottenere dalla Fondazione la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il Referente ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati e non sussiste altro fondamento giuridico per il trattamento;

b) l'interessato revoca il consenso su cui si basa il trattamento e non sussiste altro fondamento giuridico per il trattamento;

c) l'interessato si oppone al trattamento ai sensi del successivo art.17, per motivi connessi alla sua situazione particolare e non sussiste alcun motivo legittimo cogente prevalente per procedere al trattamento, che prevalgano sugli interessi, sul diritto e sulle libertà dell'interessato;

d) i dati personali sono stati trattati illecitamente;

e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dalla vigente normativa nazionale e/o comunitaria cui è soggetto la Fondazione.

L'istanza è formulata dall'interessato per iscritto e inviata anche tramite posta elettronica. Il Referente, se ha reso pubblici dati personali ed è obbligato a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per cancellare qualsiasi link, copia o riproduzione dei dati di cui è stata chiesta la cancellazione.

Le disposizioni di cui al presente articolo non si applicano nella misura in cui il trattamento sia necessario:

a) per l'esercizio del diritto alla libertà di espressione e di informazione;

b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dalla vigente normativa nazionale e/o comunitaria cui è soggetta la Fondazione o per l'esecuzione di un compito svolto nel pubblico interesse;

c) per motivi di interesse pubblico nel settore della sanità pubblica;

d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, nella misura in cui l'esercizio del diritto all'oblio rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;

e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Il Referente dei dati oggetto della richiesta deve comunicare, con tempestività:

- a ciascuno dei destinatari cui sono stati trasmessi;
- alle strutture interne alla Fondazione che trattano i medesimi dati;

la cancellazione effettuata, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato.

Art.15 - Diritto di limitazione di trattamento

L'interessato ha il diritto di ottenere dal Referente in materia di trattamento dei dati personali la limitazione del trattamento quando ricorre una delle seguenti ipotesi:

a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario alla Fondazione per verificare l'esattezza di tali dati personali;

b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;

c) benché l'Ente non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

d) l'interessato si è opposto al trattamento, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi della Fondazione rispetto a quelli dell'interessato.

Se il trattamento è limitato a norma del presente articolo, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o dello Stato.

Qualora la limitazione sia revocata, il Referente informa l'interessato tempestivamente e, comunque, prima che la revoca sia operativa.

Il Referente dei dati oggetto della richiesta deve comunicare, con tempestività:

- a ciascuno dei destinatari cui sono stati trasmessi;
- alle strutture interne alla Fondazione che trattano i medesimi dati

la limitazione del trattamento effettuata, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato.

Art.16 - Diritto alla portabilità dei dati

L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti alla Fondazione e ha il diritto di trasmettere tali dati ad altro Titolare del trattamento senza impedimenti da parte dell'Ente qualora il trattamento dei dati sia basato sul consenso dell'interessato stesso e il trattamento sia effettuato con mezzi automatizzati.

Il diritto alla portabilità non si applica ai trattamenti svolti dalla Fondazione necessari per l'esecuzione di un compito di interesse pubblico.

Art.17 - Diritto di opposizione

L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano necessario per l'esecuzione di un compito di interesse pubblico di cui è investita la Fondazione, compresa la profilazione sulla base di tali disposizioni.

Il Referente dei dati si astiene dal trattare ulteriormente i dati personali salvo che dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

L'opposizione è formulata dall'interessato per iscritto ed è inviata al Referente anche per posta elettronica.

Da parte del Referente il relativo diritto è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.

Art.18 - Diritti connessi all'attuazione di processi decisionali automatizzati

L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona, salvo l'ipotesi in cui la decisione:

a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e la Fondazione;

b) sia autorizzata dalla vigente normativa nazionale e/o comunitaria, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;

c) si basi sul consenso esplicito dell'interessato.

Nei casi di cui alle lettere a) e c), il Referente attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato.

Le decisioni di cui alle lettere a), b), c) non si basano sulle particolari categorie di dati personali, salvo nell'ipotesi in cui l'interessato non abbia prestato il proprio consenso esplicito al trattamento di tali dati per una o più finalità specifiche o il trattamento sia necessario per motivi di interesse pubblico rilevante e proporzionato alla finalità perseguita, sulla base della vigente normativa nazionale e/o comunitaria.

TITOLO IV – MODALITA' DI TRATTAMENTO E SICUREZZA DEI DATI

Art.19 - Attività propedeutiche al trattamento dei dati

Le attività propedeutiche consistono nell'insieme di azioni finalizzate alla ricognizione e alla valutazione delle misure di sicurezza normative, organizzative e tecnologiche che la Fondazione è tenuto ad osservare a tutela della privacy di tutti i dati trattati. Le predette attività sono svolte dal Responsabile della protezione dei dati, sulla base di analisi, studi, interviste direttamente realizzate presso gli uffici della Fondazione nonché sulla scorta delle informazioni raccolte presso il Sovrintendente, i Referenti, i Responsabili del trattamento, il Responsabile per la sicurezza informatica, ognuno nell'ambito delle rispettive competenze.

Art.20 – Registro delle attività di trattamento dei dati personali

Il Responsabile della protezione dei dati, nell'ambito delle attività propedeutiche al trattamento di cui al precedente art.19, provvede alla predisposizione del Registro generale dei trattamenti, da sottoporre al Sovrintendente, per l'approvazione mediante proprio provvedimento.

Nel predetto Registro, per ogni tipologia di trattamento sono indicati:

- articolazione dell'Ente competente al trattamento;
- nome e dati di contatto del Responsabile del trattamento e del RPD;

- categorie di trattamenti effettuati: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, interconnessione, limitazione, cancellazione, distruzione, profilazione, pseudonimizzazione, ogni altra operazione applicata a dati personali;
- natura dei dati trattati, specie se particolari categorie di dati personali e dati personali relativi a condanne penali e reati;
- eventuali altre strutture, anche esterne, che concorrono al trattamento dei dati e che possono pertanto accedere alla banca dati, ivi compreso l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
- i luoghi di custodia dei dati e il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

Ai fini dell'aggiornamento, qualora siano avviati nuovi processi di trattamento, anche a seguito dell'acquisizione di nuovi software gestionali, i Referenti devono darne immediata comunicazione al Responsabile della protezione dei dati e al Responsabile della sicurezza informatica.

Art.21 – Liceità del trattamento e consenso dell'interessato

Il trattamento degli altri dati personali, effettuato dalla Fondazione nell'ambito delle finalità di cui al precedente articolo 1 del presente Regolamento, è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

- l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità per le quali il Referente abbia verificato l'assenza di una posizione di soggezione da parte dell'interessato nei confronti della Fondazione;
- il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso interessato;
- il trattamento è necessario all'adempimento di un obbligo legale a cui è soggetto la Fondazione;
- il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica, se non trova applicazione alcuna delle altre predette condizioni;
- il trattamento è necessario per l'esecuzione di un compito di interesse pubblico di cui è investita la Fondazione.

La Fondazione non è tenuta a chiedere il consenso dell'interessato nelle ipotesi in cui il trattamento dei dati sia effettuato nello svolgimento dei propri compiti istituzionali di interesse pubblico o, comunque, nei casi previsti

- dall'articolo 6, paragrafo 1, lettere dalla b) alla f);
- dall'articolo 9, paragrafo 2, lettere dalla b) alla j)

dell'RGPD.

In ogni altra ipotesi, il consenso al trattamento dei dati deve essere libero, specifico, informato e inequivocabile e, laddove il trattamento sia basato sul consenso, il Referente deve essere in grado di dimostrare la sussistenza di tale consenso da parte dell'interessato. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre

questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente Regolamento è vincolante.

Nelle ipotesi in cui l'interessato sia un minore di età inferiore a 14 anni, il trattamento dei dati è lecito se e nella misura in cui il consenso è prestato o autorizzato dal titolare delle responsabilità genitoriali.

Ciascun Referente, limitatamente al proprio ambito di competenza, adegua la modulistica, sia essa cartacea che digitale, alle previsioni dei precedenti capoversi.

L'interessato ha diritto di revocare il proprio consenso in qualsiasi momento sebbene la revoca non pregiudichi la liceità del trattamento basato sul consenso, effettuato preliminarmente alla revoca.

Laddove il trattamento per una finalità diversa da quella per cui i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto normativo comunitario o nazionale che "*costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi*", ai sensi dell'articolo 23, paragrafo 1 del RGPD, al fine di verificare se tale trattamento sia compatibile con la finalità per cui i dati erano stati inizialmente raccolti, il Referente del trattamento dovrà valutare:

- ogni nesso fra le finalità per cui i dati erano stati raccolti e le finalità dell'ulteriore trattamento previsto;
- il contesto in cui i dati personali sono stati raccolti, con particolar riferimento alla relazione fra l'interessato e la Fondazione;
- la natura dei dati personali, specialmente se siano trattate particolari categorie di dati personali e/o dati personali relativi a condanne penali e reati;
- delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;
- dell'esistenza di garanzie adeguate, quali la cifratura o la pseudonimizzazione.

Art.22 - Informativa agli interessati

Nel rispetto della normativa vigente, con particolare riferimento all'esercizio dei diritti di cui al Titolo III del presente Regolamento, l'interessato deve ricevere le seguenti informazioni:

- identità e dati di contatto del Titolare e del Responsabile della protezione dei dati;
- natura obbligatoria o facoltativa del conferimento dei dati;
- finalità a cui i dati sono destinati;
- modalità di trattamento;
- soggetti o categorie di soggetti a cui i dati possono essere comunicati;
- diritti connessi al trattamento dei dati;
- conseguenze dell'eventuale rifiuto a consentire il trattamento.

A tal fine, i Referenti utilizzano apposita modulistica da cui si evincano tutte le informazioni utili per il soggetto interessato, nel momento in cui sono raccolti i dati personali.

Art.23 - Informativa per i dati da raccogliere presso l'interessato

In caso di raccolta presso l'interessato di dati che lo riguardano, oltre alle informazioni di cui al precedente art.22, il Referente dei dati fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni necessarie per garantire un trattamento corretto e trasparente:

a) periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

b) esistenza del diritto dell'interessato di chiedere alla Fondazione l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

c) qualora il trattamento di dati non identificabili come particolari categorie di dati personali né come dati personali relativi a condanne penali e reati sia basato sul consenso espresso dall'interessato per una o più specifiche finalità oppure il trattamento di particolari categorie di dati personali sia basato sul consenso espresso dall'interessato per una o più specifiche finalità e la vigente normativa nazionale e/o comunitaria abbia disposto l'irrevocabilità del divieto di trattare le stesse particolari categorie di dati personali, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

d) diritto di proporre reclamo a un'autorità di controllo oltre che la facoltà di rivolgersi all'autorità giudiziaria

e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;

f) esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Qualora si renda necessario un ulteriore trattamento dei dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento, il Referente di questo ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al presente articolo.

Le disposizioni di cui al presente articolo non si applicano se e nella misura in cui l'interessato disponga già delle predette informazioni.

Art.24 - Informativa per i dati da ottenere da soggetti diversi dall'interessato

Qualora i dati non siano stati ottenuti presso l'interessato, oltre alle informazioni di cui ai precedenti articoli 22 e 23, il Referente dei dati fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, indicazioni relative alla fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico.

Il Referente fornisce le informazioni di cui al presente articolo:

a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi, entro 1 (un) mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;

b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato;

c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati.

Qualora si renda necessario un ulteriore trattamento dei dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento, il Referente di questo ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al presente articolo.

Le disposizioni di cui al presente articolo non si applicano:

a) se e nella misura in cui l'interessato disponga già delle predette informazioni;

b) comunicare tali informazioni risulti impossibile o implicherebbe uno sforzo sproporzionato. In tali casi, il Referente adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni;

c) l'ottenimento o la comunicazione sono espressamente previsti dalla vigente normativa nazionale e/o comunitaria e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato;

d) qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dalla vigente normativa nazionale e/o comunitaria, compreso un obbligo di segretezza previsto per legge.

Art.25 – Misure per la sicurezza dei dati personali

I Referenti e il Responsabile per la sicurezza informatica, unitamente al Responsabile della protezione dei dati, per quanto di rispettiva competenza, dopo aver effettuato una adeguata valutazione dei rischi per ogni processo di trattamento, pongono in essere adeguata misure tecniche ed organizzative atte a garantire un livello di sicurezza correlato al rischio tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono: la pseudonimizzazione; la minimizzazione; la cifratura dei dati

personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi con cui sono trattati i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

La conformità del trattamento dei dati al RGDP in materia di protezione dei dati personali può essere dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato.

I Referenti provvedono a impartire adeguate istruzioni sul rispetto delle predette misure ai soggetti autorizzati al trattamento.

I Referenti provvedono, nell'ambito dei propri poteri di controllo, a effettuare periodiche verifiche sulla corretta applicazione della normativa in materia di trattamento dei dati personali nell'ambito dei Servizi cui sono preposti, in accordo con i controlli specifici effettuati dal Responsabile della protezione dei dati.

Art.26 – Valutazione di impatto sulla protezione dei dati

Nel caso in cui una tipologia di trattamento, specie se prevede, in particolare, l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Referente, prima di effettuarlo, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA), considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento, finalizzata a realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.

Ai fini della decisione di effettuare o meno la DPIA si tiene conto, oltre che dell'art. 35 del RGPD, dell'elenco allegato al provvedimento del Garante n. 467 dell'11 ottobre 2018.

Fermo restando quanto indicato dal citato art. 35 del RGDP, al paragrafo 3, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:

a) trattamenti valutativi o di *scoring*, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;

b) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;

c) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;

d) trattamenti di particolari categorie di dati personali o dati di natura estremamente personale;

e) trattamenti di dati su larga scala, tenendo conto: del numero di numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati

oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;

f) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;

g) dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di squilibrio nel rapporto con la Fondazione, come i dipendenti dell'Ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;

h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;

i) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale, condurre una DPIA, salvo che il Referente, sentito il Responsabile della protezione dei dati e il Responsabile per la sicurezza informatica, ritenga motivatamente che non può presentare un rischio elevato. In ogni caso, il Referente può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA. Il predetto Referente deve consultarsi con il Responsabile della protezione dei dati anche per assumere la decisione di effettuare o meno la DPIA, documentando nella stessa DPIA la consultazione effettuata e le decisioni conseguentemente assunte. Il Referente garantisce l'effettuazione della DPIA ed è responsabile della stessa.

Il Responsabile della protezione dei dati può proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale.

Il Responsabile per la sicurezza informatica fornisce il necessario supporto durante lo svolgimento della DPIA e può, a sua volta, proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

La DPIA non è necessaria nei casi seguenti:

a) se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, paragrafo 1, del RGDP;

b) se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;

c) se il trattamento è stato sottoposto a verifica da parte del Garante prima del 25 maggio 2018 in condizioni specifiche che non hanno subito modifiche;

d) se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.

Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante e che proseguano con le stesse modalità oggetto di tale verifica.

La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:

a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati. Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);

b) valutazione della necessità e proporzionalità dei trattamenti, sulla base:
   - delle finalità specifiche, esplicite e legittime;
   - della liceità del trattamento;
   - dei dati adeguati, pertinenti e limitati a quanto necessario;
   - del periodo limitato di conservazione;
   - delle informazioni fornite agli interessati;
   - del diritto di accesso e portabilità dei dati;
   - del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
   - dei rapporti con i responsabili del trattamento;
   - delle garanzie per i trasferimenti internazionali di dati;
   - consultazione preventiva del Garante;

c) valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;

d) individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il RGPD, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Il Referente può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.

Il Referente, per il tramite del Titolare del trattamento, deve consultare il Garante prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. La medesima consultazione è prevista anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.

La DPIA deve essere effettuata - con eventuale riesame delle valutazioni condotte - anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.

E’ pubblicata sul sito istituzionale dell’Ente, in apposita sezione, una sintesi delle principali risultanze del processo di valutazione ovvero una semplice dichiarazione relativa all’effettuazione della DPIA.

Art.27 – Violazione dei dati personali

Per violazione dei dati personali (c.d. *data breach*) si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dalla Fondazione.

Il Referente, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede, per il tramite del responsabile dell’ufficio Affari Generali e di Sovrintendenza, alla notifica della violazione al Garante. La notifica dovrà avvenire entro 72 ore dalla notizia dell’avvenuta violazione e, comunque, senza ingiustificato ritardo.

I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del RGPD, sono i seguenti:

a) danni fisici, materiali o immateriali alle persone fisiche;

b) perdita del controllo dei dati personali;

c) limitazione dei diritti, discriminazione;

d) furto o usurpazione d’identità;

e) perdite finanziarie, danno economico o sociale.

f) decifratura non autorizzata della pseudonimizzazione;

g) pregiudizio alla reputazione;

h) perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, dati personali relativi a condanne penali e reati).

Se il Referente ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. I rischi per i diritti e le libertà degli interessati possono essere considerati “elevati” quando la violazione può, a titolo di esempio:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- riguardare categorie particolari di dati personali;
- comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
- comportare rischi imminenti e con un’elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).

La notifica deve avere il contenuto minimo previsto dall'art. 33 del RGPD, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al su citato art. 33.

Il Referente deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante al fine di verificare il rispetto delle disposizioni del RGPD.

Art.28 – Modalità di trattamento di particolari categorie di dati personali

La Fondazione, di regola, non tratta dati personali che rientrano nelle categorie di cui agli articoli 9 e 10 del RGPD. Nei casi in cui è necessario trattare tali categorie di dati personali, la Fondazione adegua il trattamento a quanto previsto dagli articoli 2-sexies, 2-septies e 2-octies del D.Lgs. 196/2003 oltre che alle previsioni dell'art. 9 e dell'art. 10 del RGPD, evitando, per quanto compatibile, il ricorso al consenso dell'interessato. Il ogni caso, il consenso potrà costituire base giuridica del trattamento solo dopo che il Referente abbia verificato l'assenza di una posizione di soggezione da parte dell'interessato nei confronti della Fondazione.

Pertanto, fermo restando quanto previsto al precedente capoverso, il trattamento delle particolari categorie di dati personali è consentito quando si verifichi una delle seguenti ipotesi:

a) l'interessato abbia prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche;

b) il trattamento sia necessario per assolvere gli obblighi ed esercitare i diritti specifici della Fondazione o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dalla vigente normativa nazionale e/o comunitaria o da un contratto collettivo, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;

c) il trattamento sia necessario per la tutela di un interesse vitale dell'interessato o di un'altra persona fisica, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

d) il trattamento riguardi dati personali resi manifestamente pubblici dall'interessato;

e) il trattamento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;

f) il trattamento sia necessario per motivi di interesse pubblico rilevante sulla base della vigente normativa nazionale e/o comunitaria, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti e le libertà fondamentali dell'interessato;

g) relativamente ai dipendenti della Fondazione, il trattamento sia necessario per finalità di valutazione della capacità lavorativa dei medesimi;

h) il trattamento sia necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici laddove sia proporzionato alla finalità perseguita,

rispetti l'essenza del diritto alla protezione dei dati e preveda misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

I Referenti, per quanto di rispettiva competenza, adottano idonee e preventive misure di sicurezza che valgano a ridurre al minimo i rischi di distruzione o perdita, anche accidentale dei dati stessi nonché di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, al fine di evitare che la Fondazione possa incorrere in responsabilità civile, penale, amministrativa e/o contabile.

Art.29 - Modalità di trattamento dei dati personali relativi a condanne penali e reati

Sono definiti "*dati personali relativi a condanne penali e reati*" i dati che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (*ad esempio*, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato.

Il trattamento dei predetti dati deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dalla vigente normativa nazionale e/o comunitaria che preveda garanzie appropriate per i diritti e le libertà degli interessati.

Pertanto, il trattamento dei dati relativi a condanne penali e reati è consentito solo nei limiti previsti dalle norme italiane o unionali.

Art.30 – Verifiche nei confronti dei responsabili del trattamento

Nella ipotesi in cui la Fondazione affidi a soggetti pubblici o privati esterni, tramite delega o concessione o contratto lo svolgimento di compiti e/o servizi di propria competenza cui debba conseguire il trattamento di dati personali, il provvedimento o contratto di affidamento deve prevedere norme specifiche attraverso le quali si provvede:

- a nominare il soggetto pubblico o privato ovvero la persona fisica affidatario quale responsabile del trattamento dei dati personali, ex art. 28 del RGPD, per l'intera durata dell'affidamento;
- ad obbligare il soggetto affidatario ad osservare le prescrizioni di cui alla vigente normativa nazionale e comunitaria nonché del presente Regolamento in materia di protezione dei dati personali;
- a consentire le verifiche sul rispetto delle predette disposizioni normative.

Il Referente competente per materia in relazione al compito e/o al servizio affidato comunica con la massima sollecitudine al Responsabile della protezione dei dati e al Responsabile per la sicurezza informatica l'affidamento del compito/servizio e vigila che il soggetto esterno osservi le predette prescrizioni. Il Responsabile della sicurezza informatica verifica che siano osservate le norme riferite all'attuazione delle misure minime di sicurezza.

La periodicità delle predette verifiche, previste nel provvedimento o contratto di affidamento, é determinata in funzione della natura dei dati, della probabile gravità dei rischi, dei mezzi da utilizzare per il trattamento e della durata dell'affidamento.

Le verifiche e i risultati delle stesse sono registrate in appositi distinti verbali, sottoscritti, in duplice originale, dal Referente del trattamento e dal soggetto esterno affidatario del compito/servizio.

Art.31 – Comunicazione interna e utilizzo interno di documenti contenenti dati personali

La comunicazione di documenti amministrativi, secondo la definizione di cui all'art. 1, comma 1, lettera a), del DPR n. 445/2000, contenenti dati personali ai componenti degli organi di governo ovvero all'interno della struttura organizzativa della Fondazione, per ragioni d'ufficio e nell'ambito delle specifiche competenze delle articolazioni interne, non è soggetta a limitazioni particolari, salvo quelle espressamente previste dalla vigente normativa.

Il Referente può tuttavia disporre, con adeguata motivazione, le misure necessarie per la protezione dei dati personali, qualora la comunicazione concerna particolari categorie di dati personali e/o dati personali relativi a condanne penali e reati.

Il Sovrintendente, i Consiglieri ed i componenti degli organi di controllo interno hanno diritto di accedere a documenti amministrativi detenuti dalle articolazioni della Fondazione contenenti dati personali nei limiti e con le modalità previsti dalla vigente normativa e dal presente Regolamento.

Le notizie e le informazioni così acquisite devono essere utilizzate esclusivamente per le finalità pertinenti alle rispettive competenze, rispettando il divieto di divulgazione dei predetti documenti nonché l'obbligo della segretezza del loro contenuto.

TITOLO V – DISPOSIZIONI FINALI

Art. 32 – Rinvio alla normativa generale

Per tutto quanto non espressamente previsto dal presente Regolamento, si fa rinvio al Regolamento europeo n. 679 del 27 aprile 2016 "*Regolamento generale sulla protezione dei da*ti" (RGPD), alle vigenti fonti di diritto nazionali, alle Linee guida e ai provvedimenti del Comitato Europeo per la Protezione dei Dati nonché del Garante per la Protezione dei Dati Personali, alle direttive impartite dal Titolare del trattamento, dai Referenti, dal Responsabile della protezione dei dati e dal Responsabile per la sicurezza informatica.

Art.33 – Entrata in vigore

Il presente regolamento, alla data della sua entrata in vigore, sostituisce integralmente ogni precedente regolamentazione interna in materia di protezione dei dati personali.

Il presente regolamento entra in vigore ad esecutività conseguita della relativa Deliberazione di adozione da parte del Consiglio d'Indirizzo.