DOSSIER PRIVACY

Elaborato in base al D.Lgs.30 giugno 2003 n.196 e ss.mm.ii., al RGPD 2016/679/UE del 27 aprile 2016 in "MATERIA DI TRATTAMENTO DEI DATI PERSONALI"
nonché alla libera circolazione di tali dati

TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI

FONDAZIONE LIRICO SINFONICA
PETRUZZELLI E TEATRI DI BARI

Ministero dei Beni e delle Attività Culturali e del Turismo | Comune di Bari | Città Metropolitana di Bari | Regione Puglia

SEDE DI BARI IN

Strada San Benedetto n.15

Timbro e Firma del Titolare del Trattamento dei Dati Personali
FONDAZIONE LIRICO SINFONICA PETRUZZELLI E TEATRI DI BARI

FONDAZIONE PETRUZZELLI
BARI
04 APR 2019
Prot. N° 412
AMMINISTRAZIONE

FONDAZIONE LIRICO SINFONICA PETRUZZELLI E TEATRI DI BARI	DEFINIZIONI – Art.4 RGPD 2016/679/UE

«Dato Personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

«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;

«Limitazione di Trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

«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;

«Pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

«Archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

«Titolare del Trattamento (T)»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

FONDAZIONE URSO SINFONICA PETRUZZELLI E TEATRI DI BARI	DEFINIZIONI – Art.4 RGPD 2016/679/UE

«Responsabile del Trattamento (R)»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

«Destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

«Terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

«Consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

«Violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

«Dati Genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

«Dati Biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

«Dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

FONDAZIONE LIRICO SINFONICA PETRUZZELLI E TEATRI DI BARI	DEFINIZIONI – Art.4 RGPD 2016/679/UE

«Stabilimento Principale»:
a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;
b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

«Rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

«Impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

«Gruppo Imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

«Norme vincolanti d'impresa»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

«Autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

«Autorità di controllo interessata»: un'autorità di controllo interessata dal trattamento di dati personali in quanto:
a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;
b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure
c) un reclamo è stato proposto a tale autorità di controllo;

«Trattamento Transfrontaliero»:
a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure
b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

«Obiezione pertinente e motivata»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione.

	PREMESSA

Il seguente documento è redatto ai sensi del D.Lgs. 196/2003 ss.mm.ii., del Regolamento Generale Europeo n.679/2016 in materia di Protezione Dati e del D.Lgs. 101/2018.

Premesso che la Fondazione Lirico Sinfonica Petruzzelli e Teatri di Bari (d'ora in avanti la Fondazione) è un Ente senza scopo di lucro che ha come finalità generale quella di dotare Bari, la Città Metropolitana di Bari, nonché la Regione Puglia di una struttura essenziale per lo sviluppo dell'attività lirico sinfonica (art. 2 Statuto) e considerando che nell'ambito della propria attività la Fondazione effettua trattamento di dati personali, il presente documento raccoglie e fornisce le informazioni utili per l'identificazione delle misure di sicurezza, organizzative, tecniche, fisiche e logiche, previste per la tutela dei dati trattati.

In conformità alla normativa vigente nazionale e a quella europea sopra richiamate, si forniscono, nel presente documento, informazioni riguardanti:

1- Principi Generali Privacy
2- Diritti dell'Interessato
3- Sistema Organizzativo Privacy
4- Analisi dei Rischi Privacy e Valutazione di Impatto sulla Protezione dei Dati (VIPD)
5- Misure di Sicurezza e Violazione dei Dati Personali (Data Breach)
6- Il Trattamento dei Dati Personali
7- Sistema di Gestione Privacy: Certificazione Privacy e Codici di Condotta
8- Trasferimento dei Dati all'Estero
9- Geolocalizzazione
10- Altre Informazioni

Allegato A): Registro dei Trattamenti dei Dati Personali
Allegato B): Registro delle Violazioni dei Dati Personali
Allegato C): Relazione Tecnica sulla Stato di Sicurezza Informatica
Allegato D): Informativa Privacy
Allegato E): Consenso dell'Interessato
Allegato F): Organigramma della Fondazione

	PREMESSA

Al fine di poter dimostrare la conformità al Regolamento Europeo Privacy, il Titolare del Trattamento deve definire politiche interne e adottare procedure aziendali che garantiscano il rispetto dei principi quali:

- Privacy by Design, il quale stabilisce che la protezione dei dati debba avvenire fin dal disegno o progettazione di un processo aziendale;
- Privacy by Default, il quale stabilisce la necessità di tutelare la vita privata dei cittadini di default ovvero come impostazione predefinita dell'organizzazione aziendale, in modo da limitare al massimo la raccolta di dati personali.

FONDAZIONE LIRICO SINFONICA PETRUZZELLI E TEATRI DI BARI	1. PRINCIPI GENERALI PRIVACY

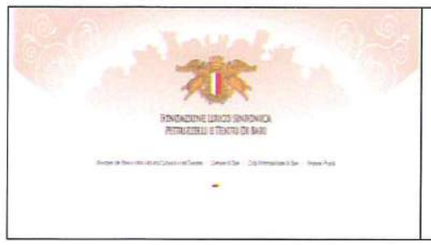
Il RGPD (Regolamento Generale sulla Protezione dei Dati), che ha esplicato pienamente i propri effetti a partire dal 25 maggio 2018, offre un quadro di riferimento in termini di compliance per la protezione dei dati in Europa, aggiornato e fondato sul principio di responsabilizzazione (Accountability).

Il Regolamento Europeo Privacy definisce una serie di principi fondamentali privacy (art. 5) che devono essere obbligatoriamente rispettati in ogni attività di trattamento.

1. I dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
d) 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 («esattezza»);
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
f) 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 («integrità e riservatezza»).

2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).



1. PRINCIPI GENERALI PRIVACY

Concetti chiave in breve

Liceità
Un trattamento di dati personali è "lecito" qualora ricorra almeno una delle seguenti condizioni:

1) è stato espresso il consenso al trattamento dei dati personali per una o più specifiche finalità;
2) il trattamento è necessario all'esecuzione di un contratto o di adempimenti precontrattuali;
3) il trattamento è necessario per adempiere ad un obbligo di legge;
4) il trattamento è necessario per la salvaguardia della vita umana;
5) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri;
6) il trattamento è necessario per il perseguimento di interessi legittimi.

Trasparenza
Qualsiasi trattamento di dati personali deve essere svolto in maniera "trasparente".
Le persone fisiche devono sempre essere preventivamente informate riguardo alle modalità attraverso le quali i loro dati personali potranno essere trattati.
Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento dei dati personali siano scritte in un linguaggio semplice, chiaro e comprensibile e siano sempre facilmente accessibili.
È opportuno, inoltre, che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità del loro esercizio.

Limitazione della finalità
Un trattamento di dati personali è legittimo soltanto se le finalità per le quali vengono trattati i dati sono state definite ed esplicitamente dichiarate prima dell'inizio del trattamento.
Un trattamento di dati personali per finalità indefinite e/o illimitate è illegittimo.
Un trattamento non può basarsi semplicemente sul fatto che i dati siano stati inizialmente acquisiti o trattati per un'altra finalità.
Ogni nuova finalità richiede una nuova dichiarazione esplicita e preventiva.
Il trasferimento di dati a terzi deve essere considerata una nuova finalità e come tale deve essere dichiarata.
E' consentito, comunque, l'utilizzo di dati per finalità compatibili con quelle inizialmente dichiarate o per fini di archiviazione nel pubblico interesse, di ricerca scientifica, storica o statistica.

Minimizzazione dei dati
Un trattamento di dati personali è legittimo soltanto se i dati trattati sono adeguati, pertinenti e limitati a quelli necessari al raggiungimento della finalità per i quali sono stati raccolti.
I dati scelti per il trattamento devono essere solo quelli pertinenti al raggiungimento dell'obiettivo generale dichiarato e il loro trattamento deve essere strettamente limitato a tali dati.

Esattezza
Prima di trattare dati personali ci si deve accertare con ragionevole certezza che i dati siano esatti ed aggiornati.
E' necessario, inoltre, adottare tutte le misure ragionevoli per cancellare o rettificare tempestivamente tutti quei dati personali che non risultino esatti rispetto alle finalità per le quali devono essere trattati.

Limitazione della Conservazione
I dati personali devono essere conservati, in una forma che consenta l'identificazione delle persone fisiche, per un periodo non superiore a quello necessario al conseguimento delle finalità dichiarate.
Il periodo di conservazione dei dati personali deve essere sempre limitato al minimo necessario. Una volta che la finalità dichiarata è stata raggiunta, la conservazione non è più necessaria e i dati personali devono essere obbligatoriamente cancellati.
I dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente per finalità previste dalla legge.
Al fine di assicurare che i dati personali non siano conservati più a lungo del necessario, deve essere stabilito in via preliminare un termine ultimo per la cancellazione o per la verifica periodica della necessità di un ulteriore prolungamento dei tempi di conservazione.

Integrità e Riservatezza
Le operazioni di trattamento devono essere effettuate in modo da garantire un'adeguata sicurezza e riservatezza dei dati personali.
I dati personali e le attrezzature utilizzate per il trattamento devono essere protetti mediante l'adozione di misure tecniche e organizzative adeguate ad impedire:

- Accessi non autorizzati
- Trattamenti non autorizzati
- Trattamenti illeciti
- Perdita
- Distruzione
- Danneggiamenti accidentali

Responsabilizzazione
Il Principio di Responsabilità richiede l'adozione preventiva di misure finalizzate alla promozione e salvaguardia della protezione dei dati durante le operazioni di trattamento.
Chi compie operazioni di trattamento è responsabile della loro conformità alla normativa in materia di protezione dei dati personali e deve essere sempre in grado di dimostrare, con idonea documentazione, di operare nel pieno rispetto della legge.

	2. DIRITTI DELL'INTERESSATO

DIRITTO ALLA TRASPARENZA

1. Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento 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.

2. Il titolare del trattamento agevola l'esercizio dei diritti dell'interessato ai sensi degli articoli da 15 a 22. Nei casi di cui all'articolo 11, paragrafo 2, il titolare del trattamento non può rifiutare di soddisfare la richiesta dell'interessato al fine di esercitare i suoi diritti ai sensi degli articoli da 15 a 22, salvo che il titolare del trattamento dimostri che non è in grado di identificare l'interessato.

3. Il titolare del trattamento fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta ai sensi degli articoli da 15 a 22 senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Il titolare del trattamento informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta. Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato.

4. Se non ottempera alla richiesta dell'interessato, il titolare del trattamento informa l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale.

5. Le informazioni fornite ai sensi degli articoli 13 e 14 ed eventuali comunicazioni e azioni intraprese ai sensi degli articoli da 15 a 22 e dell'articolo 34 sono gratuite. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può:
a) addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; oppure
b) rifiutare di soddisfare la richiesta. Incombe al titolare del trattamento l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

6. Fatto salvo l'articolo 11, qualora il titolare del trattamento nutra ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta di cui agli articoli da 15 a 21, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato.

7. Le informazioni da fornire agli interessati a norma degli articoli 13 e 14 possono essere fornite in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone sono leggibili da dispositivo automatico.

8. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 92 al fine di stabilire le informazioni da presentare sotto forma di icona e le procedure per fornire icone standardizzate.

DIRITTO DI ACCESSO

1. L'interessato ha il diritto di ottenere dal titolare del trattamento 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) quando 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 al titolare del trattamento 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, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.

3. Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

4. Il diritto di ottenere una copia di cui al paragrafo 3 non deve ledere i diritti e le libertà altrui.

DIRITTO DI RETTIFICA

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

DIRITTO DI CANCELLAZIONE – DIRITTO ALL'OBLIO

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento 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;
b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;
c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;
d) i dati personali sono stati trattati illecitamente;
e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.

2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione, adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

3. I paragrafi 1 e 2 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 dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;
d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o
e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

DIRITTO DI LIMITAZIONE DI TRATTAMENTO

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:

a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;
b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
c) benché il titolare del trattamento 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 ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

2. Se il trattamento è limitato a norma del paragrafo 1, 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 di uno Stato membro.

3. L'interessato che ha ottenuto la limitazione del trattamento a norma del paragrafo 1 è informato dal titolare del trattamento prima che detta limitazione sia revocata.

OBBLIGO DI NOTIFICA

Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma dell'articolo 16, dell'articolo 17, paragrafo 1, e dell'articolo 18, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

DIRITTO ALLA PORTABILITA' DEI DATI

1. 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 a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:
a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e
b) il trattamento sia effettuato con mezzi automatizzati.

2. Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.

3. L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

4. Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui.

DIRITTO DI OPPOSIZIONE

1. 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 ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli 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.

2. Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.

3. Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità.

4. Il diritto di cui ai paragrafi 1 e 2 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.

5. Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.

6. Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

DIRITTO SUI PROCESSI AUTOMATIZZATI

1. 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.

2. Il paragrafo 1 non si applica nel caso in cui la decisione:

a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, 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.

3. Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.

4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

IL TITOLARE DEL TRATTAMENTO

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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (art. 4, punto7) del RGPD).

Il ruolo di titolare del trattamento implica quale principale conseguenza la responsabilità giuridica dell'ottemperanza degli obblighi previsti in materia di protezione dei dati.

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonchè dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonchè della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

CONTITOLARE DEL TRATTAMENTO

Allorchè due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati.

L'accordo di cui al paragrafo 1 riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

Indipendentemente dalle disposizioni dell'accordo di cui al paragrafo 1, l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento.

In breve: il Regolamento Europeo Privacy prevede che entità giuridicamente distinte, possano agire, singolarmente o unitamente, come titolari di uno stesso trattamento, qualora decidano di trattare i dati per una finalità comune e prendano congiuntamente decisioni in tal senso. In questo caso, si configura una situazione giuridica definita come "contitolarità del trattamento" (Contitolare).

Una situazione di contitolarità può verificarsi anche nel caso in cui un titolare del trattamento non adempia correttamente all'obbligo di vigilare sulle attività delegate ad un responsabile del trattamento e quest'ultimo utilizzi i dati per proprio conto.

In caso di contitolarità, i titolari del trattamento determinano congiuntamente e in modo trasparente le finalità e i mezzi del trattamento, sottoscrivendo un accordo interno, nel quale devono essere chiaramente definite le rispettive responsabilità e le modalità reciproche di:

1) *osservanza degli obblighi derivanti dal Regolamento Europeo Privacy*
2) *esercizio dei diritti dell'interessato*
3) *comunicazione delle informazioni*

RAPPRESENTANTE DEL TITOLARE DEL TRATTAMENTO

Il regolamento europeo definisce il rappresentante la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento.

In breve: i Titolari del Trattamento non stabiliti nell'Unione Europea, che trattano dati di cittadini europei, devono obbligatoriamente designare per iscritto un proprio "Rappresentante del Titolare del Trattamento" con sede all'interno dell'Unione Europea.

Il Rappresentante del Titolare del Trattamento può essere una persona fisica o una persona giuridica e deve essere stabilito in uno degli Stati Membri in cui sono residenti le persone fisiche i cui dati sono oggetto delle attività di trattamento.

Il Rappresentante del Titolare ha il compito di rappresentare il titolare per quanto riguarda gli obblighi previsti dal Regolamento Europeo Privacy, fungendo da interlocutore principale nei rapporti con le autorità di controllo e con le persone fisiche i cui dati sono oggetto delle attività di trattamento.

La designazione del rappresentante non incide sulla responsabilità generale del titolare del trattamento, ma il rappresentante designato può essere oggetto di misure attuative in caso di inadempienza da parte del titolare del trattamento.

RESPONSABILE DEL TRATTAMENTO

L'art. 4 punto 8) del regolamento europeo definisce il responsabile del trattamento la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

c) adotti tutte le misure richieste ai sensi dell'articolo 32;

d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;

e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III del RGPD;

f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;

h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato. Con riguardo alla lettera h) del primo comma, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto

misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

DATA PROTECTION OFFICER (DPO)

In base all'art. 37 del Regolamento Europeo, alcuni titolari del trattamento e responsabili del trattamento sono tenuti a nominare un Responsabile della Protezione dei Dati (RPD/DPO). Ciò vale per tutte le autorità pubbliche e tutti i soggetti pubblici, indipendentemente dai dati oggetto di trattamento, e per altri soggetti che, come attività principale, effettuino un monitoraggio regolare e su larga scala delle persone fisiche ovvero trattino su larga scala categorie particolari di dati personali. Nel caso in cui si proceda alla nomina di un RPD su base volontaria, troveranno applicazione tutti i requisiti di cui agli articoli 37-39 per quanto concerne la nomina stessa, lo status e i compiti del RPD esattamente come nel caso di una nomina obbligatoria.
La Fondazione, dopo aver verificato i requisiti previsti dall'art.37 del RGPD, ha proceduto, sin da subito, all'individuazione del Responsabile Protezione Dati (esterno), il quale è tenuto alla sottoscrizione del Codice Deontologico dei Responsabili Protezione Dati oltre ad non versare in alcuna situazione di conflitto di interessi rispetto al ruolo assunto.

Inoltre, così come chiarito dal paragrafo 7 del predetto articolo, il Titolare del Trattamento o il Responsabile del Trattamento sarà tenuto:

- a pubblicare i dati di contatto del RPD, oltre
- a comunicare i dati di contatto del RPD alle pertinenti autorità di controllo (Garante Privacy).

Tale disposizione mira a garantire che tanto gli interessati (all'interno o all'esterno della Fondazione) quanto le autorità di controllo possano contattare agevolmente e in modo diretto il RPD senza doversi rivolgere ad un'altra struttura operante presso il Titolare/Responsabile del Trattamento. Nonostante l'art. 37, settimo paragrafo del regolamento europeo, chiarisca che non sia necessario pubblicare anche il nominativo del RPD, tuttavia, comunicare il nominativo del RPD all'autorità di controllo è fondamentale affinché il RPD funga da punto di contatto fra la Fondazione e l'autorità di controllo stessa (articolo 39, paragrafo 1, lettera e)).

Il RPD è tenuto ad osservare le norme in materia di segreto o riservatezza nello svolgimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri, così come chiarito nel paragrafo 5 art. 38 del RGPD.

Ai sensi dell'articolo 38 del RGPD, il titolare del trattamento e il responsabile del trattamento assicurano che il RPD sia "tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali".

Dunque, tra le altre cose, il titolare del trattamento o il responsabile del trattamento è tenuto alla comunicazione ufficiale della nomina del RPD a tutto il personale della Fondazione, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'Ente.

Il RPD non è responsabile personalmente in caso di inosservanza degli obblighi in materia di protezione dei dati. Spetta al titolare del trattamento o al responsabile del trattamento garantire ed essere in grado di dimostrare che il trattamento sia effettuato conformemente al regolamento. La responsabilità di garantire l'osservanza della normativa in materia di protezione dei dati ricade sul titolare del trattamento o sul responsabile del trattamento.

Per quanto concerne la valutazione di impatto sulla protezione dei dati, l'art. 39, paragrafo 1, lett. c), chiarisce che il RPD fornisce, se richiesto, un parere in merito alla Valutazione di Impatto sulla Protezione Dati (VIPD/DPIA) e sorvegliarne lo svolgimento ai sensi dell'art 35.
Dunque, il titolare del trattamento o il responsabile del trattamento dovrebbero consultarsi con il RPD, fra l'altro, sulle seguenti tematiche:

- se condurre o meno una DPIA;
- quale metodologia adottare nel condurre una DPIA;
- se condurre la DPIA con le risorse interne ovvero esternalizzandola;
- quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate;
- se la DPIA sia stata condotta correttamente o meno, e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi ai requisiti in materia di protezione dei dati.

Per quanto riguarda il Registro dei Trattamenti, la sua tenuta è un obbligo che ricade sul titolare del trattamento o sul responsabile del trattamento. Cionondimeno, non è posto divieto alcuno al titolare del trattamento o al responsabile del trattamento di affidare al RPD il compito di tenere il registro delle attività di trattamento sotto la responsabilità del titolare o del responsabile stesso. Tale registro va considerato uno degli strumenti che consentono al RPD di adempiere agli obblighi di sorveglianza del rispetto del regolamento, informazione e consulenza nei riguardi del titolare del trattamento o del responsabile del trattamento.

INCARICATI DEL TRATTAMENTO

Pur non prevedendo espressamente la figura dell' "*incaricato*" del trattamento (ex art. 30 del Codice), il regolamento europeo non ne esclude la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" (si veda, in particolare, art. 4, n. 10), del regolamento europeo – definizione di "Terzo").

Le disposizioni del Codice in materia di incaricati del trattamento sono pienamente compatibili con la struttura e la filosofia del regolamento europeo, in particolare alla luce del principio di "responsabilizzazione" di titolari e responsabili del trattamento che prevede l'adozione di misure atte a garantire proattivamente l'osservanza del regolamento nella sua interezza.

AMMINISTRATORE DI SISTEMA (ADS)

L'Autorità Garante per la Protezione dei Dati Personali, con il Provvedimento a Carattere Generale emesso il 27 novembre 2008 denominato "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema", ha posto come obbligo ai titolari dei trattamenti quello di individuare e designare in modo specifico ed analitico i propri Amministratori di Sistema, individuando gli incarichi assegnati e i meccanismi previsti per la verifica del loro operato.

Tale Provvedimento definisce "Amministratore di Sistema" ogni soggetto al quale è conferito un compito di gestione, amministrazione e manutenzione di un sistema informatico, di un elaboratore elettronico, di una rete, di un apparato di sicurezza, di un software applicativo, di una base di dati o di una banca dati.

Qualora i servizi di Amministratore di Sistema siano affidati in outsourcing ad una persona giuridica, tale soggetto deve essere nominato "Responsabile del Trattamento" ai sensi dell'art. 4 comma 9) del Regolamento Europeo Privacy UE/2016/679 e dell'art. 4 comma 1) lettera g) del D.lgs. 196/03 e s.m.i. con funzioni di Amministratore di Sistema.

Ai sensi dell'art. 28 comma 1) del Regolamento Europeo Privacy UE/2016/679, il responsabile del trattamento deve presentare "garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti di legge e garantisca la tutela dei diritti dell'interessato".

Inoltre, si tenga conto che:

- ai sensi dell'art. 29 comma 3) del D. Lgs.196/03 e s.m.i., per esigenze di natura organizzativa è possibile designare uno o più responsabili del trattamento mediante suddivisione dei relativi compiti e che, ai sensi dei commi 4) e 5) del predetto articolo, tali compiti devono essere analiticamente specificati per iscritto;
- l'Amministratore di Sistema deve essere "individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza";
- l'attribuzione delle funzioni di Amministratore di Sistema deve avvenire previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza;
- la designazione delle persone fisiche, a cui il responsabile del trattamento affiderà materialmente lo svolgimento delle attività di amministratore di sistema, deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.
- i compiti affidati al responsabile del trattamento devono essere analiticamente specificati per iscritto dal titolare del trattamento e i trattamenti da parte di un responsabile del trattamento devono essere "disciplinati da un contratto o da altro atto giuridico" con il titolare del trattamento, che deve essere obbligatoriamente stipulato in forma scritta, anche in formato elettronico.

AMMINISTRATORE DI SISTEMA: OBBLIGHI E MODALITA' DEL TRATTAMENTO

Nominando un Amministratore di Sistema Esterno (ADS Esterno), la Fondazione lo autorizza a trattare dati personali relativi a propri dipendenti e/o clienti e/o fornitori:

- solamente per lo svolgimento delle attività contrattualmente previste (elencate nelle premesse);
- unicamente nel rispetto delle direttive, delle procedure e delle istruzioni impartite dalla Fondazione;
- esclusivamente attraverso l'utilizzo di personale alle proprie dirette dipendenze, di strumenti elettronici e di software applicativi presenti nel territorio dello Stato Italiano e di proprietà dell'ADS o dalla Fondazione e amministrati/gestiti direttamente senza l'intervento di soggetti terzi (quali a titolo esemplificativo fornitori, società controllate, partecipate o collegate);
- solamente nelle sedi dell'ADS presenti nel territorio dello Stato Italiano;

- limitatamente alle operazioni di trattamento effettivamente necessarie per il corretto svolgimento dell'incarico affidato.

Qualora l'ADS abbia necessità di trattare dati e informazioni in maniera differente dalle disposizioni sopra specificate, lo stesso dovrà darne tempestiva comunicazione alla Fondazione che le dovrà autorizzare tutte preventivamente per iscritto.

Con la sottoscrizione della predetta nomina, l'amministratore di sistema (ADS) riconosce il carattere segreto, riservato e rigorosamente confidenziale di qualsiasi dato personale e/o informazione inerente il contratto di fornitura e, conseguentemente, si impegna a:

- trattare i dati personali soltanto su istruzione documentata della Fondazione;
- adottare tutte le misure di sicurezza previste dall'articolo 32) del Regolamento Europeo Privacy UE/2016/679;
- non ricorrere ad un altro responsabile del trattamento senza preventiva autorizzazione scritta da parte della Fondazione;
- informare preventivamente la Fondazione di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento e/o amministratori di sistema, in modo che la Fondazione possa tempestivamente opporsi;
- nel caso in cui subappalti l'esecuzione di specifiche attività di trattamento ad un altro responsabile del trattamento, a stipulare con tale responsabile del trattamento un contratto, che disciplini gli stessi obblighi in materia di protezione dei dati contratti con la Fondazione;
- assistere la Fondazione con misure tecniche e organizzative idonee a dare un pronto riscontro all'esercizio dei diritti dell'interessato;
- garantire il rispetto degli obblighi imposti dai seguenti articoli del Regolamento Europeo Privacy UE/2016/679:
  art. 30 - Registro delle Attività di Trattamento
  art. 33 - Notificazione delle Violazioni dei Dati Personali
  art. 34 - Comunicazione delle Violazioni dei Dati Personali
  art. 35 - Valutazione d'Impatto sulla Protezione dei Dati
  art. 36 - Consultazione Preventiva
  art. 37 - Designazione del Responsabile della Protezione dei Dati (DPO)
- mettere a disposizione della Fondazione tutte le informazioni necessarie a dimostrare che il trattamento è svolto nel rispetto degli obblighi previsti dal Regolamento Europeo Privacy UE/2016/679 e dal D.lgs. 196/03 e s.m.i.;
- adottare ogni e qualsiasi misura idonea a garantire la protezione e la riservatezza dei dati personali e delle informazioni raccolte e trattate per conto del Committente, nonché a prevenire la loro eventuale acquisizione e/o utilizzazione da parte di terzi non autorizzati;
- rispettare le prescrizioni previste dal D.lgs. 196/2003 e s.m.i. e dai Provvedimenti dell'Autorità Garante per la Protezione dei Dati Personali con particolare riferimento a quanto in merito

agli obblighi di sicurezza (art. 31 del D.lgs. 196/03 e s.m.i.) e alle misure minime di sicurezza da adottare per il trattamento (art. 33 e seguenti del D.lgs. 196/03 così come succ. mod.);

- rispettare i Provvedimenti dell'Autorità Garante per la Protezione dei Dati Personali con particolare riferimento alle Autorizzazioni Generali e ai Provvedimenti in materia di Amministratore di Sistema, Posta Elettronica e Internet;
- non rivelare e/o comunicare, direttamente o indirettamente, i dati personali e le informazioni, in qualsiasi modo acquisite, a soggetti terzi, né in tutto né in parte, né in forma scritta o orale;
- non trattare, venire a conoscenza o utilizzare in alcuna maniera dati personali e informazioni acquisiti con modalità contrarie ai principi di buona fede e correttezza professionale o in modalità difformi da quanto contrattualmente stabilito;
- non trattare dati personali e utilizzare informazioni confidenziali con modalità e/o per finalità tali da arrecare, anche solo potenzialmente, direttamente o indirettamente, danno e/o pregiudizio alla Fondazione;
- garantire che le persone autorizzate al trattamento dei dati personali abbiano sottoscritto una lettera di incarico con la quale siano impegnati a rispettare gli obblighi di riservatezza;
- collaborare con la Fondazione nelle attività di progettazione, implementazione, mantenimento e revisione del sistema di gestione privacy aziendale, compresi audit e ispezioni, realizzate dalla Fondazione o da un altro soggetto da questi incaricato;
- informare immediatamente la Fondazione di qualsiasi violazione della normativa in materia di protezione dei dati personali di cui venga a conoscenza.

Con riferimento ai suddetti dati personali e/o informazioni, che potranno essere raccolti, registrati, elaborati e conservati con strumenti elettronici e applicativi (hardware e software) e più in generale trattati mediante l'utilizzo di sistemi informatici di proprietà del Fornitore (ADS), si fa presente che tali dati potranno essere trattati solamente da personale appositamente incaricato dal Fornitore (ADS) ed esclusivamente per le finalità contrattualmente previste; tali dati non dovranno e non potranno, in alcun modo e per nessuna ragione essere consultati, elaborati e trattati per finalità non contrattualmente previste o trattati da personale non autorizzato dal Fornitore (ADS) e/o da soggetti terzi (comprese eventuali società del Gruppo) senza una preventiva autorizzazione per iscritto da parte della Fondazione.

Anche l'eventuale accesso al sistema informativo, all'area riservata del sito web, agli applicativi, alle banche dati e agli archivi cartacei messi a disposizione dalla Fondazione al Fornitore (ADS) per il regolare svolgimento del contratto stipulato, dovrà essere limitato al solo personale formalmente incaricato dal Fornitore (ADS) previo il rispetto delle misure di sicurezza e delle procedure di autenticazione e autorizzazione concordate con la Fondazione committente.

Il Fornitore (ADS) dovrà trattare tali dati per il tempo strettamente necessario allo svolgimento delle attività contrattualmente previste, con ogni conseguente divieto di utilizzo, diffusione e comunicazione dei dati stessi oltre i termini contrattualmente stabiliti.

In particolare, con la sottoscrizione della nomina, il Fornitore (ADS) si obbliga a:

1. non raccogliere e trattare dati personali e informazioni, non pertinenti e eccedenti rispetto alle finalità contrattualmente previste;
2. attribuire le funzioni di amministratore di sistema ai propri dipendenti e collaboratori esclusivamente dopo aver attentamente valutato le caratteristiche di esperienza, capacità e affidabilità dei soggetti che si intendono designare, assicurandosi che siano idonei a garantire il pieno rispetto delle vigenti disposizioni in materia di trattamento di dati personali e sicurezza delle informazioni;
3. designare individualmente, ai sensi dell'art. 30 del D.lgs. 196/03 e s.m.i., le persone fisiche alle quali saranno assegnati ruoli di amministratore di sistema, specificando analiticamente gli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;
4. comunicare preventivamente per iscritto, alla Fondazione committente, gli estremi identificativi delle persone fisiche che potranno svolgere attività di amministrazione di sistema, con l'elenco delle funzioni ad essi attribuite;
5. redigere e mantenere aggiornato e disponibile un documento interno nel quale sono riportati gli estremi identificativi delle persone fisiche designate amministratori di sistema, con l'elenco delle funzioni ad essi attribuite;
6. verificare, con cadenza almeno annuale, l'operato dei soggetti designati amministratori di sistema;
7. adottare idonei sistemi di registrazione degli accessi logici agli strumenti elettronici, agli applicativi e alle banche dati effettuati dagli amministratori di sistema, garantendo i requisiti di completezza, inalterabilità, integrità e conservazione delle registrazioni previsti dalla normativa vigente;
8. limitare il trattamento dei suoi incaricati alle sole attività effettivamente necessarie allo svolgimento delle attività contrattualmente previste;
9. utilizzare per il trattamento esclusivamente sistemi informativi e applicativi software valutati idonei dalla Fondazione;
10. istruire il personale incaricato affinché si astenga dall'effettuare qualsiasi accesso non autorizzato, trattamento non consentito o non necessario alle banche dati e agli archivi contenenti dati personali di titolarità della Fondazione;
11. istruire il personale incaricato affinché si impegni a trattare con l'assoluto riserbo, con divieto di diffusione o comunicazione di qualsivoglia notizia e/o dato dei quali dovessero venire comunque a conoscenza;
12. avvertire prontamente la Fondazione in caso di trattamenti illeciti, carenze o violazioni in materia di misure di sicurezza previste per legge;

13. formare il personale incaricato in merito agli adempimenti previsti dalla normativa privacy e alle relative responsabilità amministrative, civili e penali;

14. fornire alla Fondazione committente una relazione periodica annuale sul sistema di gestione privacy adottato, comprensiva di ruoli, mansioni e ambito di trattamento e procedure di incaricati, responsabili e amministratori di sistema autorizzati a trattare dati personali di titolarità della Fondazione, di analisi dei rischi e misure di sicurezza adottate per ridurre al minimo i rischi ai sensi dell'art. 32 del Regolamento Europeo Privacy UE/2016/679 e dell'art. 31 del D.lgs. 196/03 e s.m.i. e di descrizione del sistema informatico (hardware e software) utilizzato per il trattamento comprensivo delle specifiche modalità di trattamento definite.

Alla scadenza del contratto, tutta la documentazione cartacea contenente dati personali di titolarità della Fondazione dovrà essere fisicamente riconsegnata o distrutta e tutti gli eventuali dati registrati in applicativi o su supporti informatici, non di proprietà della Fondazione, dovranno essere copiati su supporti removibili e consegnati a quest'ultima. Al termine delle suddette operazioni, una volta che la Fondazione abbia verificato la leggibilità dei dati registrati sui supporti consegnati, il Fornitore (ADS) dovrà riconsegnare tutti gli strumenti elettronici e i supporti informatici di proprietà della Fondazione e cancellare e/o a far cancellare, in maniera da tale da impedire un loro successivo recupero, tutti i file contenenti dati personali di titolarità della Fondazione presenti nei propri strumenti elettronici e applicativi, salvo quelli la cui conservazione sia obbligatoria legge, che comunque dovranno essere cancellati al termine del periodo prescritto.

Ai sensi del Provvedimento del Garante Privacy in materia di Amministratori di Sistema, la Fondazione verificherà periodicamente, con cadenza almeno annuale, l'operato del Fornitore (ADS) in modo da controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza previste per legge. A tal fine la Fondazione committente adotterà idonei sistemi per la registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte del Fornitore (ADS). Le registrazioni (access log) comprenderanno i riferimenti temporali e la descrizione dell'evento che le ha generate e saranno conservate per un periodo, non inferiore a sei mesi.

AMMINISTRATORE DI SISTEMA (ADS): RESPONSABILITA'

Con la nomina del Fornitore (ADS), questi si assume la responsabilità del rispetto delle misure minime di sicurezza privacy previste per legge e delle ulteriori misure di sicurezza impartite dalla Fondazione per la protezione dei dati personali e il mantenimento della riservatezza delle informazioni apprese nel corso del rapporto oggetto del presente accordo.

Nel caso in cui il Fornitore (ADS), per lo svolgimento delle suddette attività di trattamento, si avvalga della collaborazione di personale incaricato, esso si intende comunque operare sotto la sua

diretta ed esclusiva responsabilità. Il Fornitore (ADS), pertanto, si impegna a rendere edotti i propri incaricati e amministratori di sistema delle modalità convenute con il presente accordo, ferma restando la sua personale responsabilità in ordine al trattamento dei dati oggetto della presente nomina.

La Fondazione potrà in ogni momento - anche tramite ispezioni, visite e controlli periodici presso le sedi del Fornitore (ADS) – verificare la puntuale osservanza delle direttive e procedure/istruzioni impartite, delle misure di sicurezza adottate e dell'assolvimento di tutti gli obblighi in materia di protezione di dati personali. In caso di inosservanza delle procedure/istruzioni impartite, di mancata adozione di adeguate misure di sicurezza e di inadempimento a obblighi in materia di protezione di dati personali, il Fornitore (ADS) sarà ritenuto responsabile nei confronti della Fondazione, per il risarcimento degli eventuali danni diretti ed indiretti derivanti da trattamenti illeciti, ferme restando le sue ulteriori responsabilità civili, amministrative e penali derivanti da trattamenti non autorizzati e mancato rispetto della normativa in materia di protezione di dati personali. In tal caso il contratto si intenderà immediatamente risolto per gravi inadempienze del Fornitore (ADS).

ADDETTO ALLA MANUTENZIONE DEL SISTEMA INFORMATICO

Si definiscono "Addetti alla Manutenzione del Sistema Informatico" (Addetti IT) quei soggetti che solo occasionalmente per fini di manutenzione o di assistenza tecnica intervengono su un sistema informatico, una rete informatica, uno strumento elettronico, un dispositivo hardware o un applicativo software. Gli Addetti IT non possiedono e non sono a conoscenza delle credenziali di autenticazione che permettono i massimi privilegi di accesso al sistema.

L'Addetto alla Manutenzione del Sistema Informatico opera sotto la diretta autorità, responsabilità e supervisione dell'Amministratore di Sistema. Qualora necessario, per esigenze tecniche, all'Addetto IT può essere assegnato un profilo temporaneo di amministratore di sistema con permessi strettamente limitati e circostanziati alla durata e all'oggetto dell'incarico assegnato. Al termine dell'incarico, le credenziali di autenticazione temporaneamente assegnate devono essere disattivate dall'Amministratore di Sistema.

La designazione ad Addetto alla Manutenzione del Sistema Informatico deve essere formalizzata per iscritto. Qualora il Titolare del Trattamento si avvalga di soggetti esterni alla propria struttura per provvedere all'adozione di misure di sicurezza dovrà sottoscrivere un Contratto o una Convenzione di Servizio che preveda l'obbligo, per l'Addetto IT di rilasciare una descrizione scritta dell'intervento e un attestato di conformità privacy.

	4. ANALISI DEI RISCHI PRIVACY E VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

Nel caso in cui una particolare tipologia di trattamento possa presentare un elevato rischio per i diritti e le libertà delle persone fisiche, il Titolare del Trattamento, prima di dare avvio a qualsiasi operazione di trattamento, deve obbligatoriamente procedere ad una valutazione preliminare dell'impatto che tali trattamenti possano avere sulla protezione dei dati personali degli interessati (Valutazione di Impatto sulla Protezione dei Dati).

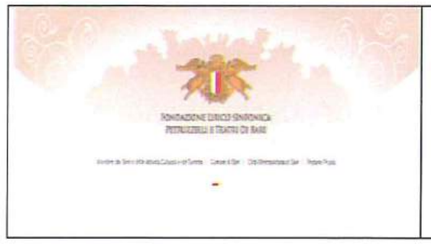
L'art.35 del Regolamento europeo chiarisce che il Titolare del Trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il Responsabile della Protezione dei Dati, designato dalla Fondazione.

Le linee guida WP 248-17/IT definiscono la valutazione d'impatto sulla protezione dei dati (VIPD) un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli. Le valutazioni d'impatto sulla protezione dei dati sono strumenti importanti per la responsabilizzazione (c.d. accountability) in quanto sostengono i Titolari del Trattamento non soltanto nel rispettare i requisiti del regolamento generale sulla protezione dei dati, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del Regolamento.

In linea con l'approccio basato sul rischio adottato dal regolamento generale sulla protezione dei dati, non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento. Infatti, è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando il trattamento "*può presentare un rischio elevato per i diritti e le libertà delle persone fisiche*" (art.35, paragrafo 1).

A titolo di definizione, per "rischio" si intende uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità, mentre per "gestione dei rischi" si definisce l'insieme delle attività coordinate volte a indirizzare e controllare un'organizzazione in relazione ai rischi. L'articolo 35 del regolamento europeo fa riferimento al possibile rischio elevato "per i diritti e le libertà delle persone fisiche", intesi questi ultimi quali: diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la libertà di parola, la libertà di pensiero, la libertà di circolazione, il divieto di discriminazione, il diritto alla libertà di coscienza e di religione.

Nel corso delle attività di valutazione dei rischi, il Titolare del Trattamento deve valutare attentamente la probabilità e la gravità delle conseguenze che determinati tipi di trattamento possano comportare per i diritti dell'interessato.



4. ANALISI DEI RISCHI PRIVACY E VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

Dunque, una corretta valutazione di impatto deve prendere in considerazione e stimare almeno i seguenti rischi:

1) Discriminazioni;
2) Furto d'identità;
3) Perdite finanziarie o economiche;
4) Danni materiali, immateriali o sociali;
5) Pregiudizio alla reputazione;
6) Violazione del segreto professionale;
7) Decifratura non autorizzata;
8) Perdita del controllo sui dati personali;
9) Profilazione e Geolocalizzazione non autorizzate.

Al termine delle attività di valutazione di impatto sulla protezione dei dati personali, il titolare del trattamento deve redigere una "Relazione di Impatto Privacy" che contenga almeno i seguenti elementi:

1. una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento;
2. l'interesse legittimo perseguito dal titolare del trattamento;
3. una valutazione dei principi di necessità e proporzionalità dei trattamenti in relazione alle finalità perseguite;
4. una valutazione dei rischi per i diritti e le libertà degli interessati;
5. le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali;
6. le modalità adottate per dimostrare la conformità al Regolamento Europeo Privacy.

Nel caso in cui l'esito della valutazione d'impatto rilevi un rischio elevato che non può essere attenuato con idonee contromisure (es: a causa degli elevati costi di attuazione o per indisponibilità tecnologica…), il titolare del trattamento è tenuto a consultare preventivamente l'Autorità Garante Privacy Nazionale, prima di iniziare le operazioni di trattamento (art. 36 RGPD).

A seguito della richiesta di consultazione preventiva, l'Autorità Garante Privacy Nazionale è tenuta a fornire al titolare del trattamento un parere scritto, entro un termine massimo di 8 settimane dal ricevimento della richiesta. In caso di particolare complessità del trattamento, il termine può essere prolungato fino a 14 settimane, previo comunicazione al titolare del trattamento, entro un mese dal ricevimento della richiesta di consultazione, della motivazione del ritardo. La decorrenza dei termini può essere sospesa, qualora l'Autorità Garante Privacy Nazionale necessiti di informazioni aggiuntive e il titolare del trattamento non vi provveda tempestivamente.

Conclusioni e raccomandazioni: La valutazione d'impatto sulla protezione dei dati è uno strumento, di cui dispongono i titolari del trattamento, utile per attuare sistemi di trattamento dei dati conformi al regolamento generale sulla protezione dei dati e possono essere obbligatorie per talune tipologie di trattamenti. Hanno natura modulabile e possono assumere forme diverse. Tuttavia, il regolamento generale sulla protezione dei dati stabilisce i requisiti essenziali di una valutazione d'impatto sulla protezione dei dati efficace. I titolari del trattamento dovrebbero considerare la realizzazione di una valutazione d'impatto sulla protezione dei dati come un'attività utile e positiva che contribuisce alla conformità giuridica.

L'articolo 24, paragrafo 1, definisce la responsabilità fondamentale del titolare del trattamento in termini di rispetto del regolamento generale sulla protezione dei dati: "*Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il Titolare del Trattamento mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate ed aggiornate qualora necessario*".

La valutazione d'impatto sulla protezione dei dati è un aspetto fondamentale del rispetto del regolamento laddove si preveda di svolgere o si stia svolgendo un trattamento di dati soggetto a rischio elevato. Ciò significa che i titolari del trattamento dovrebbero utilizzare i criteri stabiliti nel presente documento per stabilire se devono realizzare una valutazione d'impatto sulla protezione dei dati o meno. La politica interna dei titolari del trattamento potrebbe estendere questo elenco andando oltre i requisiti giuridici sanciti dal regolamento generale sulla protezione dei dati. Ciò dovrebbe suscitare un maggior senso di fiducia e riservatezza negli interessati e in altri titolari del trattamento.

Qualora si preveda di effettuare un trattamento che possa presentare un rischio elevato, il titolare del trattamento deve:

- scegliere una metodologia per la valutazione d'impatto sulla protezione dei dati oppure specificare ed attuare un processo sistematico di valutazione d'impatto sulla protezione dei dati;
- fornire la relazione relativa alla valutazione d'impatto sulla protezione dei dati all'autorità di controllo, laddove gli venga richiesto di procedere in tal senso;
- consultare l'autorità di controllo, qualora il titolare del trattamento non sia riuscito a determinare misure sufficienti per attenuare i rischi elevati;
- riesaminare periodicamente la valutazione d'impatto sulla protezione dei dati e il trattamento che essa valuta, almeno quando si registra una variazione del rischio posto dal trattamento;
- documentare le decisioni prese.

	4. ANALISI DEI RISCHI PRIVACY E VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

Il titolare del trattamento, di concerto con il responsabile protezione dati (RPD) della Fondazione Lirico Sinfonica Petruzzelli e Teatri di Bari, procede alla mappatura ed analisi dei rischi legati al trattamento dei dati personali, al fine di verificare se esistano trattamenti che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche. La procedura di cui sopra prevede:

- interviste personali ai soggetti potenzialmente coinvolti;
- questionari specifici, suddivisi per Aree Funzionali;
- analisi, intervista e questionario legati al settore dell' Information Tecnology ed in particolare all'Amministratore di Sistema (ADS).

Di seguito vengono riportate le valutazioni inerenti il rischio. Nella valutazione dei rischi ci si è attenuti alle procedure in atto ed alle modalità operative con cui i dati sono effettivamente trattati, nonché a tutte le situazioni di rischio derivanti da fattori esterni di minaccia all'integrità dei dati (accidentali o deliberati). L'analisi di impatto è stata effettuata combinando due tipologie di rilevazioni:

1) la tipologia dei dati trattati, la loro appetibilità, nonché la loro pericolosità per la privacy dei soggetti cui si riferiscono;
2) le caratteristiche degli strumenti utilizzati per il trattamento dei dati.

I rischi individuati sono raggruppati nelle seguenti categorie:

- Infrastrutture (I);
- Hardware (H);
- Documenti Cartacei (D);
- Apparecchiature di Comunicazione (C);
- Software (S);
- Personale (P).

	4. ANALISI DEI RISCHI PRIVACY E VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

RISCHI LEGATI ALLE INFRASTRUTTURE [TEATRO E PALAZZO SAN MICHELE]

N.	DESCRIZIONE DEL RISCHIO	SITUAZIONE ATTUALE	TIPOLOGIA DI RISCHIO
I-1	Assenza di Protezione dell'edificio (porte, finestre, etc.)	Buona protezione della sede	Lieve
I-2	Assenza di controllo di accesso	L'accesso agli edifici è controllato attraverso citofono, videocamera e portierato	Lieve
I-3	Linea elettrica instabile	Quasi tutti i sistemi di elaborazione dati (Pc) sono collegati ad una unità di continuità	Medio
I-4	Sede suscettibile di allagamenti	La sede del Teatro è ubicata su più superfici. Quella che potrebbe essere, in qualche modo, esposta a tale tipologia di evento è il c.d. "golfo mistico", nel quale, però, non sono conservati documenti o dispositivi elettronici contenenti dati personali. La sede ubicata in Strada San Benedetto 15 è disposta su più superfici. Gli uffici sono ubicati al I° e II° piano. Dunque, tale evento ha scarsa probabilità di verificarsi	Lieve
I-5	Rischio di incendio	Possibilità legata a guasti imprevedibili dell'impianto elettrico e/o evento accidentale Entrambe le sedi dispongono di sistema antincendio	Medio

	4. ANALISI DEI RISCHI PRIVACY E VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

RISCHI LEGATI AI SISTEMI HARDWARE [TEATRO E PALAZZO SAN MICHELE]

N.	DESCRIZIONE DEL RISCHIO	SITUAZIONE ATTUALE	TIPOLOGIA DI RISCHIO
H-1	Assenza di sistemi di rimpiazzo	Sono parzialmente presenti sistemi di rimpiazzo	Medio
H-2	Suscettibilità a variazioni di tensione	Quasi tutti i dispositivi Hardware sono protetti da gruppi di continuità	Medio
H-3	Suscettibilità a variazioni di temperatura	Gli uffici, dotati di impianto centralizzato di climatizzazione, ricevono, sia d'inverno che d'estate, una temperatura costante ed accettabile, evitando sbalzi repentini di temperatura	Lieve
H-4	Suscettibilità a umidità, polvere e sporcizia	Gli ambienti di lavoro sono puliti, non polverosi, né umidi	Lieve
H-5	Suscettibilità a radiazioni elettromagnetiche	Bassa suscettibilità	Lieve
H-6	Manutenzione insufficiente	L'ente non possiede ancora un piano delle manutenzioni e revisioni necessarie per verificare lo stato di efficienza dei dispositivi, in particolare quelli composti da parti meccaniche (stampanti, hard disk, mouse, etc.)	Medio
H-7	Carenze di controllo di configurazione (update/ upgrade dei sistemi)	L'ente non possiede ancora un piano periodico di controllo delle configurazioni	Medio

	4. ANALISI DEI RISCHI PRIVACY E VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

RISCHI LEGATI ALLA GESTIONE DEI DOCUMENTI CARTACEI [TEATRO E PALAZZO SAN MICHELE]

N.	DESCRIZIONE DEL RISCHIO	SITUAZIONE ATTUALE	TIPOLOGIA DI RISCHIO
D-1	Accesso ai documenti non protetto	Utilizzo di armadi e cassettiere per la conservazione dei documenti contenenti dati personali – Accesso alla sede controllato	Lieve
D-2	Carenza di precauzioni nell'eliminazione	I documenti, contenenti dati personali, sono eliminati utilizzando contenitori per la raccolta differenziata della carta, dopo averli accuratamente distrutti. Non sono utilizzati i trita-carte elettronici	Medio
D-3	Non controllo delle copie	I documenti, contenenti dati personali, non sono generalmente duplicati e/o trasmessi all'estero, salvo rari casi	Lieve

RISCHI LEGATI ALLE APPARECCHIATURE DI COMUNICAZIONE [TEATRO E PALAZZO SAN MICHELE]

N.	DESCRIZIONE DEL RISCHIO	SITUAZIONE ATTUALE	TIPOLOGIA DI RISCHIO
C-1	Presenza di linee dial-up (con Modem)	Possibilità di intercettazione delle comunicazioni e di degrado delle performance	Lieve
C-2	Connessione a linea pubblica non protetta	Possibilità di accesso dall'esterno ai documenti contenenti dati personali	Medio

RISCHI LEGATI AL SOFTWARE [TEATRO E PALAZZO SAN MICHELE]

N.	DESCRIZIONE DEL RISCHIO	SITUAZIONE ATTUALE	TIPOLOGIA DI RISCHIO
S-1	Mancanza di autenticazione/ identificazione	Possibilità di accesso da parte di estranei ai dati personali	Lieve
S-2	Carenza/assenza di password management e scorretta allocazione dei diritti di accesso	Possibilità di accesso da parte di estranei ai dati personali	Lieve
S-3	Permanenza di sessioni aperte senza utente	Possibilità di accesso da parte di estranei ai dati personali	Medio
S-4	Carenza di controllo nel caricamento e uso di software/ carenza di controllo di configurazione	Possibilità di malfunzionamenti nel software o presenza di software maligni (virus) che possano precludere o danneggiare i documenti o gli archivi elettronici contenenti dati personali, sono minimizzati dall'utilizzo	Lieve

		di programmi antivirus per i pc con sistema operativo windows. Mentre per i pc con sistema operativo ios non sono installati programmi antivirus	
S-5	Mancanza di copie di backup	Perdita di dati senza possibilità di un corretto ripristino	Lieve
S-6	Incuria nella dismissione di supporti riscrivibili	Possibilità di accessi non autorizzati ai documenti contenenti dati personali	Lieve
S-7	Mancanza del registro delle attività (log)	Impossibilità di conoscere chi ha effettuato accessi non autorizzati ai dati	Lieve
S-8	Errori noti del software	Possibili guasti del software che impediscono il normale svolgimento delle attività o che possono indurre alla perdita dei documenti contenenti dati personali	Lieve

RISCHI LEGATI ALLA GESTIONE DEL PERSONALE [TEATRO E PALAZZO SAN MICHELE]

N.	DESCRIZIONE DEL RISCHIO	SITUAZIONE ATTUALE	TIPOLOGIA DI RISCHIO
P-1	Formazione insufficiente sulla sicurezza e gestione della privacy	Buona la preparazione sulla normativa e sugli adempimenti del Titolare	Lieve
P-2	Rischio di divulgazione accidentale delle informazioni o di accesso non controllato alle informazioni personali	Buona la preparazione sulla normativa e sugli adempimenti del Titolare	Medio

P-3	Rischio di comportamenti sleali o fraudolenti	Buona la preparazione sulla normativa e sugli adempimenti del Titolare, oltre l'adozione del codice etico della Fondazione	Lieve
P-4	Rischio di disattenzione, incuria ed errore materiale	Probabilità legata alla professionalità e competenze, nonché al livello di consapevolezza individuale	Medio

5. MISURE DI SICUREZZA E VIOLAZIONE DEI DATI PERSONALI

Ai sensi dall'art. 32 del Regolamento Europeo in materia di privacy, il titolare del trattamento e il responsabile del trattamento, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo, dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

La protezione dei dati personali non si ottiene solo mettendo in atto misure tecniche di sicurezza informatica, ma richiede anche adeguate misure di sicurezza di tipo organizzativo quali:

- *Formazione periodica di tutto il personale in materia di privacy e sicurezza delle informazioni;*
- *Distribuzione chiara delle responsabilità e delineazione netta delle competenze privacy;*
- *Trattamento dei dati personali solo in osservanza delle procedure e istruzioni aziendali;*
- *Protezione dell'accesso fisico alle sedi e agli strumenti hardware e software;*
- *Controllo delle modalità di assegnazione delle autorizzazioni all'accesso ai dati;*
- *Controllo sulle modalità di accesso ai dati personali;*
- *Documentazione aggiornata periodicamente descrittiva del sistema di gestione privacy.*

In caso di violazione dei dati personali (Data Breach), il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 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 i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo (art. 33 RGPD).
[Con riferimento al c.d. "*data breach*", si prende atto che nel mese di agosto dell'anno 2018, la Fondazione ha subito un "attacco informatico esterno". E' stata prontamente esperita la procedura sopra richiamata e sono state implementate le relative misure tecnologiche ed organizzative].

Al paragrafo 2 del precedente articolo, si chiarisce che il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

Inoltre, il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo (33).

Una violazione di dati personali, se non affrontata in modo adeguato e tempestivo, può provocare danni fisici, materiali o immateriali alle persone fisiche.

Dunque, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento è tenuto a comunicare la violazione anche all'interessato senza ingiustificato ritardo, al fine di consentirgli di prendere tutte le precauzioni necessarie per ridurre l'eventuale danno.
La comunicazione all'interessato deve essere effettuata dal titolare del trattamento descrivendo con un linguaggio semplice e chiaro la natura della violazione dei dati personali e formulando raccomandazioni su come attenuare i potenziali effetti negativi derivanti dalla violazione. La comunicazione deve essere effettuata il prima possibile in stretta collaborazione con l'Autorità Garante Privacy Nazionale competente e nel rispetto degli orientamenti da questa impartiti.

INDIVIDUAZIONE DELLE MISURE PREVENTIVE DA ADOTTARE:

A fronte dell'analisi dei rischi precedentemente descritti, di seguito sono riportate le relative misure di prevenzione, ritenute necessarie oltre che opportune, ai fini del miglioramento della sicurezza dei dati trattati. I rischi sono identificati con la stessa nomenclatura con cui sono stati introdotti precedentemente.

Le contromisure riportate individuano le azioni che si intendono porre, al fine di annullare o limitare le varie vulnerabilità e di contrastare le minacce inerenti il trattamento dei dati personali.

N.	TRATTAMENTI INTERESSATI	MISURA DA ADOTTARE	STRUTTURA O PERSONE ADDETTE ALLA ADOZIONE	TEMPISTICA DI INTERVENTO	RISCHIO RESIDUO
I-1	Tutti	Nessun provvedimento migliorativo da adottare	-	-	Lieve
I-2	Tutti	Nessun provvedimento migliorativo da adottare	-	-	Lieve

N.	TRATTAMENTI INTERESSATI	MISURA DA ADOTTARE	STRUTTURA O PERSONE ADDETTE ALLA ADOZIONE	TEMPISTICA DI INTERVENTO	RISCHIO RESIDUO
I-3	Dati elettronici	a) Installare su tutti i sistemi di elaborazione (Pc) un gruppo di continuità	Titolare/Resp. ADS	Misura adottata parzialmente: Intervento Immediato	Medio
		b) Verificare periodicamente che il gruppo di continuità sia efficiente	Titolare/Resp. ADS	Ogni mese	
I-4	Tutti	Tutti i dispositivi (compreso Pc) di cui dispone la Fondazione, devono essere collocati su un piano rialzato rispetto al pavimento, in modo da ridurre la possibilità che un eventuale allagamento danneggi gli stessi. Anche i documenti cartacei devono essere conservati su ripiani sollevati rispetto al pavimento	Titolare/Resp.	Misura già adottata	Lieve
I-5	Tutti	Come contromisura generale, si consiglia l'installazione di estintori destinati ad essere eventualmente utilizzati nei luoghi nei quali sono conservati i documenti cartacei ed i dispositivi elettronici per l'archiviazione dei dati, nonché le copie dei backup. Per i documenti cartacei si consigliano armadietti e cassettiere ignifughe	Titolare/Resp.	Misure adottate parzialmente: Intervento immediato	Medio
H-1	Dati elettronici	La corretta esecuzione delle operazioni di backup / restore consente di disporre di dispositivi di archiviazione rimovibili con i quali i dati possono facilmente essere ripristinati su altri computer, opportunamente configurati. Possibilità di utilizzo di cloud-ue. Nel caso di cloud extra-ue, il paese in cui ha sede il fornitore deve garantire, in termini di privacy, standard equivalenti a quelli dei paesi europei	Titolare/Resp. ADS	Sempre	Medio

N.	TRATTAMENTI INTERESSATI	MISURA DA ADOTTARE	STRUTTURA O PERSONE ADDETTE ALLA ADOZIONE	TEMPISTICA DI INTERVENTO	RISCHIO RESIDUO
H-2	Dati elettronici (si veda I-3)	a) Installare su tutti i sistemi di elaborazione (Pc) un gruppo di continuità b) Verificare periodicamente che il gruppo di continuità sia efficiente	Titolare/Resp. ADS Titolare/Resp. ADS	Misura adottata parzialmente: Intervento Immediato Ogni mese	Medio
H-3	Dati elettronici	Utilizzare correttamente i sistemi climatizzazione all'interno delle aree in cui sono presenti i dispositivi elettronici utilizzati per il trattamento	Titolare	Sempre	Lieve
H-4	Dati elettronici	Tenere sempre pulito l'ambiente in cui sono utilizzati i dispositivi per il trattamento. Provvedere ad un corretto ricambio d'aria, evitando di creare correnti.	Titolare	Sempre	Lieve
H-5	Dati elettronici	Si ritiene di non dover adottare alcun provvedimento migliorativo	-	Sempre	Lieve
H-6	Dati elettronici	Effettuare mensilmente una verifica via software dell'efficienza dei rischi per individuare eventuali tracce e settori danneggiati. Effettuare annualmente la pulizia ed il controllo di efficienza dei dispositivi che utilizzano parti meccaniche (stampanti, tastiere, fax, mouse,server, etc.)	Titolare/Resp. ADS	Sempre	Lieve
H-7	Dati elettronici	Effettuare periodicamente i controlli di configurazione (update-upgrade dei sistemi)	Titolare/Resp. ADS	Sempre	Lieve
D-1	Dati cartacei	a) Acquisire un armadio dotato di serratura meccanica o, in alternativa, rendere inaccessibile, ad estranei, l'area di lavoro in assenza del titolare o del responsabile	Titolare/Resp. Incaricato	Misura adottata parzialmente	Lieve
		b) Conservare sempre i documenti cartacei, contenenti dati personali, nelle cassettiere destinate alla loro custodia e dotate di chiave di accesso,	Titolare/Resp. Incaricato	La procedura di archiviazione va eseguita sempre	Lieve

N.	TRATTAMENTI INTERESSATI	MISURA DA ADOTTARE	STRUTTURA O PERSONE ADDETTE ALLA ADOZIONE	TEMPISTICA DI INTERVENTO	RISCHIO RESIDUO
		prima di lasciare incustodita l'area di lavoro			
D-2	Dati cartacei	Distruggere i documenti cartacei contenenti dati personali prima di eliminarli	Titolare/Resp. Incaricato	Sempre	Lieve
D-3	Dati cartacei	Si ritiene di non dover adottare nessun provvedimento migliorativo	-	-	Lieve
C-1	Dati elettronici	Si ritiene di non dover adottare nessun provvedimento migliorativo	-	-	Lieve
C-2	Dati elettronici	Utilizzare e verificare che il software Firewall, installato sui computer, sia regolarmente funzionante	Titolare/Resp. ADS	Ogni mese	Medio
S-1	Dati elettronici	Impostare le politiche di sicurezza dei computer in modo che gli utenti siano obbligati ad autenticarsi, prima di accedere agli stessi, utilizzando propriamente username e password di accesso lunga almeno otto caratteri	Titolare ADS	Sempre	Lieve
S-2	Dati elettronici	Impostare le politiche di sicurezza dei computer in modo che le password di accesso ai sistemi siano cambiate ogni sei mesi (o ogni tre mesi nel caso di trattamento di dati sensibili)	Titolare ADS	Sempre	Lieve
S-3	Dati elettronici	Impostare le politiche di sicurezza dei computer in modo che quando un utente lascia incustodita ed attiva la propria postazione di lavoro per più di cinque minuti, l'accesso alla stessa venga inibito costringendo l'utente stesso a ricollegarsi, utilizzando nuovamente le proprie credenziali di accesso	Titolare ADS	Sempre	Medio

N.	TRATTAMENTI INTERESSATI	MISURA DA ADOTTARE	STRUTTURA O PERSONE ADDETTE ALLA ADOZIONE	TEMPISTICA DI INTERVENTO	RISCHIO RESIDUO
S-4	Dati elettronici	Verificare che siano messe in atto le procedure di controllo e di protezione dei software, con particolare rilievo per i software antivirus	Titolare/Resp. ADS	Sempre	Lieve
S-5	Dati elettronici	Eseguire correttamente le procedure di backup e di ripristino dati	Titolare/Resp. ADS	Sempre	Lieve
S-6	Dati elettronici	I dati non più utilizzati non devono poter essere più trattati	Titolare/Resp. Incaricato	Sempre	Lieve
S-7	Dati elettronici	Si consiglia di adottare un registro delle atttività (log), al fine di tracciare eventuali accessi non autorizzati	Titolare	Misura in fase di adozione	Lieve
S-8	Dati elettronici	Si ritiene di non dover adottare alcun provvedimento migliorativo	-	-	Lieve
P-1	Tutti	Mantenersi aggiornati sulle problematiche relative alla gestione dei dati personali e sui relativi adempimenti	Titolare/Resp.	Sempre	Lieve
		Realizzare un meccanismo di separazione dei dati sensibili rispetto agli altri dati personali	Titolare	Entro 05/2018	-
P-2	Tutti	Come punto precedente (P-1)	Titolare	Sempre	Medio
P-3	Tutti	Informare il personale rispetto alle responsabilità e sanzioni in caso di comportamenti sleali e/o fraudolenti	Titolare/Resp.	Sempre	Lieve
P-4	Tutti	Adottare misure che minimizzino errori legati alla disattenzione, incuria ed agli errori materiali	Titolare/Resp.	Sempre	Lieve

FONDAZIONE LIRICO SINFONICA PETRUZZELLI E TEATRI DI BARI	6. IL TRATTAMENTO DEI DATI PERSONALI

Il regolamento europeo all'art. 30 chiarisce che ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:
a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:
a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.

Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.

Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

Tale previsione è una delle varie esplicitazioni del principio di responsabilizzazione (*accountability*) di titolari e responsabili che è una delle importanti novità introdotte con il GDPR. Infatti, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici, viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali. Saranno poi i titolari stessi a dover dimostrare, anche attraverso comportamenti proattivi, di aver concretamente adottato le misure finalizzate ad assicurare l'applicazione del Regolamento.

Dunque, così come chiarito dal Garante della Privacy "*il registro dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema di corretta gestione dei dati personali*", invitando tutti i titolari del trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro.

La Fondazione Lirico Sinfonica Petruzzelli e Teatri di Bari, in qualità di Titolare del Trattamento dei dati, produce il Registro dei Trattamenti del Titolare, incaricando il Responsabile della Protezione Dati (RPD) alla sua tenuta.

Di seguito sono chiariti alcuni aspetti legati al Trattamento dei Dati Personali, i quali verranno schematizzati nel relativo Registro (Allegato A del presente dossier).

TIPOLOGIE DI DATI TRATTATI

Si ricordi che l'art.4, punto 2) del RGPD definisce 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*"; mentre per dato personale, l'art. 4, punto 1) definisce *qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*".

FONDAZIONE LIRICO SINFONICA PETRUZZELLI E TEATRI DI BARI	6. IL TRATTAMENTO DEI DATI PERSONALI

Dalla valutazione di impatto sulla protezione dei dati e dalle risultanze dei questionari predisposti per Aree Funzionali è emerso che la Fondazione tratta le seguenti tipologie di dati:

- Dati Personali, nella fattispecie: Dati identificatici, Dati Sensibili, Dati Giudiziari e Dati di Minori.

Di seguito sono riportati, a titolo esemplificativo e non esaustivo, alcuni elementi che potrebbero essere utilizzati per la costituzione del Registro dei Trattamenti:

- Trattamento
- Ufficio
- Finalità
- Tipi di dati personali
- Categorie di interessati
- Consenso
- Informativa
- Conservazione
- Misure di sicurezza tecniche ed organizzative
- Contitolare del trattamento
- Rappresentante del titolare
- Responsabile del trattamento
- Destinatari delle comunicazioni dei dati personali
- Paese terzo o organizzazione internazionale
- Se applicabile, le garanzie adeguate per il trasferimento

AREE, LOCALI E STRUMENTI CON I QUALI SI EFFETTUANO I TRATTAMENTI

Gli uffici della Fondazione Lirico Sinfonica Petruzzelli e Teatri di Bari sono ubicati presso Strada San Benedetto n.15 (Palazzo San Michele), oltre che in Corso Cavour n.12 (sede del teatro).

Nello specifico, al I° piano di Palazzo San Michele sono ubicati i seguenti uffici:

1 Ufficio Pagamenti e Controllo
2 Ufficio Acquisti
3 Coordinatore Ufficio Contabilità, Finanza e Pagamenti

mentre al II° piano dello stesso edificio sono ubicati i seguenti uffici:

1 Ufficio Grafica ed Editing
2 Ufficio Consulente Informatico
3 Ufficio Responsabile del Personale
3.1 Ufficio del Personale

4 Ufficio Elaborazione Paghe
5 Segreteria Amministrativa
6 Ufficio Protocollo
7 Capo Segreteria di Sovrintendenza
8 Coordinatore Area Educational
9 Segreteria di Sovrintendenza Area Educational
10 Ufficio Direttore Amministrativo
11 Ufficio del Sovrintendente
12 Direzione Artistica
13 Deposito

Al pian terreno rialzato si trova la portineria.

Con riferimenti, invece, agli uffici siti in Teatro, questi sono ubicati in:

Piano strada	I° Piano	II° Piano
1 Botteghino	1 Ufficio del Sovrintendente	1 Ufficio Maestro del Coro
2 Portineria	2 Segreteria Educational	2 Ufficio Manutenzioni
3 Ufficio Stampa	3 Ufficio Capo Reparto Luci e Fonica	3 Ufficio Logistica e Servizi
4 Ufficio Promozione	4 Ufficio Capo Reparto Macchinisti	
5 Archivio Partiture		

III° Piano

1 Ufficio Produzione
2 Ufficio Direttore degli Allestimenti
3 Ufficio Ispettore Coro ed Orchestra
4 Sartoria

Si segnala che in Teatro è situata anche la c.d. Fossa d'Orchestra (Golfo Mistico).

Gli strumenti con i quali si effettuano i trattamenti sono sia elaboratori in rete pubblica (ossia utilizzano, anche solo per alcuni tratti, reti di telecomunicazione disponibili al pubblico, ivi inclusi la rete internet), sia rete privata (ossia sono accessibili, da altri elaboratori o più in generale da altri strumenti elettronici, solo attraverso reti proprietarie, sulle quali possono viaggiare unicamente i dati del titolare del sistema).

In sintesi gli strumenti con i quali si effettuano i trattamenti sono:
1- Elettronici (PC)
2- Cartacei

	6. IL TRATTAMENTO DEI DATI PERSONALI

Di seguito, la tabella riporta sinteticamente la mappa delle Aree funzionali della Fondazione coinvolte nel trattamento dei dati personali, oltre agli strumenti utilizzati.

AREA FUNZIONALE	CARTACEO	PC	ALTRI STRUMENTI
AREA DI SOVRINTENDENZA	X	X	
AREA DI SEGRETERIA ARTISTICA	X	X	
AREA AMMINISTRATIVA	X	X	
AREA DEL PERSONALE	X	X	
AREA DELLA PRODUZIONE		X	
AREA DEI PROCESSI	X	X	
AREA TECNICA	X	X	

Il Trattamento dei dati personali, oltre che dal Titolare, viene effettuato solo da soggetti (Responsabile del Trattamento / Incaricato etc.) che hanno ricevuto un formale incarico, mediante designazione per iscritto di ogni singolo incaricato, con la quale si individua puntualmente l'ambito del trattamento consentito.

Le lettere ed i contratti di nomina dei responsabili, le lettere di incarico di designazione degli incaricati vengono raccolte in modo ordinato, in base alla unità organizzativa cui i soggetti appartengono: in tale modo il Titolare dispone di un quadro chiaro di chi fa cosa, nell'ambito del trattamento dei dati personali. La Fondazione procederà ad aggiornare, periodicamente, la definizione dei dati cui i responsabili e/o incaricati sono autorizzati ad accedere e dei trattamenti che sono autorizzati a porre in essere, al fine di verificare la sussistenza delle condizioni che giustificano tali autorizzazioni.

Oltre alle istruzioni generali su come devono essere trattati i dati personali, agli incaricati e responsabili sono fornite esplicite istruzioni relativamente a:

- procedure da eseguire per la classificazione dei dati personali;
- modalità di reperimento dei documenti contenenti dati personali e modalità da osservare per la custodia e l'archiviazione degli stessi;
- modalità per elaborare e custodire le password necessarie per accedere agli elaboratori elettronici e ai dati in essi contenuti, nonché per fornire copia al preposto alla custodia della parola chiave (Lettera di nomina del Custode delle Password);
- prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro;
- procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi;
- procedure per il salvataggio dei dati;
- modalità di utilizzo, custodia e archiviazione dei supporti rimovibili contenenti dati personali;

- aggiornamento continuo, utilizzando il materiale e gli strumenti forniti dal Responsabile, sulle misure di sicurezza.

Ai soggetti incaricati al trattamento, il Responsabile Protezione dei Dati fornisce la necessaria formazione:
- al momento dell'ingresso in servizio;
- in occasione di cambiamenti di mansione;
- in occasione dell'introduzione di nuovi strumenti e programmi informatici, con l'ausilio dell'Amministratore di Sistema e/o dell'Addetto IT.

La formazione impartita riguarda:
- norme generali in materia di privacy;
- conoscenza dei rischi;
- conoscenza delle misure di sicurezza e dei comportamenti da adottare;
- responsabilità.

La formazione viene documentata.

PRESCRIZIONI DI CARATTERE GENERALE PER IL TRATTAMENTO DEI DATI PERSONALI DA PARTE DELL'AMMINISTRATORE DI SISTEMA ESTERNO (ADS)

Di seguito sono indicate alcune prescrizioni di carattere generale per il trattamento dei dati personali da parte dell'ADS Esterno:

1) Richiedere e utilizzare soltanto i dati personali necessari al raggiungimento delle finalità contrattuali;
2) Procedere alla classificazione dei dati personali al momento della loro raccolta;
3) Accertarsi che gli interessati abbiano ricevuto l'informativa e dato il consenso al trattamento;
4) Rispettare le procedure per il reperimento, la custodia e l'archiviazione dei dati personali;
5) Custodire i dati oggetto del trattamento in luoghi non accessibili a soggetti non autorizzati;
6) Rispettare le procedure per la configurazione e l'utilizzo degli strumenti elettronici e degli applicativi aziendali;
7) Osservare le prescrizioni per la creazione, l'utilizzo, la custodia e la modifica delle credenziali di autenticazione;
8) Rispettare le procedure per la configurazione e l'utilizzo di internet, della posta elettronica e del telefono aziendale;
9) Non lasciare incustoditi e accessibili gli strumenti elettronici utilizzati per il trattamento;
10) Non rendere accessibili o comunicare a terzi le proprie credenziali di autenticazione (username e password);
11) Rispettare le procedure per il salvataggio periodico dei dati;

12) Osservare le procedure per l'utilizzo, la custodia e l'archiviazione dei supporti rimovibili;
13) Non lasciare incustodito il proprio posto di lavoro prima di aver provveduto alla messa in sicurezza dei dati;
14) Procedere all'archiviazione definitiva dei documenti al termine delle attività di trattamento;
15) Accertarsi dell'identità di terzi e della loro autorizzazione al ritiro di documentazione in uscita;
16) Non comunicare dati senza l'autorizzazione dell'interessato e l'identificazione del richiedente;
17) Non diffondere dati personali sensibili e/o giudiziari;

Il Registro dei Trattamenti riporterà, in maniera esaustiva, ogni dettaglio inerente i Trattamenti dei dai personali della Fondazione (Allegato A).

VIDEOSORVEGLIANZA

La Fondazione è dotata di sistema di videosorveglianza sia per la sede ubicata in Strada San Benedetto n.15 che per la sede del Teatro (*Allegato C*).

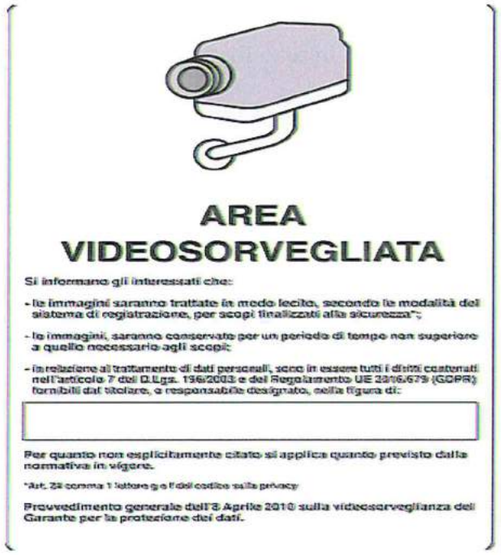
Il c.d. supporto con l'informativa, in caso di utilizzo di tale strumento:

- deve essere collocato nei luoghi ripresi o nelle immediate vicinanze, non necessariamente a contatto con la telecamera;
- deve avere un formato ed un posizionamento tale da essere chiaramente visibile;
- può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati se le immagini sono solo visionate o anche registrate.

Il Garante promuove la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato con strumenti elettronici di rilevamento di immagini, prevedendo specifiche modalità di trattamento e forme semplificate di informativa all'interessato per garantire la liceità e la correttezza del trattamento (art.134 D.Lgs. 196/03 e s.m.i.).

Informativa sintetica da trascrivere su appositi cartelli in caso di videosorveglianza: "I locali sono videosorvegliati. Ai sensi dell'art. 13 del D.Lgs. 196/2003 e s.m.i., Codice in materia di protezione dei dati personali e ai sensi del DGPD n.679/16, si informa che il trattamento dei dati personali è effettuato esclusivamente per finalità di accertamento e prevenzione dei reati. I dati potranno essere oggetto di comunicazione ai soggetti che effettuano indagini giudiziarie. I dati sono conservati per il periodo strettamente necessario al perseguimento delle finalità menzionate presso la Fondazione Lirico Sinfonica Petruzzelli e Teatri di Bari in qualità del Titolare del Trattamento dei dati. I diritti previsti dall'art. 7 del D.Lgs. 196/03 e s.m.i., fra cui il diritto di ottenere l'indicazione dell'origine dei dati, delle finalità e delle modalità del trattamento, la cancellazione dei dati trattati in violazione

di legge, possono essere esercitati rivolgendosi al Titolare del Trattamento".



AREA VIDEOSORVEGLIATA

Si informano gli interessati che:

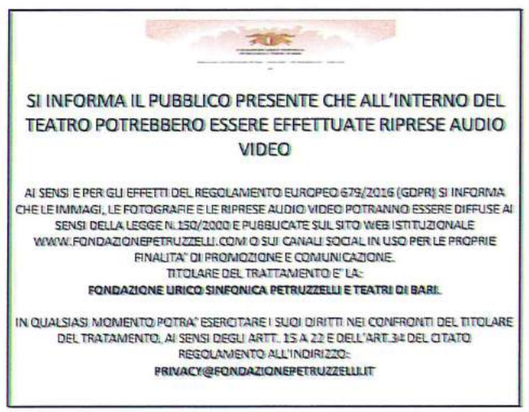
- le immagini saranno trattate in modo lecito, secondo le modalità del sistema di registrazione, per scopi finalizzati alla sicurezza*;
- le immagini, saranno conservate per un periodo di tempo non superiore a quello necessario agli scopi;
- in relazione al trattamento di dati personali, sono in essere tutti i diritti contenuti nell'articolo 7 del D.Lgs. 196/2003 e del Regolamento UE 2016/679 (GDPR) fornibili dal titolare, o responsabile designato, nella figura di:

Per quanto non esplicitamente citato si applica quanto previsto dalla normativa in vigore.

*Art. 24 comma 1 lettera g e f del codice sulla privacy

Provvedimento generale dell'8 Aprile 2010 sulla videosorveglianza del Garante per la protezione dei dati.

Con riferimento alla sede del Teatro, la Fondazione esposte una targa, collocata in una posizione visibile, di facile accesso e lettura, contenente la dicitura, come di seguito:



SI INFORMA IL PUBBLICO PRESENTE CHE ALL'INTERNO DEL TEATRO POTREBBERO ESSERE EFFETTUATE RIPRESE AUDIO VIDEO

AI SENSI E PER GLI EFFETTI DEL REGOLAMENTO EUROPEO 679/2016 (GDPR) SI INFORMA CHE LE IMMAGI, LE FOTOGRAFIE E LE RIPRESE AUDIO VIDEO POTRANNO ESSERE DIFFUSE AI SENSI DELLA LEGGE N. 150/2000 E PUBBLICATE SUL SITO WEB ISTITUZIONALE WWW.FONDAZIONEPETRUZZELLI.COM O SUI CANALI SOCIAL IN USO PER LE PROPRIE FINALITA' DI PROMOZIONE E COMUNICAZIONE.
TITOLARE DEL TRATTAMENTO E' LA:
FONDAZIONE LIRICO SINFONICA PETRUZZELLI E TEATRI DI BARI.

IN QUALSIASI MOMENTO POTRA' ESERCITARE I SUOI DIRITTI NEI CONFRONTI DEL TITOLARE DEL TRATAMENTO, AI SENSI DEGLI ARTT. 15 A 22 E DELL'ART.34 DEL CITATO REGOLAMENTO ALL'INDIRIZZO:
PRIVACY@FONDAZIONEPETRUZZELLI.IT

La Fondazione individua internamente, fra i propri dipendenti, il soggetto incaricato alla visione del materiale video-registrato.

La Fondazione, procede alla predisposizione della Valutazione di Impatto Rischi in connessione ai trattamenti di Videosorveglianza ex art. 35 GDPR (*Allegato C*).

DATI PERSONALI DI MINORI

I minori meritano una specifica protezione dei loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze nonché dei loro diritti in relazione al trattamento dei propri dati personali. Per tale motivo, l'offerta diretta di servizi della Fondazione a minori è lecita solo se il minore abbia compiuto almeno 16 anni ed abbia firmato il proprio consenso al trattamento dei propri dati personali. Nel caso in cui il minore abbia una età inferiore a 16 anni, il trattamento dei dati è lecito soltanto se il consenso è prestato o autorizzato da un genitore o da un soggetto avente la legale potestà. Il Titolare del Trattamento ha sempre l'obbligo di verificare la validità del consenso di un minore.

7. SISTEMA DI GESTIONE PRIVACY: CERTIFICAZIONE PRIVACY E CODICI DI CONDOTTA

L'articolo 40 del RGPD stabilisce che gli Stati membri, le autorità di controllo, il comitato e la commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del presente regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese.

Le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento possono elaborare i codici di condotta, modificarli o prorogarli, allo scopo di precisare l'applicazione del presente regolamento, ad esempio relativamente a:

a) il trattamento corretto e trasparente dei dati;
b) i legittimi interessi perseguiti dal responsabile del trattamento in contesti specifici;
c) la raccolta dei dati personali;
d) la pseudonimizzazione dei dati personali;
e) l'informazione fornita al pubblico e agli interessati;
f) l'esercizio dei diritti degli interessati;
g) l'informazione fornita e la protezione del minore e le modalità con cui è ottenuto il consenso dei titolari della responsabilità genitoriale sul minore;
h) le misure e le procedure di cui agli articoli 24 e 25 e le misure volte a garantire la sicurezza del trattamento di cui all'articolo 32;
i) la notifica di una violazione dei dati personali alle autorità di controllo e la comunicazione di tali violazioni dei dati personali all'interessato;
j) il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali; o
k) le procedure stragiudiziali e di altro tipo per comporre le controversie tra titolari del trattamento e interessati in materia di trattamento, fatti salvi i diritti degli interessati ai sensi degli articoli 77 e 79.

Oltre all'adesione ai codici di condotta approvati ai sensi del paragrafo 5 del presente articolo e aventi validità generale a norma del paragrafo 9 del presente articolo da parte di titolari o responsabili soggetti al presente regolamento, possono aderire a tali codici di condotta anche i titolari del trattamento o i responsabili del trattamento che non sono soggetti al presente regolamento ai sensi dell'articolo 3, al fine di fornire adeguate garanzie nel quadro dei trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali alle condizioni di cui all'articolo 46, paragrafo 2, lettera e). Detti titolari del trattamento o responsabili del trattamento assumono l'impegno vincolante e azionabile, mediante strumenti contrattuali o di altro tipo giuridicamente vincolanti, di applicare le stesse adeguate garanzie anche per quanto riguarda i diritti degli interessati.

Il codice di condotta di cui al paragrafo 2 del presente articolo contiene i meccanismi che consentono all'organismo di cui all'articolo 41, paragrafo 1, di effettuare il controllo obbligatorio del rispetto delle norme del codice da parte dei titolari del trattamento o dei responsabili del trattamento che si impegnano ad applicarlo, fatti salvi i compiti e i poteri delle autorità di controllo competenti ai sensi degli articoli 55 o 56.

Le associazioni e gli altri organismi di cui al paragrafo 2 del presente articolo che intendono elaborare un codice di condotta o modificare o prorogare un codice esistente sottopongono il progetto di codice, la modifica o la proroga all'autorità di controllo competente ai sensi dell'articolo 55. L'autorità di controllo esprime un parere sulla conformità al presente regolamento del progetto di codice, della modifica o della proroga e approva tale progetto, modifica o proroga, se ritiene che offra in misura sufficiente garanzie adeguate.

Qualora il progetto di codice, la modifica o la proroga siano approvati ai sensi dell'articolo 55, e se il codice di condotta in questione non si riferisce alle attività di trattamento in vari Stati membri, l'autorità di controllo registra e pubblica il codice.

Qualora il progetto di codice di condotta si riferisca alle attività di trattamento in vari Stati membri, prima di approvare il progetto, la modifica o la proroga, l'autorità di controllo che è competente ai sensi dell'articolo 55 lo sottopone, tramite la procedura di cui all'articolo 63, al comitato, il quale formula un parere sulla conformità al presente regolamento del progetto di codice, della modifica o della proroga o, nel caso di cui al paragrafo 3 del presente articolo, sulla previsione di adeguate garanzie.

Qualora il parere di cui al paragrafo 7 confermi che il progetto di codice di condotta, la modifica o la proroga è conforme al presente regolamento o, nel caso di cui al paragrafo 3, fornisce adeguate garanzie, il comitato trasmette il suo parere alla Commissione.

La Commissione può decidere, mediante atti di esecuzione, che il codice di condotta, la modifica o la proroga approvati, che le sono stati sottoposti ai sensi del paragrafo 8 del presente articolo, hanno validità generale all'interno dell'Unione. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.

La Commissione provvede a dare un'adeguata pubblicità dei codici approvati per i quali è stata decisa la validità generale ai sensi del paragrafo 9.

Il comitato raccoglie in un registro tutti i codici di condotta, le modifiche e le proroghe approvati e li rende pubblici mediante mezzi appropriati.

MONITORAGGIO DEI CODICI DI CONDOTTA

Fatti salvi i compiti e i poteri dell'autorità di controllo competente di cui agli articoli 57 e 58, il controllo della conformità con un codice di condotta ai sensi dell'articolo 40 può essere effettuato da un organismo in possesso del livello adeguato di competenze riguardo al contenuto del codice e del necessario accreditamento a tal fine dell'autorità di controllo competente.

L'organismo di cui al paragrafo 1 può essere accreditato a monitorare l'osservanza di un codice di condotta se esso ha:
a) dimostrato in modo convincente all'autorità di controllo competente di essere indipendente e competente riguardo al contenuto del codice;
b) istituito procedure che gli consentono di valutare l'ammissibilità dei titolari del trattamento e dei responsabili del trattamento in questione ad applicare il codice, di controllare che detti titolari e responsabili ne rispettino le disposizioni e di riesaminarne periodicamente il funzionamento;
c) istituito procedure e strutture atte a gestire i reclami relativi a violazioni del codice o il modo in cui il codice è stato o è attuato da un titolare del trattamento o un responsabile del trattamento e a rendere dette procedure e strutture trasparenti per gli interessati e il pubblico; e
d) dimostrato in modo convincente all'autorità di controllo competente che i compiti e le funzioni da esso svolti non danno adito a conflitto di interessi.

L'autorità di controllo competente presenta al comitato il progetto di criteri per l'accreditamento dell'organismo di cui al paragrafo 1 del presente articolo, ai sensi del meccanismo di coerenza di cui all'articolo 63.

Fatti salvi i compiti e i poteri dell'autorità di controllo competente e le disposizioni del capo VIII, un organismo di cui al paragrafo 1 del presente articolo adotta, stanti garanzie appropriate, le opportune misure in caso di violazione del codice da parte di un titolare del trattamento o responsabile del trattamento, tra cui la sospensione o l'esclusione dal codice del titolare del trattamento o del responsabile del trattamento. Esso informa l'autorità di controllo competente di tali misure e dei motivi della loro adozione.

L'autorità di controllo competente revoca l'accreditamento dell'organismo di cui al paragrafo 1, se le condizioni per l'accreditamento non sono, o non sono più, rispettate o se le misure adottate dall'organismo violano il presente regolamento.

Il presente articolo (art. 41) non si applica al trattamento effettuato da autorità pubbliche e da organismi pubblici.

CERTIFICAZIONE

Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano, in particolare a livello di Unione, l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento. Sono tenute in considerazione le esigenze specifiche delle micro, piccole e medie imprese.

Oltre all'adesione dei titolari del trattamento o dei responsabili del trattamento soggetti al presente regolamento, i meccanismi, i sigilli o i marchi approvati ai sensi del paragrafo 5 del presente articolo, possono essere istituiti al fine di dimostrare la previsione di garanzie appropriate da parte dei titolari del trattamento o responsabili del trattamento non soggetti al presente regolamento ai sensi dell'articolo 3, nel quadro dei trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali alle condizioni di cui all'articolo 46, paragrafo 2, lettera f). Detti titolari del trattamento o responsabili del trattamento assumono l'impegno vincolante e azionabile, mediante strumenti contrattuali o di altro tipo giuridicamente vincolanti, di applicare le stesse adeguate garanzie anche per quanto riguarda i diritti degli interessati.

La certificazione è volontaria e accessibile tramite una procedura trasparente.

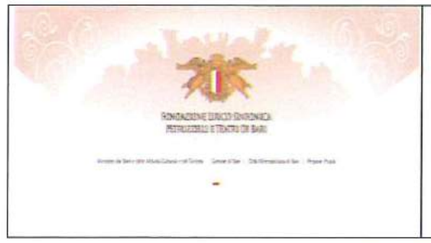
La certificazione ai sensi del presente articolo non riduce la responsabilità del titolare del trattamento o del responsabile del trattamento riguardo alla conformità al presente regolamento e lascia impregiudicati i compiti e i poteri delle autorità di controllo competenti a norma degli articoli 55 o 56.

La certificazione ai sensi del presente articolo è rilasciata dagli organismi di certificazione di cui all'articolo 43 o dall'autorità di controllo competente in base ai criteri approvati da tale autorità di controllo competente ai sensi dell'articolo 58, paragrafo 3, o dal comitato, ai sensi dell'articolo 63. Ove i criteri siano approvati dal comitato, ciò può risultare in una certificazione comune, il sigillo europeo per la protezione dei dati.

Il titolare del trattamento o il responsabile del trattamento che sottopone il trattamento effettuato al meccanismo di certificazione fornisce all'organismo di certificazione di cui all'articolo 43 o, ove applicabile, all'autorità di controllo competente tutte le informazioni e l'accesso alle attività di trattamento necessarie a espletare la procedura di certificazione.

La certificazione è rilasciata al titolare del trattamento o responsabile del trattamento per un periodo massimo di tre anni e può essere rinnovata alle stesse condizioni purché continuino a essere soddisfatti i requisiti pertinenti. La certificazione è revocata, se del caso, dagli organismi di certificazione di cui all'articolo 43 o dall'autorità di controllo competente, a seconda dei casi, qualora non siano o non siano più soddisfatti i requisiti per la certificazione.

Il comitato raccoglie in un registro tutti i meccanismi di certificazione e i sigilli e i marchi di protezione dei dati e li rende pubblici con qualsiasi mezzo appropriato.



7. SISTEMA DI GESTIONE PRIVACY: CERTIFICAZIONE PRIVACY E CODICI DI CONDOTTA

ORGANISMI DI CERTIFICAZIONE

Fatti salvi i compiti e i poteri dell'autorità di controllo competente di cui agli articoli 57 e 58, gli organismi di certificazione in possesso del livello adeguato di competenze riguardo alla protezione dei dati, rilasciano e rinnovano la certificazione, dopo averne informato l'autorità di controllo al fine di consentire alla stessa di esercitare i suoi poteri a norma dell'articolo 58, paragrafo 2, lettera h), ove necessario. Gli Stati membri garantiscono che tali organismi di certificazione siano accreditati da uno o entrambi dei seguenti organismi:
a) dall'autorità di controllo competente ai sensi degli articoli 55 o 56;
b) dall'organismo nazionale di accreditamento designato in virtù del regolamento (CE) n.765/2008 del Parlamento europeo e del Consiglio (20) conformemente alla norma ENISO/IEC 17065/2012 e ai requisiti aggiuntivi stabiliti dall'autorità di controllo competente ai sensi degli articoli 55 o 56.2.

Gli organismi di certificazione di cui al paragrafo 1 sono accreditati in conformità di tale paragrafo solo se:
a) hanno dimostrato in modo convincente all'autorità di controllo competente di essere indipendenti e competenti riguardo al contenuto della certificazione;
b) si sono impegnati a rispettare i criteri di cui all'articolo 42, paragrafo 5, e approvati dall'autorità di controllo competente ai sensi degli articoli 55 o 56 o dal comitato, ai sensi dell'articolo 63;
c) hanno istituito procedure per il rilascio, il riesame periodico e il ritiro delle certificazioni, dei sigilli e dei marchi di protezione dei dati;
d) hanno istituito procedure e strutture atte a gestire i reclami relativi a violazioni della certificazione o il modo in cui la certificazione è stata o è attuata dal titolare del trattamento o dal responsabile del trattamento e a rendere dette procedure e strutture trasparenti per gli interessati e il pubblico; e
e) hanno dimostrato in modo convincente all'autorità di controllo competente che i compiti e le funzioni da loro svolti non danno adito a conflitto di interessi.

L'accreditamento degli organi di certificazione di cui ai paragrafi 1 e 2 del presente articolo ha luogo in base ai criteri approvati dall'autorità di controllo competente ai sensi degli articoli 55 o 56 o dal comitato, ai sensi dell'articolo 63. In caso di accreditamento ai sensi del paragrafo 1, lettera b), del presente articolo, tali requisiti integrano quelli previsti dal regolamento (CE) n. 765/2008 nonché le norme tecniche che definiscono i metodi e le procedure degli organismi di certificazione.

Gli organismi di certificazione di cui al paragrafo 1 sono responsabili della corretta valutazione che comporta la certificazione o la revoca di quest'ultima, fatta salva la responsabilità del titolare del trattamento o del responsabile del trattamento riguardo alla conformità al presente regolamento. L'accreditamento è rilasciato per un periodo massimo di cinque anni e può essere rinnovato alle stesse condizioni purché l'organismo di certificazione soddisfi i requisiti.

L'organismo di certificazione di cui al paragrafo 1 trasmette all'autorità di controllo competente i motivi del rilascio o della revoca della certificazione richiesta.

I requisiti di cui al paragrafo 3 del presente articolo e i criteri di cui all'articolo 42, paragrafo 5, sono resi pubblici dall'autorità di controllo in forma facilmente accessibile. Le autorità di controllo provvedono a trasmetterli anche al comitato. Il comitato raccoglie in un registro tutti i meccanismi di certificazione e i sigilli di protezione dei dati e li rende pubblici con qualsiasi mezzo appropriato.

Fatto salvo il capo VIII, l'autorità di controllo competente o l'organismo nazionale di accreditamento revoca l'accreditamento di un organismo di certificazione di cui al paragrafo 1 del presente articolo, se le condizioni per l'accreditamento non sono, o non sono più, rispettate o se le misure adottate da un organismo di certificazione violano il presente regolamento.

Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 92 al fine di precisare i requisiti di cui tenere conto per i meccanismi di certificazione della protezione dei dati di cui all'articolo 42, paragrafo 1.

La Commissione può adottare atti di esecuzione per stabilire norme tecniche riguardanti i meccanismi di certificazione e i sigilli e marchi di protezione dei dati e le modalità per promuovere e riconoscere tali meccanismi di certificazione, i sigilli e marchi di protezione dei dati. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.

8. TRASFERIMENTO DEI DATI ALL'ESTERO

L'articolo 44 del regolamento europeo chiarisce che qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui al presente capo, fatte salve le altre disposizioni del presente regolamento. Tutte le disposizioni del presente capo sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato.

Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche.

Nel valutare l'adeguatezza del livello di protezione, la Commissione prende in considerazione in particolare i seguenti elementi:
a) lo stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, la pertinente legislazione generale e settoriale (anche in materia di sicurezza pubblica, difesa, sicurezza nazionale, diritto penale e accesso delle autorità pubbliche ai dati personali), così come l'attuazione di tale legislazione, le norme in materia di protezione dei dati, le norme professionali e le misure di sicurezza, comprese le norme per il trasferimento successivo dei dati personali verso un altro paese terzo o un'altra organizzazione internazionale osservate nel paese o dall'organizzazione internazionale in questione, la giurisprudenza nonché i diritti effettivi e azionabili degli interessati e un ricorso effettivo in sede amministrativa e giudiziaria per gli interessati i cui dati personali sono oggetto di trasferimento;
b) l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti nel paese terzo o cui è soggetta un'organizzazione internazionale, con competenza per garantire e controllare il rispetto delle norme in materia di protezione dei dati, comprensiva di adeguati poteri di esecuzione, per assistere e fornire consulenza agli interessati in merito all'esercizio dei loro diritti e cooperare con le autorità di controllo degli Stati membri; e
c) gli impegni internazionali assunti dal paese terzo o dall'organizzazione internazionale in questione o altri obblighi derivanti da convenzioni o strumenti giuridicamente vincolanti come pure dalla loro partecipazione a sistemi multilaterali o regionali, in particolare in relazione alla protezione dei dati personali.

La Commissione, previa valutazione dell'adeguatezza del livello di protezione, può decidere, mediante atti di esecuzione, che un paese terzo, un territorio o uno o più settori specifici all'interno di un paese terzo, o un'organizzazione internazionale garantiscono un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo. L'atto di esecuzione prevede un meccanismo di riesame periodico, almeno ogni quattro anni, che tenga conto di tutti gli sviluppi pertinenti nel paese terzo o nell'organizzazione internazionale.

L'atto di esecuzione specifica il proprio ambito di applicazione geografico e settoriale e, ove applicabile, identifica la o le autorità di controllo di cui al paragrafo 2, lettera b), del presente articolo. L'atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.

La Commissione controlla su base continuativa gli sviluppi nei paesi terzi e nelle organizzazioni internazionali che potrebbero incidere sul funzionamento delle decisioni adottate a norma del paragrafo 3 del presente articolo e delle decisioni adottate sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46/CE.

Se risulta dalle informazioni disponibili, in particolare in seguito al riesame di cui al paragrafo 3 del presente articolo, che un paese terzo, un territorio o uno o più settori specifici all'interno di un paese terzo, o un'organizzazione internazionale non garantiscono più un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo, la Commissione revoca, modifica o sospende nella misura necessaria la decisione di cui al paragrafo 3 del presente articolo mediante atti di esecuzione senza effetto retroattivo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 93, paragrafo 2, o, in casi di estrema urgenza, secondo la procedura di cui all'articolo 93, paragrafo 3. Per imperativi motivi di urgenza debitamente giustificati, la Commissione adotta atti di esecuzione immediatamente applicabili secondo la procedura di cui all'articolo 93, paragrafo 3.

La Commissione avvia consultazioni con il paese terzo o l'organizzazione internazionale per porre rimedio alla situazione che ha motivato la decisione di cui al paragrafo 5.

Una decisione ai sensi del paragrafo 5 del presente articolo lascia impregiudicato il trasferimento di dati personali verso il paese terzo, il territorio o uno o più settori specifici all'interno del paese terzo, o verso l'organizzazione internazionale in questione, a norma degli articoli da 46 a 49.

La Commissione pubblica nella Gazzetta ufficiale dell'Unione europea e sul suo sito web l'elenco dei paesi terzi, dei territori e settori specifici all'interno di un paese terzo, e delle organizzazioni internazionali per i quali ha deciso che è o non è più garantito un livello di protezione adeguato.

Le decisioni adottate dalla Commissione in base all'articolo 25, paragrafo 6, della direttiva 95/46/CE restano in vigore fino a quando non sono modificate, sostituite o abrogate da una decisione della Commissione adottata conformemente al paragrafo 3 o 5 del presente articolo.

TRASFERIMENTO SULLA BASE DI UNA DECISIONE DI ADEGUATEZZA

In mancanza di una decisione ai sensi dell'articolo 45, paragrafo 3, il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi.

Possono costituire garanzie adeguate di cui al paragrafo 1 senza necessitare di autorizzazioni specifiche da parte di un'autorità di controllo:
a) uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici;
b) le norme vincolanti d'impresa in conformità dell'articolo 47;
c) le clausole tipo di protezione dei dati adottate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2;
d) le clausole tipo di protezione dei dati adottate da un'autorità di controllo e approvate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2;
e) un codice di condotta approvato a norma dell'articolo 40,unitamente all'impegno vincolante ed esecutivo da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati; o
f) un meccanismo di certificazione approvato a norma dell'articolo 42, unitamente all'impegno vincolante ed esigibile da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati.

Fatta salva l'autorizzazione dell'autorità di controllo competente, possono altresì costituire in particolare garanzie adeguate di cui al paragrafo 1:
a) le clausole contrattuali tra il titolare del trattamento o il responsabile del trattamento e il titolare del trattamento, il responsabile del trattamento o il destinatario dei dati personali nel paese terzo o nell'organizzazione internazionale; o
b) le disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati.

L'autorità di controllo applica il meccanismo di coerenza di cui all'articolo 63 nei casi di cui al paragrafo 3 del presente articolo.

Le autorizzazioni rilasciate da uno Stato membro o dall'autorità di controllo in base all'articolo 26, paragrafo 2, della direttiva 95/46/CE restano valide fino a quando non vengono modificate, sostituite o abrogate, se necessario, dalla medesima autorità di controllo.

Le decisioni adottate dalla Commissione in base all'articolo 26, paragrafo 4, della direttiva 95/46/CE restano in vigore fino a quando non vengono modificate, sostituite o abrogate, se necessario, da una decisione della Commissione adottata conformemente al paragrafo 2 del presente articolo.

TRASFERIMENTO O COMUNICAZIONE NON AUTORIZZATI DAL DIRITTO

Le sentenze di un'autorità giurisdizionale e le decisioni di un'autorità amministrativa di un paese terzo che dispongono il trasferimento o la comunicazione di dati personali da parte di un titolare del trattamento o di un responsabile del trattamento possono essere riconosciute o assumere qualsivoglia carattere esecutivo soltanto se basate su un accordo internazionale in vigore tra il paese terzo richiedente e l'Unione o un suo Stato membro, ad esempio un trattato di mutua assistenza giudiziaria, fatti salvi gli altri presupposti di trasferimento a norma del presente capo.

	9. GEOLOCALIZZAZIONE

GEOLOCALIZZAZIONE

Con l'evoluzione delle nuove tecnologie, altri dati personali hanno assunto un ruolo significativo, come quelli relativi alle comunicazioni elettroniche (via Internet o telefono) e quelli che consentono la geolocalizzazione, fornendo informazioni sui luoghi frequentati e sugli spostamenti.

La Fondazione utilizza un sistema di gestione delle presenze/assenze del proprio personale dipendente che consente di poter scegliere l'opzione di timbratura (da supporto fisso oppure con utilizzo di timbratura virtuale). La timbratura virtuale è fruibile dagli smartphone dei dipendenti della Fondazione, attraverso una specifica applicazione (Keros), che necessita dell'attivazione del sistema di geolocalizzazione.

A tal riguardo, il Titolare del Trattamento o il Responsabile ove individuato, potrà utilizzare i dati personali rinvenienti dal sistema di gestone del personale, esclusivamente per le finalità per cui sono stati raccolti e per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

I dipendenti della Fondazione potranno configurare il proprio apparecchio mobile in modo tale che la geolocalizzazione si attivi solo durante la procedura di timbratura virtuale. Al termine della stessa, il dipendente potrà disattivare la funzione di localizzazione.

Ad ogni modo, la Fondazione non ha facoltà alcuna a poter utilizzare i dati rinvenienti dalla geolocalizzazione, quale strumento di controllo dei propri dipendenti durante e/o fuori le ore di lavoro, fermo restando che, in caso di timbratura virtuale, la Fondazione potrà riscontrare la coerenza tra il luogo dal quale si è timbrato ed il luogo dal quale si sarebbe dovuto timbrare (es. un dipendente che lavora presso la sede di Palazzo San Michele, non può timbrare virtualmente dalla propria abitazione).

In casi di eventi improvvisi e pericolosi, la Fondazione, di concerto con le autorità competenti, potrà utilizzare i dati rinvenienti dalla geolocalizzazione dei dipendenti, esclusivamente per fini legati alla prevenzione e sicurezza (es. in caso di incendio l'autorità di polizia e/o i Vigili del Fuoco possono utilizzare i dati estrapolabili dalla localizzazione dei dipendenti, per conoscere, ad esempio, chi risiede al momento dell'incendio all'interno della sede).

Tutti i dati inseriti ed archiviati sono protetti da nome utente e password e non sono accessibili dal fornitore del sistema di gestione del personale. Quest'ultimo potrà accedervi, con proprie credenziali, esclusivamente per eventuali aggiornamenti e/o manutenzione del programma.

	10. ALTRE INFORMAZIONI

COOKIES

Il sito della Fondazione, www.fondazionepetruzzelli.com, utilizza cookies tecnici ed analitici, anche di terze parti, necessari al funzionamento del sito ed al miglioramento dell'esperienza di navigazione dell'utente. Con riferimento alla privacy policy sintetica ed integrale consultabile sul sito istituzionale, la Fondazione ha posto in essere interventi correttivi necessari all'adeguamento al Regolamento Europeo 679/2016.

NOTE DI RISERVATEZZA DA INSERIRE IN CALCE ALLE EMAIL

Con riferimento alle e-mail in uscita, la Fondazione potrà utilizzare, in calce alle stesse, la seguente dicitura:

Questo documento è formato esclusivamente per il destinatario. Tutte le informazioni ivi contenute, compresi eventuali allegati, sono da ritenere esclusivamente confidenziali e riservate secondo i termini del vigente D.Lgs. 196/2003 e s.m.i. in materia di privacy e del Regolamento europeo 679/2016 – GDPR- e quindi ne è proibita l'utilizzazione ulteriore non autorizzata. Se avete ricevuto per errore questo messaggio, Vi preghiamo cortesemente di contattare immediatamente il mittente e cancellare la e-mail.

Confidentiality Notice – This e-mail message including any attachments is for the sole use of the intended recipient and may contain confidential and privileged information pursuant to Legislative Decree 196/2003 and s.m.i and the European General Data Protection Regulation 679/2016 – GDPR-. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply e-mail and destroy all copies of the original message.

Il presente documento che sostituisce, modifica ed integra il precedente, è composto da 67 pagine, oltre gli allegati A), B), C), D), E), F).

Documento Privacy Aggiornato al 02 aprile 2019

Timbro e Firma del Titolare del Trattamento Dati Personali
FONDAZIONE LIRICO SINFONICA PETRUZZELLI E TEATRI DI BARI