MODELLO DI CONFORMITA'

PRIVACY GDPR

Emissione Anno 2022

(da riemettersi entro fine anno solare successivo)

Redatto ed applicato ai sensi e per gli effetti di:
Reg.UE 2016/679 – GDPR – General Data Protection Regulation
D.Lgs.196/2003, così come modificato ed integrato da D.Lgs.101/2018

DOCUMENTO DI PRESIDIO E VERIFICA PERIODICA DEL SISTEMA DI CONFORMITA' PRIVACY GDPR,
PREDISPOSTO IN RIFERIMENTO AL CRITERIO DELL'ACCOUNTABILITY, SANCITO DALL'ART.5, COMMA2 DEL REG.UE 2016/679

REDATTO ED AGGIORNATO DAL RESPONSABILE DELLA PROTEZIONE DEI DATI:

GALLI DATA SERVICE SRL
Strada della Viggioletta, 8
29121 Piacenza
C.F. e P.I. 01690860331

SOMMARIO

ALLEGATI E FORMAT:

1) PRINCIPI GENERALI IN MATERIA DI PROTEZIONE DEI DATI

1.1) Il diritto fondamentale alla protezione dei dati

La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un **diritto fondamentale**. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che **ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano**.

Sulla base di tale principio l'Unione Europea ha ritenuto di emanare uno specifico Regolamento (**GDPR**), contenente i principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali finalizzato a garantirne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza. Il GDPR è inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche.

1.2) I principi generali in materia di privacy

Il Fondazione Val Tidone Musica garantisce l'applicazione dei principi fondamentali della privacy, sanciti dal GDPR ed identificati nella seguente tabella.

PRINCIPIO E RIF. LEGGE	DESCRIZIONE
LICEITÀ, CORRETTEZZA E TRASPARENZA (GDPR, Art.5, c.1, l.a)	Ogni trattamento di dati è legittimato da specifici requisiti di liceità, tra quelli espressamente previsti dall'Art.6, comma1 del GDPR. In generale il requisito di liceità dei trattamenti effettuati dal Fondazione Val Tidone Musica è da rinvenirsi nella lettera e) del suddetto articolo, ossia "*il trattamento è necessario per l'**esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri** di cui è investito il titolare del trattamento*" Risulta altresì possibile effettuare trattamenti fondati sugli ulteriori principi di liceità, ossia un consenso espresso dell'interessato, un obbligo di legge, un contratto tra le parti, la salvaguardia di un interesse vitale dell'interessato, un interesse legittimo del titolare. Nell'ambito delle politiche contro la corruzione, **la trasparenza delle pubbliche amministrazioni** assume un ruolo centrale. A tale proposito il Fondazione Val Tidone Musica recepisce ed applica le varie fonti di diritto in materia di trasparenza: • L.241/1990 "Norme sul procedimento amministrativo"; • D.Lgs.267/200 TUEL "Testo unico delle leggi sull'ordinamento degli enti locali"; • D.P.R. 184/2006 "Regolamento recante disciplina in materia di accesso ai documenti amministrativi"; • L.190/2012 "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione"; • D.Lgs.33/2013 "Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni"; • D.L. 34/2019, recante misure in materia di crescita, che ha introdotto alcune disposizioni sulla trasparenza dei contributi pubblici. Le prescrizioni di trasparenza e pubblicità derivanti dalle suddette fonti normative sono costantemente bilanciate con il diritto alla protezione dei dati personali, sulla base delle indicazioni e linee guida dell'Autorità per la protezione dei dati personali: **"Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati"** *(pubblicate in Gazzetta Ufficiale N°134 del 12/06/2014)*

PRINCIPIO E RIF. LEGGE	DESCRIZIONE
FINALITÀ' (GDPR, Art.5, c.1, l.b)	I dati personali sono raccolti e trattati solo per finalità predeterminate, esplicite e legittime. In generale il Fondazione Val Tidone Musica effettua trattamenti di dati personali esclusivamente nell'ambito del **perseguimento delle proprie finalità statutarie e delle funzioni attribuite, conferite o delegate dallo Stato o dalla Regione**, tra cui: • esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (es: servizi sociali, assetto ed utilizzazione del territorio, sviluppo economico, sicurezza, ...) • adempimento di un obbligo legale al quale è soggetto l'Ente (es: normativa sulla trasparenza) • esecuzione di un contratto con soggetti interessati (es: gestione fornitori, gestione gare ed appalti, …) • specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento
NECESSITÀ', NON ECCEDENZA, ESSENZIALITÀ (GDPR, Art.5, c.1, l.c)	L'utilizzo dei dati personali è sempre ridotto al minimo necessario essenziale per il raggiungimento delle finalità dichiarate; i dati personali sono raccolti e trattati solo se funzionali al raggiungimento delle finalità dichiarate; i dati personali sono trattati con modalità e strumenti proporzionali alle finalità da raggiungere. L'Ente può trattare **categorie particolari di dati personali** (GDPR, Art.9) nell'ambito delle materie di cui all'Art.2-sexies del D.Lgs.196/2003 (come modificato ed integrato dal D.Lgs.101/2018), tra cui si citano a titolo esemplificativo, non esaustivo: accesso a documenti amministrativi e accesso civico, tenuta degli atti e dei registri dello stato civile, delle anagrafi e delle liste elettorali, rilascio documenti di riconoscimento, cambiamento delle generalità, tenuta pubblici registri relativi a beni immobili, cittadinanza, immigrazione, asilo, ecc. Particolare attenzione è posta nel contenuto degli **atti amministrativi contenenti dati personali**: • in caso di dati comuni occorre attenersi al principio della minimizzazione (omettendo dati non necessari al contesto dell'atto) • in caso di dati particolari occorre procedere alla completa oscurazione
ESATTEZZA, COMPLETEZZA, AGGIORNAMENTO (GDPR, Art.5, c.1, l.d)	I dati personali sono puntualmente verificati, in modo che sia garantita la loro esattezza, completezza ed aggiornamento
CONSERVAZIONE (GDPR, Art.5, c.1, l.e)	I dati personali sono conservati per un periodo di tempo limitato al raggiungimento delle finalità dichiarate. In conformità alle proprie funzioni istituzionali il Fondazione Val Tidone Musica è tenuto al rispetto delle vigenti normative in materia di conservazione della documentazione amministrativa ed alla eventuale storicizzazione in appositi archivi, anche per esercitare il proprio diritto di difesa in ordine ad eventuali contenziosi sull'attività istituzionale.
SICUREZZA E RISERVATEZZA (GDPR, Art.5, c.1, l.f)	I dati sono sempre raccolti e trattati previa adozione di idonee misure di sicurezza tecniche ed organizzative. I dati sono trattati da soggetti adeguatamente identificati, autorizzati ed istruiti

SCOPO DOCUMENTATIVO: Il presente documento e relativi allegati, riportano adeguate e complete evidenze in merito ai suddetti principi generali, ottemperando al requisito di Accountability previsto dall'Art.5, comma 2 del GDPR ***("il Titolare è competente per il rispetto dei principi generali in materia di privacy ed in grado di comprovarlo")***

SCOPO ORIENTATIVO Il presente documento definisce le linee guida generali da implementare, aggiornare e rispettare per garantire il pieno rispetto dei requisiti normativi in materia di privacy.

2) RIFERIMENTI NORMATIVI E DEFINIZIONI

2.1) Riferimenti normativi

Il Modello di conformità privacy è implementato in relazione ai requisiti delle seguenti norme, comunitarie e nazionali:

- Regolamento UE 2016/679 "**General Data Protection Regulation**";
- D.Lgs.196/2003 "Codice Privacy", come modificato ed integrato da D.Lgs.101/2018.

Allo stato attuale, mediante l'implementazione del presente Modello, il Fondazione Val Tidone Musica **recepisce inoltre i profili di norma (provvedimenti / integrazioni / linee guida / interpretazioni) emanati dalle Autorità competenti a seguito dell'entrata in vigore del GDPR**, di seguito classificate:

ANNO	PROFILO DI NORMA	AUTORITA'	RECEPIMENTO (se applicabile)
2021	Provvedimento 10/06/2021 "Linee guida **cookie** e altri strumenti di tracciamento" *(nuovo banner in relazione all'eventuale utilizzo di cookies di profilazione)*	Garante Italiano	*Adeguamento sito web in relazione alle prescrizioni normative*
2021	Vademecum "Suggerimenti per creare e gestire **password** a prova di privacy"	Garante Italiano	*Verifica coerenza delle proprie impostazioni rispetto ai suggerimenti dell'Autorità*
2021	Normativa **Green-Pass** e relativi pareri Autorità Garante *(DL 52 del 22/04/2021 "Misure urgenti per la graduale ripresa delle attività economiche e sociali nel rispetto delle esigenze di contenimento della diffusione dell'epidemia da COVID-19" e successive modifiche ed integrazioni)*	Governo Italiano; Garante Italiano	*Introduzione di procedure, modalità e strumenti di verifica coerenti con le prescrizioni di legge e con le relative pronunce del Garante*
2021	Linee di indirizzo del Garante Privacy sull'attività degli **RPD/DPO** *Faq sul Responsabile della Protezione dei Dati (RPD/DPO) in ambito privato*	Garante Italiano	*Verificata applicabilità e coerenza delle linee guida al contesto dell'Ente*
2021	**Vaccinazioni sul luogo di lavoro** e ruolo del medico competente *(documento di indirizzo per il trattamento dei dati connessi all'adesione alla campagna vaccinale sui luoghi di lavoro – Protocollo nazionale 06/04/2021)*	Governo Italiano; Garante Italiano	*Valutata possibilità di adesione e (nel caso) applicate le misure*
2021	**Vaccinazioni dei dipendenti:** le FAQ del Garante Privacy *(indicazioni e principi generali per una corretta applicazione della disciplina sulla protezione dei dati)*	Garante Italiano	*Verificate ed applicate (se necessario) le indicazioni*
2021	Pareri congiunti su nuove **Clausole Contrattuali Tipo** proposte dalla Commissione Europea da parte *(aggiornamento delle clausole da utilizzarsi al fine di legittimare trasferimenti di dati extra UE e delle clausole da utilizzarsi per i contratti tra Titolari e Responsabili del trattamento)*	EDPB[(1)]; EDPS[(2)]	*Verificata applicabilità dei pareri e coerenza del proprio sistema di compliance*
2020	**Data Breach** *(nuovo servizio del Garante per supportare i titolari del trattamento negli adempimenti previsti in caso di Data Breach; modello di notifica al Garante e procedura di auto-valutazione che aiuta il titolare nell'assolvimento degli obblighi in materia di Notifica di una violazione dei dati personali all'autorità di controllo e di Comunicazione di una violazione dei dati personali all'interessato – 23 dicembre 2020).*	Garante Italiano	*Verifica della coerenza tra le indicazioni fornite dal Garante e la procedura interna di cui al Capitolo 7 del presente Modello e moduli allegati)*

ANNO	PROFILO DI NORMA	AUTORITA'	RECEPIMENTO (se applicabile)
2020	**Siti web e cookies** *(Avviso relativo alla consultazione sulle "Linee guida sull'utilizzo di cookie e di altri strumenti di tracciamento" - 10 dicembre 2020)*	Garante Italiano	*Verifica della coerenza del proprio sito web e relativa privacy policy con le indicazioni del Garante (eventuali ulteriori valutazioni a seguito del termine della consultazione ed eventuale entrata in vigore del regolamento e-Privacy Europeo)*
2020	**Videosorveglianza** *(le indicazioni del Garante privacy: le regole per installare ed utilizzare telecamere – 05 dicembre 2020)*	Garante Italiano	*Verifica della coerenza dei sistemi di videosorveglianza con le indicazioni del Garante (vedi registro trattamenti ed eventuali allegati dedicati)*
2020	**Fatturazione elettronica** *(Parere sullo schema di provvedimento del Direttore dell'Agenzia delle entrate concernente Regole tecniche per l'emissione e la ricezione delle fatture elettroniche per le cessioni di beni e le prestazioni di servizi effettuate tra soggetti residenti e stabiliti nel territorio dello Stato e per le relative variazioni - 9 luglio 2020)*	Garante Italiano	*Adozione di strumenti coerenti con gli obblighi di legge e procedure di compilazione adeguate rispetto ai criteri di pertinenza e minimizzazione dei dati*
2020	**Emergenza Coronavirus** *(indicazioni del Garante privacy su scuola, lavoro, sanità, ricerca ed enti locali. Chiarimenti e indicazioni per pubbliche amministrazioni e imprese private – 4 maggio 2020)*	Garante Italiano	*Adeguate le procedure di sicurezza alle indicazioni dei protocolli nazionali e dei dpcm applicabili (vedi registro trattamenti)*
2020	**Flussi di dati extra-UE Linee guida 2/2020 e raccomandazioni** *(il Comitato europeo per la protezione dei dati ha adottato raccomandazioni sulle misure che integrano gli strumenti di trasferimento dei dati per garantire il rispetto del livello UE di protezione dei dati personali, nonché raccomandazioni sulle cosiddette "garanzie essenziali europee" in rapporto alle misure di sorveglianza).*	EDPB	*Verifica di eventuali trasferimenti di dati extra UE e del relativo principio di legittimità (vedi registro trattamenti)*
2020	**Linee guida 5/2020 Consenso** *(indicazioni per acquisizione di un consenso valido)*	EDPB	*Verifica modalità e casistiche di acquisizione consenso (vedi informative allegate e registro trattamenti)*
2020	**Linee guida 3,4/2020 Emergenza sanitaria** *(trattamento dei dati relativi alla salute a fini di ricerca scientifica nel contesto dell'emergenza legata al COVID-19; uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19)*	EDPB	*Adeguate le procedure di sicurezza alle indicazioni dei protocolli nazionali e dei dpcm applicabili (vedi registro trattamenti)*
2019	Linee guida 2/2019 "trattamento dei dati personali nel contesto della fornitura di servizi on-line"	EDPB	*Verificata eventuale presenza on-line e connesse valutazioni su informativa e registro trattamenti*
2019	Raccomandazione 1/2019 "trattamenti soggetti all'obbligo di valutazione di impatto privacy"	EDPB	*Verificato registro trattamenti, in riferimento ai 9 criteri relativi alla PIA*
2019	Linee guida 3/2019 "trattamento dei dati tramite sistemi di videosorveglianza"	EDPB	*Verificata applicabilità e coerenza con i requisiti richiesti*
2019	Linee guida 4/2019 "criteri di valutazione della Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita"	EDPB	*Verificate attività censite nel registro dei trattamenti*

ANNO	PROFILO DI NORMA	AUTORITA'	RECEPIMENTO (se applicabile)
2019	Linee giuda 5/2019 "criteri di garanzia di esercizio del diritto all'oblio"	EDPB	*Verifica presenza di apposita modulistica per gestione delle richieste*
2019	Linee guida WP29 sulla gestione del consenso	WP Art.29 (3)	*Verificati trattamenti svolti sotto il principio di legittimità del consenso*
2019	Linee guida WP29 sulla gestione data breach	WP Art.29	*Verifica presenza di apposita modulistica per gestione violazioni dati personali*
2019	Linee guida WP29 sul registro dei trattamenti	WP Art.29	*Verificata presenza registro trattamenti*
2019	Tutorial del Garante sulla "individuazione e gestione del rischio"	Garante Italiano	*Verificata procedura e assegnazione rating*

(1) European Data Protection Board (Comitato della Autorità Garanti nazionali)

(2) European Data Protection Supervisor (Garante Europeo per la protezione dei dati)

(3) Working Party Art.29 (Gruppo di lavoro privacy europeo)

2.2) Definizioni

1) «**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;

2) **«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;

3) «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) «**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;

5) «**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;

6) «**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;

7) «**titolare del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

8) «**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;

9) «**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;

10) «**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;

11) «**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;

12) «**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;

13) «**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;

14) «**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;

15) «**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;

16) «**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;

17) «**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;

18) «**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;

19) «**gruppo imprenditoriale**»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

20) «**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;

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

22) «**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;

23) «**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;

24) «**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;

25) «**servizio della società dell'informazione**»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;

26) «**organizzazione internazionale**»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

3) METODOLOGIA DI GESTIONE DELLA COMPLIANCE

L'obiettivo del presente sistema è definire e monitorare le procedure operative necessarie al corretto recepimento ed implementazione delle vigenti normative in materia di privacy e data protection (Regolamento Europeo 2016/679 "General Data Protection Regulation", di seguito anche GDPR e D.Lgs.196/2003 così come modificato ed integrato dal D.Lgs.101/2018).

In sostanza il Fondazione Val Tidone Musica attraverso l'implementazione ed attuazione del presente Modello, recepisce i requisiti di conformità previsti dal GDPR, nonché dai provvedimenti nazionali dell'Autorità Garante per la protezione dei dati, fatti espressamente salvi dal decreto di armonizzazione (D.Lgs.101/2018 Art.22, comma4 "*4. A decorrere dal 25 maggio 2018, i provvedimenti del Garante per la protezione dei dati personali continuano ad applicarsi, in quanto compatibili con il suddetto regolamento e con le disposizioni del presente decreto*").

Il presente Modello è strutturato in capitoli corrispondenti ai requisiti di conformità, di seguito schematizzati.

REQUISITO	RIF.GDPR	EVIDENZA NEL MANUALE	ALLEGATI
Definire il perimetro di applicazione e gli elementi essenziali del contesto	Art.2,3,6,24, 25, 32, 35	**Capitolo 4** CONTESTO	
Definire ruoli e responsabilità dei soggetti coinvolti nel sistema	Art.26-29	**Capitolo 5** ORGANIGRAMMA	• Elenchi ed atti di nomina dei vari soggetti
Mappare le attività di trattamento, valutando i rischi per gli interessati ed il relativo piano di sicurezza	Art.30-32	**Capitoli 6,7,8** ACCOUNTABILITY	• Registro trattamenti • Piano sicurezza
Gestire eventuali incidenti di sicurezza	Art.33,34	**Capitolo 9** DATA BREACH	• Data breach
Divulgare adeguate informazioni agli interessati	Art.12-14	**Capitolo 10** INFORMATIVE	• Modelli di informativa
Garantire i diritti degli interessati	Art.15-22	**Capitolo 11** DIRITTI DEGLI INTERESSATI	• Moduli di gestione delle richieste di esercizio dei diritti
Gestire la verifica e l'aggiornamento del sistema	Art.24	**Capitolo 12** VERIFICA ED AGGIORNAMENTO DEL SISTEMA CONFORMITA'	

4) ANALISI DI CONTESTO

Il presente capitolo classifica gli **elementi significativi, dal punto di vista del trattamento di dati personali, del contesto in cui opera il Titolare.**

4.1 Finalità dell'analisi di contesto

L'analisi di contesto persegue un duplice obiettivo:

A. Ottemperare a **specifici obblighi** normativi

(vedi seguenti articoli di legge che richiedono esplicitamente una preventiva analisi di contesto)

Art. 6, comma 4, lettera c) "Liceità del trattamento"	*[…] 4. Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro:* *a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;* *b) del **contesto** in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento; […]*
Art. 24, comma 1 "Responsabilità del titolare del trattamento"	*[…] 1. 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 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. […]*
Art. 25, comma 1 "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita"	*[…] 1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché 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. […]*
Art. 32, comma 1 "Sicurezza del trattamento"	*[…] 1. 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, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio […]*
Art. 35, comma 1 "Valutazione d'impatto sulla protezione dei dati"	*[…] 1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il **contesto** e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi […]*
Art. 39, comma 2 "Compiti del responsabile della protezione dei dati"	*[…] Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del **contesto** e delle finalità del medesimo […]*

B. Personalizzare **la classificazione dei trattamenti e la valutazione dei rischi** sulla base delle peculiarità dell'ente

Il GDPR pone con forza l'accento sulla "responsabilizzazione" del Titolare, ossia sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento. Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di **decidere autonomamente**, in relazione alle proprie peculiarità, le modalità, le garanzie e i limiti del trattamento dei dati personali. Tale valutazione deve essere basata su una **stima del rischio** (che impatta sui diritti e le libertà fondamentali delle persone) connesso alle attività di trattamento e analizzato attraverso un'apposita metodologia (risk-assessment). A tale proposito si ritiene di prendere a riferimento la **norma UNI ISO 31000:2010** che prevede la "**Comprensione dell'organizzazione e del suo contesto" quale primo elemento di progettazione del sistema.**

4.2 Definizione del contesto, elementi caratterizzanti ed evidenze

In relazione alla struttura dell'ente vengono analizzati i seguenti elementi caratterizzanti:

Informazioni generali	• Regione • Provincia • Zona • Codice fiscale • Cap • Prefisso telefonico • Sito internet

Organizzazione	• Classificazione dell'ente in funzioni / servizi / uffici, al fine di identificare aree omogenee di classificazione del registro dei trattamenti

Infrastruttura tecnologica	Elementi significativi correlati agli asset hw/sw tecnologici utilizzati nel trattamento: • censimento server/computer • censimento principali applicativi in uso

INFORMAZIONI GENERALI
La seguente tabella riporta una sintetica classificazione dei dati anagrafici della Fondazione, al fine di contestualizzare indicativamente l'ordine di grandezza delle variabili che possono influire sul concetto di trattamento su larga scala.

Ente	**Fondazione Val Tidone Musica**
Regione	Emilia Romagna
Provincia	Piacenza
Zona	Italia Nord Occidentale
Codice fiscale	91092480333
Sito internet	www.valtidone-competitions.com

ORGANIZZAZIONE
La seguente tabella riporta una classificazione delle aree organizzative della Fondazione, al fine di contestualizzare le analisi necessarie alla predisposizione del registro dei trattamenti e le nomine dei soggetti autorizzati.
I dati sono trattati dalla sezione "Amministrazione Trasparente", istituita dal D.Lgs.33/2013 e consultabile sulla sezione "Amministrazione Trasparente" del sito web istituzionale della Fondazione.

ORGANIZZAZIONE/ARTICOLAZIONE UFFICI

Sono Organi della Fondazione:

- **l'Assemblea Generale**, come di seguito rappresentata:
FORNASARI GIANPAOLO – Presidente
TRAVERSONE SIMONA
BURZI MARCO
ZANGRANDI FILIPPO
CESARIO WENDALINA
CALZA PATRIZIA
GATTONI GINEVRA
BAROCELLI ROBERTINO
CATTIVELLI ROMINA
CAVALLI BENEDETTA
JANUSZEWSKI ELAINE JEANNE
GALVANI PAOLA
CARRA' ANNA MARIA
BRACCHI NICOLETTA
INTROZZI GIANLUCA

- **il Consiglio di Amministrazione**, come di seguito rappresentato:
FORNASARI GIANPAOLO – Presidente
RONCONI DONATELLA – Vicepresidente
BAROCELLI ANDREA – Consigliere
SQUERI ALBERTO – Consigliere
FERRARI CLAUDIA – Consigliere
FONTANA LUCIA – Consigliere

- **il Presidente**;

- **il Revisore dei Conti**.

Consulenti, collaboratori e Responsabili di procedimento:

- **Direttore artistico** – Livio Luigi BOLLANI;
- **Responsabile Trasparenza** – Segretario Comunale: Dott.ssa Laura CASSI;
- **Responsabile Anticorruzione** - Segretario Comunale: Dott.ssa Laura CASSI;
- **Responsabili del procedimento**:
  Dott.ssa Laura CASSI – Segretario Comunale;
  Rag. Orietta AGUERITI – Resp. Finanziario;
  Rag. Orietta AGUERITI – Resp. Segreteria.

INFRASTRUTTURA TECNOLOGICA

La classificazione degli asset significativi dell'infrastruttura tecnologica e degli archivi cartacei rappresenta un punto di riferimento per la declinazione del principio dell'accountability, risultando propedeutica al registro dei trattamenti – analisi dei rischi – contromisure.

SINTESI DELLE ATTIVITA' DI TRATTAMENTO

AREA AMMINISTRATIVO/CONTABILE	**AREA ARTISTICO/OPERATIVA**
(Attività relative alla gestione dei dati relativi all'aspetto amministrativo, contabile ed organizzativo della Fondazione, anche in adempimento degli obblighi di legge).	(Attività relative alla gestione dei dati relativi all'aspetto operativo di organizzazione di concerti, manifestazioni ed eventi rientranti negli scopi statutari della Fondazione).
Infrastruttura Tecnologica	**Infrastruttura Tecnologica**
L'infrastruttura informatica in uso fa capo al Comune di Sarmato, pertanto le misure minime di sicurezza informatica sono le medesime adottate dal predetto Ente e garantiscono il rispetto della normativa sul Disaster Recovery, le copie di backup, e il rispetto della normativa europea della privacy.	Il Direttore Artistico utilizza il proprio device ed è dotato di autonomo Piano di sicurezza informatico.

5) RUOLI E RESPONSABILITÀ PREVISTI DALLA NORMATIVA

Scopo del presente capitolo è **orientare la distribuzione dei compiti e delle responsabilità** nell'ambito dei soggetti preposti al trattamento dei dati.

Definizioni ed identificazione

TITOLARE DEL TRATTAMENTO (GDPR - Art.4, comma 7)

Titolare del trattamento, ai sensi della definizione di cui all'Art.4, comma 7 del GDPR, è lo scrivente Ente, in persona del Presidente pro-tempore.

RUOLO	ESTREMI IDENTIFICATIVI SOGGETTO
Fondazione Val Tidone Musica, in persona del Presidente pro-tempore	**Gianpaolo FORNASARI**

Modalità di designazione:
Delibera n. 13/2020

DATA PROTECTION OFFICER (GDPR – Art.37, 38, 39)

IDENTIFICAZIONE	
Tipo di nomina	◉ Persona Giuridica ◎ Persona Fisica
Estremi	Galli Data Service Srl
Persona di riferimento	◎ Singolo: ◉ Staff: Dott. Gregorio Galli, Avv. Groppi Valentina
Dati di contatto	IND: Strada della Viggioletta, 8 – 29121 Piacenza TEL: 0523.1865049 EMAIL: dpo@gallidataservice.com PEC: gallidataservicesrl@pec.it
Atto di designazione	Deliberazione N° 10/2021 del 28/04/2021
Pubblicazione riferimenti	◉ Sito internet dell'Ente ◎ Organigramma ◎ Altro

PERSONE AUTORIZZATE AL TRATTAMENTO (GDPR – Art. 29)

Nell'ambito dell'autonomia decisionale, espressamente prevista dall'Art.2-quaterdecies in funzione della complessità organizzativa dell'Ente, la Fondazione Val Tidone Musica stabilisce di definire un'**organizzazione gerarchica dei soggetti autorizzati**, al trattamento, con differenti compiti e funzioni:

- Responsabili del procedimento;
- Direttore Artistico;
- Revisore dei conti;
- organi politici (Assemblea Generale e Consiglio di Amministrazione).

RESPONSABILI ESTERNI DEL TRATTAMENTO (GDPR – Art. 4, comma 8 e Art.28)

In relazione alle definizioni normative si nominano Responsabili del trattamento le **organizzazioni esterne che effettuano un trattamento per conto del Titolare.**

E' cura della Fondazione inserire un'apposita clausola di rispetto delle vigenti normative un materia di privacy nei bandi di gara, in modo da selezionare partecipanti che garantiscano il rispetto delle vigenti normative e che si impegnino (in caso di aggiudicazione di incarichi che comportino un trattamento di dati personali) a sottoscrivere la designazione a responsabile esterno.

In apposita tabella, in uso ai settori, si classificano le organizzazioni che effettuano un trattamento di dati per conto della Fondazione, classificando:

- ragione sociale organizzazione (colonna SOGGETTO)
- tipo di incarico affidato (colonna ATTIVITA')
- modulo utilizzato per la designazione (colonna DOCUMENTO)

SOGGETTO	ATTIVITA'	DOCUMENTO
Dott. Pietro SALICE	Revisore dei Conti	◉ Modulo designazione della Fondazione ◎ Modulo designazione del soggetto esterno
Dott. Alberto TOSCANI	Commercialista	◉ Modulo designazione della Fondazione ◎ Modulo designazione del soggetto esterno

6) OBBLIGHI GENERALI DEL TITOLARE DEL TRATTAMENTO

Gli obblighi del Titolare del trattamento sono complessivamente definiti nel **Capo IV del GDPR** e sinteticamente riassunti nell'**Art.24**:

"1. 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 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.
2. 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."

Art.24 GDPR: Responsabilità del Titolare del trattamento

Il suddetto principio generale viene declinato in 3 fasi di compliance, secondo il seguente schema logico:

Il Titolare del trattamento è chiamato infine a effettuare specifiche valutazioni, nonchè implementare adeguate garanzie di tutela e protezione, nel caso di **trasferimento internazionale di dati**, verso Paesi non appartenenti alla Comunità Europea.

7) VALUTAZIONI PRELIMINARI ALLE ATTIVITÀ DI TRATTAMENTO

Al fine di poter dimostrare la conformità con il GDPR, il titolare del trattamento deve adottare politiche interne e attuare misure che soddisfino in particolare i principi della **protezione dei dati fin dalla progettazione** (Privacy by Design), della **protezione dei dati per impostazione predefinita** (Privacy by Default), nonché della **valutazione preliminare di impatto** (Privacy Impact Assessment).

Tali valutazioni sono effettuate:

- entro il 25 Maggio 2018 per i trattamenti già in essere (al fine di continuare lecitamente l'attività di trattamento ed inserire i dati nel registro dei trattamenti);
- in via antecedente all'inizio del trattamento per ogni futura attività.

7.1) Privacy by Design e Privacy by Default

La seguente tabella identifica le azioni effettuate al fine di garantire i requisiti di privacy fin dalla progettazione e privacy per impostazione predefinita:

- per i trattamenti già in essere (inseriti nei registri di cui al paragrafo successivo);
- per i futuri trattamenti;
- per i trattamenti connessi all'acquisto/utilizzo/sviluppo di software.

RIF. LEGGE	OBBLIGHI	ATTUAZIONE			CRITERI DI VALUTAZIONE
		Trattamenti inseriti nel registro	Nuovi trattamenti	Acquisto /utilizzo software	
Privacy by Design *Art.25, comma1*	*Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché 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.*	*In via preventiva all'inserimento dei trattamenti nel registro si è provveduto a verificare le misure di sicurezza*	*Attivato flusso informativo e scheda di valutazione*, al fine di presidiare nuovi trattamenti e verificarne la conformità prima dell'inizio*	*In via preventiva all'acquisto di software verranno privilegiate soluzioni già predisposte a garantire un adeguato livello di sicurezza*	• *Misure tecniche e organizzative adeguate* • *Pseudonimizzazione* • *Minimizzazione*
Privacy by Default *Art. 25, comma 2*	*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.*	*In via preventiva all'inserimento dei trattamenti nel registro si è provveduto a verificare la minimizzazione dell'utilizzo di dati, nonché la pertinenza*	*Attivato flusso informativo e scheda di valutazione*, al fine di presidiare nuovi trattamenti e verificarne la conformità prima dell'inizio*	*In via preventiva all'utilizzo di software verranno configurate modalità di utilizzo che prevedano la minimizzazione dell'utilizzo di dati, nonché la pertinenza*	• *Quantità di dati personali raccolti* • *Portata del trattamento* • *Periodo di conservazione* • *Accessibilità* • *Valutazione del life-cycle del dato*

7.2) Valutazione d'impatto sulla protezione dei dati (PIA, Privacy Impact Assessment)

Qualora, a seguito delle valutazioni di privacy by design e by default, emergano trattamenti che possono presentare un **rischio elevato** per i diritti e le libertà delle persone fisiche occorre effettuare una **valutazione di impatto sulla protezione dei dati** (Privacy Impact Assessment, Art. 35 GDPR) per determinare l'origine, la natura, la particolarità e la gravità di tale rischio.

All'esito di questa valutazione di impatto si deciderà in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento. Dunque, l'intervento delle autorità di controllo sarà principalmente "ex post", ossia si collocherà successivamente alle determinazioni assunte autonomamente dal titolare; ciò spiega l'abolizione a partire dal 25 maggio 2018 di alcuni istituti previsti dalla direttiva del 1995 e dal Codice italiano, come la notifica preventiva dei trattamenti all'autorità di controllo e il cosiddetto prior checking (o verifica preliminare: si veda art. 17 Codice), sostituiti da obblighi di tenuta di un registro dei trattamenti da parte del titolare/responsabile e, appunto, di effettuazione di valutazioni di impatto in piena autonomia. Peraltro, alle autorità di controllo, e in particolare al "Comitato europeo della protezione dei dati" spetterà un ruolo fondamentale al fine di garantire uniformità di approccio e fornire ausili interpretativi e analitici: il Comitato è chiamato, infatti, a produrre linee-guida e altri documenti di indirizzo su queste e altre tematiche connesse, ai quali il Titolare provvederà ad aggiornarsi.

ATTIVITA' DI TRATTAMENTO DA SOTTOPORRE A PIA

Il GDPR, all'interno dell'obbligo generale di condurre una PIA al ricorrere di un rischio elevato per gli interessati, fornisce alcune casistiche esemplificative (non esaustive) di trattamenti soggetti all'obbligo:

- una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o
- la sorveglianza sistematica su larga scala di una zona accessibile al pubblico;
- il ricorrere di 2 o più criteri tra quelli elencati nelle linee guida PIA del WP Art.29

ELEMENTI DI ANALISI CHE DEVE CONTENERE LA PIA

- descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
- valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- valutazione dei rischi per i diritti e le libertà degli interessati;
- misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

7.3) Evidenze sule valutazioni preliminari alle attività di trattamento

In relazione al processo di adeguamento al GDPR sviluppato dal Fondazione Val Tidone Musica, **tutte le attività in essere sono state analizzate secondo i requisiti di privacy by default, by design e PIA precedentemente elencati.**

GDPR-C2A-Registro trattamenti

Al fine di presidiare tali requisiti anche per i **futuri trattamenti**, il Titolare ha predisposto una **scheda di analisi** attraverso la quale verranno valutati i requisiti di conformità in via antecedente all'inizio del trattamento.

GDPR-C2B-Nuovo trattamento

8) IL PRINCIPIO DI ACCOUNTABILITY (RESPONSABILIZZAZIONE DEL TITOLARE)

Il GDPR pone con forza l'accento sulla "**responsabilizzazione**" (accountability nell'accezione inglese) del Titolare – ossia, sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento (Artt. 23-25, in particolare, e l'intero Capo IV del regolamento).

Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

Si richiede pertanto un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di **attività specifiche e dimostrabili (fasi del processo)**.

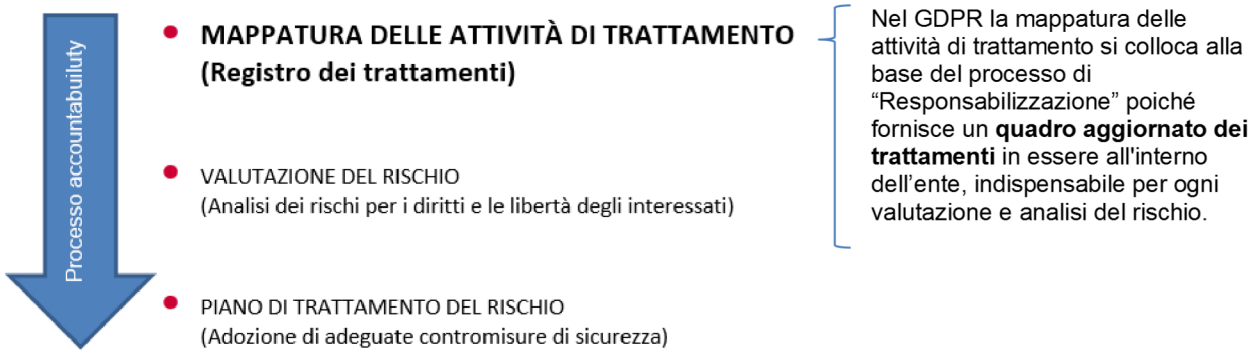
Di seguito una rappresentazione grafica delle **fasi del processo di accountability**:

Nei seguenti paragrafi verranno approfondite le 3 fasi, fornendo per ognuna:

- rappresentazione grafica e descrizione;
- riferimenti normativi;
- metodologia applicata.

8.1) Mappatura delle attività di trattamento

Rappresentazione grafica e descrizione



Riferimenti normativi

Art. 30 "Registri delle attività di trattamento"
1. 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.
3. I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.
4. 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.

Metodologia

I contenuti del registro sono chiaramente definiti dall'art.30 del GDPR sopra elencati, che possono essere integrati da ulteriori informazioni utili alla contestualizzazione delle attività di trattamento.

Il registro è strutturato secondo le indicazioni fornite in merito dall'Autorità Garante per la protezione dei dati personali:

Comunicato stampa Garante
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9047529

Pagina informativa Garante
https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento

Modello di registro Garante
https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento

GDPR-C2A-Registro trattamenti

8.2) Valutazione del rischio

Rappresentazione grafica e descrizione

- MAPPATURA DELLE ATTIVITÀ DI TRATTAMENTO
  (Registro dei trattamenti)
- **VALUTAZIONE DEL RISCHIO**
  (Analisi dei rischi per i diritti e le libertà degli interessati)
- PIANO DI TRATTAMENTO DEL RISCHIO
  (Adozione di adeguate contromisure di sicurezza)

Nel GDPR la fase di valutazione del rischio si colloca al centro del processo di "Responsabilizzazione". Tale analisi è propedeutica ad implementare adeguate misure di sicurezza organizzative e tecniche, secondo quanto richiesto dall'Art.32.

Riferimenti normativi

ARTICOLI GDPR in cui si riporta la necessità di effettuare un'analisi di rischio:

- *Art. 24 "Responsabilità del Titolare del trattamento"*
- *Art.25 "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (Privacy by Design e by Default)*
- *Art.32 "Sicurezza del trattamento"*
- *Art. 33 "Notifica di una violazione di dati personali" (Data Breach)*
- *Art.34 "Comunicazione di una violazione di dati personali"*
- *Art.35 "Valutazione d'impatto sulla protezione dei dati" (Privacy Impact Assessment)*
- *Art.36 "Consultazione preventiva"*

CONSIDERANDO GDPR:

- *Considerando 75 "I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati."*
- *Considerando 76 "La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato.*
- *Considerando 83 "Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale.*

L'attività di trattamento dati personali è considerata dal legislatore quale "attività rischiosa", poiché può comportare delle conseguenze negative nei confronti di coloro che hanno conferito tali dati. Pertanto, preliminarmente alla definizione della metodologia occorre focalizzare il **vero obiettivo dell'analisi di rischio** prevista dal GDPR, ossia l'impatto sui diritti e le libertà fondamentali delle persone fisiche. Il legislatore focalizza dunque il processo sull'interessato, invitando a sensibilizzare il Titolare sulle possibile conseguenze che i trattamenti effettuati possano generare sulle persone che hanno conferito tali dati (interessati).

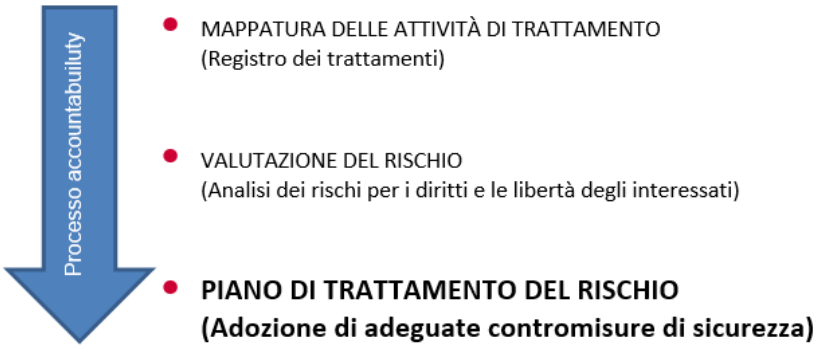
In particolare occorre identificare una **metodologia che definisca quale livello di rischio per gli interessati possa derivare da un evento dannoso quale distruzione accidentale o illegale, perdita, modifica, rivelazione o accesso non autorizzato**.

Evidenza sulla metodologia e sui risultati dell'analisi dei rischi:

📎 **GDPR-C2A-Registro trattamenti**

8.3 Piano di sicurezza

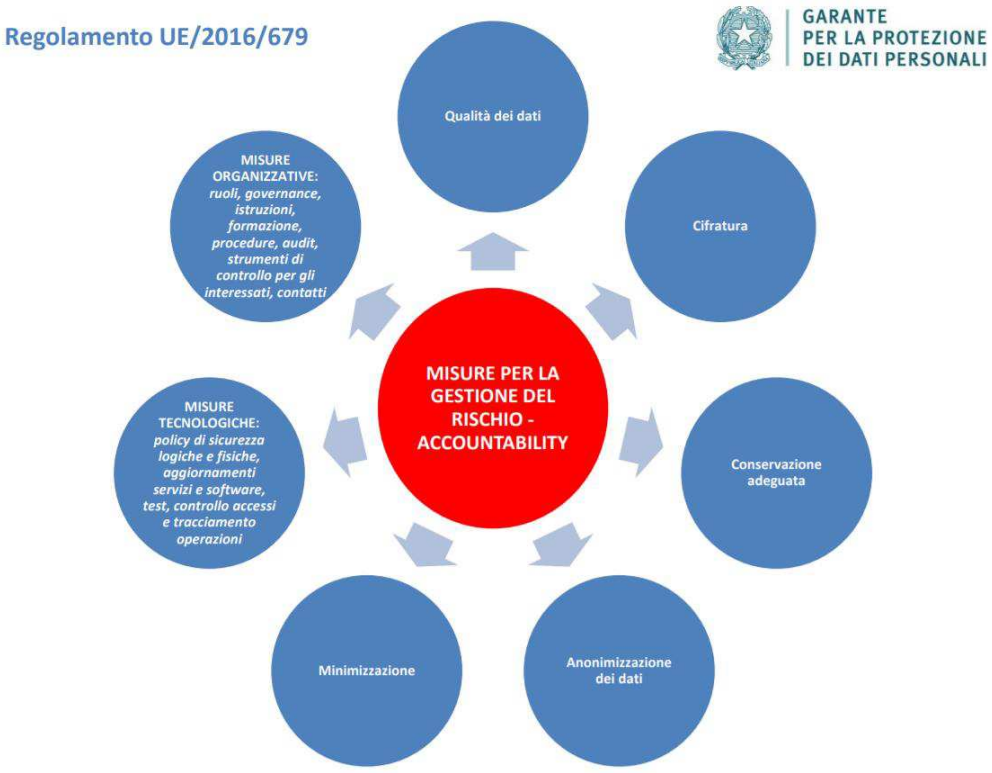
Rappresentazione grafica e descrizione



Nel GDPR l'implementazione di adeguate misure di sicurezza a tutela dei dati si colloca alla fine del processo di "responsabilizzazione". Le misure di sicurezza devono garantire un livello di sicurezza adeguato al rischio (art.32, par.1). Per tale motivo il GDPR fornisce una lista aperta non esaustiva. Per lo stesso motivo non possono sussistere dopo il 25/05/2018 obblighi generalizzati di adozione di "misure minime" di sicurezza, poiché tale valutazione è rimessa, caso per caso, al Titolare, in rapporto ai rischi specificatamente individuati.

Riferimenti normativi

Art. 32 "Sicurezza del trattamento"
1. 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, il titolare del trattamento mette 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.
Art.24 "Obblighi generali"
1. 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 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.



L'adozione di adeguate misure di sicurezza rappresenta, per le Pubbliche Amministrazioni, un preciso obbligo definito sulla base delle raccomandazioni dell'AgID (Agenzia per l'Italia digitale).

AgID ha il compito di definire raccomandazioni, strategie, norme tecniche per sensibilizzare e informare le amministrazioni sui temi della sicurezza informatica e delle emergenze ad essa collegate. AgID svolge un ruolo significativo nella tutela della sicurezza nazionale in ambito sicurezza cibernetica, la prevenzione e la gestione degli incidenti di sicurezza informatica nella pubblica amministrazione.

L'AgID ha fornito una classificazione delle **misure minime di sicurezza,** che rappresentano un importante supporto metodologico, oltre che un mezzo attraverso il quale le Amministrazioni, soprattutto quelle più piccole e che hanno meno possibilità di avvalersi di professionalità specifiche, possono verificare autonomamente la propria situazione e avviare un percorso di monitoraggio e miglioramento. Le misure minime:

- forniscono un riferimento operativo direttamente utilizzabile (checklist),
- stabiliscono una base comune di misure tecniche ed organizzative irrinunciabili;
- forniscono uno strumento utile a verificare lo stato di protezione contro le minacce informatiche e poter tracciare un percorso di miglioramento;
- responsabilizzano le Amministrazioni sulla necessità di migliorare e mantenere adeguato il proprio livello di protezione cibernetica.

L'adozione di adeguate misure tecniche e organizzative a tutela dei dati si basa pertanto sui controlli di sicurezza classificati dall'AgID, integrando eventualmente ulteriori profili di sicurezza organizzativa e fisica predisposti dall'Ente:

GDPR-C2C-Piano sicurezza

8.4 Trasferimento di dati extra UE

Il GDPR ha confermato l'approccio vigente in base alla direttiva 95/46 e al Codice italiano per quanto riguarda i **flussi di dati al di fuori dell'Unione europea** e dello spazio economico europeo, prevedendo che tali flussi sono vietati, in linea di principio, a meno che intervengano specifiche garanzie che il regolamento elenca in ordine gerarchico (GDPR, Capo V "Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali", con specifico riferimento agli art.44, 45, 46, 47, 49):

- adeguatezza del Paese terzo riconosciuta tramite decisione della Commissione europea;
- in assenza di decisioni di adeguatezza della Commissione, garanzie adeguate di natura contrattuale o pattizia che devono essere fornite dai titolari coinvolti (fra cui le norme vincolanti d'impresa - BCR, e clausole contrattuali modello);
- in assenza di ogni altro presupposto, utilizzo di deroghe al divieto di trasferimento applicabili in specifiche situazioni.

Evidenze sul trasferimento internazionale di dati

Per ogni attività censita nel registro dei trattamenti (Par.7.3), Fondazione Val Tidone Musica provvede a classificare l'ambito di eventuale trasferimento all'estero, identificando:

- Nessun trasferimento all'estero
- Trasferimento Intra UE
- Trasferimento Extra UE - Paesi adeguati
- Trasferimento Extra UE - Clausole contrattuali
- Trasferimento Extra UE - Norme vincolanti gruppo

Qualora si faccia riferimento a trasferimenti extra UE verranno specificati/allegati i riferimenti al requisito di legittimità individuato.

9) GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI (DATA BREACH)

IL GDPR prevede l'obbligo, per tutti i Titolari, di notificare all'autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (GDPR, considerando 85). Il Titolare provvede in ogni caso a documentare le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati.

9.1 La definizione e le tipologie di Data Breach

Si ha una "**violazione dei dati personali**" quando accidentalmente (colposamente) o in modo illecito (dolosamente) un evento causa la distruzione, la perdita, la modifica, la divulgazione non autorizzata, l'accesso ai dati personali trasmessi, conservati o comunque trattati. Nelle tabelle seguenti sono riportati alcuni esempi a cui è associato l'impatto prevalente sulle proprietà di sicurezza delle informazioni comunemente espresse in termini di Riservatezza (R), Integrità (I) e Disponibilità (D).

1. DISTRUZIONE:	**Indisponibilità irreversibile dei dati personali con appurata impossibilità di ripristino degli stessi**		
Accidentale	La distruzione dei dati personali può essere causata da un evento naturale al di fuori del controllo umano (allagamento, incendio, terremoto, ecc.) oppure da malfunzionamenti tecnici che provocano danni irreparabili alle infrastrutture informatiche oppure ai dati conservati nelle apparecchiature (server, PC, laptop dispositivi mobili, media, ecc.)		
Illecita	La distruzione dei dati personali può derivare da instabilità sociale (terrorismo, guerra, proteste ecc.) oppure da eventi deliberati (danneggiamento fisico o manomissione di infrastrutture informatiche, apparecchiature, ecc.)		
Proprietà di sicurezza	**R**	**I**	**D**

2. PERDITA:	**Smarrimento o sottrazione dei dati personali**		
Accidentale	La perdita dei dati personali può originare dallo smarrimento di apparecchiature (server, PC laptop, dispositivi mobili, media, ecc.), oppure dallo smaltimento non sicuro dei supporti di archiviazione dei dati (hard disk, media, ecc.), da un errori umani che compromettono la funzionalità del sistema corrompendo gli archivi di memorizzazione dei dati oppure che inavvertitamente effettuino una cancellazione sicura dei dati con appurata impossibilità di ripristino degli stessi		
Illecita	La perdita dei dati personali può essere determinata dal furto di apparecchiature (server, workstation, laptop, dispositivi mobili, media, ecc.), da eventi deliberati tesi alla cancellazione sicura dei dati con appurata impossibilità di ripristino degli stessi		
Proprietà di sicurezza	**R**	**I**	**D**

3. MODIFICA:	**Cambiamento di dati personali improprio o non autorizzato in grado di compromette la completezza e/o la correttezza delle informazioni**		
Accidentale	La modifica di dati personali può essere causata da errori umani in grado di apportare cambiamenti indesiderati alle informazioni contenuti in banche dati		
Illecita	La modifica di dati personali può derivare dall'azione di malware		
Proprietà di sicurezza	**R**	**I**	**D**

4. DIVULGAZIONE NON AUTORIZZATA:	**Rivelazione di dati personali a soggetti terzi determinati o indeterminati**		
Accidentale	La divulgazione non autorizzata dei dati personali è causata da un errore umano che espone impropriamente dati personali a terzi (es. invio via email di documenti a destinatari errati)		
Illecita	La divulgazione non autorizzata dei dati personali avviene deliberatamente da parte di criminali informatici che espongono le informazioni personali online a seguito di un accesso abusivo		
Proprietà di sicurezza	**R**	**I**	**D**

5. ACCESSO NON AUTORIZZATO	**Compimento di operazioni di trattamento da parte di soggetti non autorizzati**		
Accidentale	Errata configurazione dei sistemi che permette a soggetti non autorizzati di compiere operazioni sui dati		
Illecita	Attività di spionaggio attraverso l'uso di dispositivi hardware (es. keylogger) e software (intercettazione del traffico di rete, trojan, ecc.) Attacco alle applicazioni web per sfruttare vulnerabilità e ottenere l'accesso ai sistemi		
Proprietà di sicurezza	**R**	**I**	**D**

9.2 Gli obblighi previsti dal GDPR

Gli obblighi normativi associati a violazioni di dati personali sono riportati dagli artt. 33 e 34 del GDPR:

- documentare tutte le violazioni di dati personali
- effettuare una valutazione di rischio
- notificare l'evento all'Autorità di Controllo ed agli interessati

Tali obblighi sono espletati secondo la seguente procedura

FASE DEL PROCESSO	MODALITÀ ATTUATIVE
Rilevazione incidenti di sicurezza	Diffuse adeguate istruzioni e riferimenti a tutto il personale operativo, che è tenuto a segnalare al proprio responsabile di settore qualsiasi evento assimilabile alla definizione di data breach Sensibilizzati i referenti interni sulla necessità di comunicare gli eventi al DPO (o al coordinatore privacy interno se presente) Instaurato un canale comunicativo diretto tra DPO e referente informatico, al fine di presidiare tempestivamente eventi e rischi di sicurezza IT
Compilazione del registro	A cura del DPO, tramite allegato: **GDPR-C2D-Data breach**
Valutazione impatto di rischio	A cura del DPO, tramite allegato: **GDPR-C2D-Data breach / Procedura on-line**
Comunicazione dell'evento all'Autorità di controllo ed agli interessati	A cura del DPO, tramite allegato: **GDPR-C2D-Data breach / Procedura on-line**

10) GLI ATTI DI INFORMAZIONE (INFORMATIVE PRIVACY)

Già nel Codice della Privacy (D.Lgs. 196/2003) l'informativa all'interessato rappresentava uno degli adempimenti principali in capo al titolare del trattamento, sia esso un soggetto privato sia esso un soggetto pubblico.

Il GDPR prevede che vengano fornite all'interessato (soggetto che conferisce i propri dati alla Fondazione) le informazioni di cui all'Art.13 e 14:

- l'identità e i dati di contatto del titolare del trattamento e del responsabile della protezione dei dati;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili;
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
- qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- il diritto di proporre reclamo a un'autorità di controllo;
- se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
- 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.

La Fondazione, ai sensi dell'Art.12 del GDPR, deve adottare misure appropriate per fornire all'interessato tutte le suddette informazioni in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Il GDPR prevede che tali informazioni siano fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici.

In relazione alle suddette prescrizioni normative il Fondazione Val Tidone Musica provvede a:

- pubblicare un'informativa completa sul trattamento dei dati (**GDPR-C3A-Informativa generale sito**) per il complesso delle proprie finalità istituzionali e nei confronti dei vari soggetti interessati con cui si interfaccia (principalmente cittadini) sul sito internet www.valtidone-competitions.com;
- diffondere un'informativa semplificata, con link diretto al sito internet in cui trovare l'informativa completa, tramite il disclaimer di chiusura di tutte le email in uscita (**GDPR-C3B-Informative semplificate**);
- inserire un'informativa semplificata, con link al sito internet in cui trovare l'informativa completa, nella modulistica cartacea tramite cui si effettuano raccolte di dati personali (**GDPR-C3B-Informative semplificate**);
- diffondere ulteriori informative specifiche per specifici ambiti di trattamento (es: bandi di selezione personale, servizi bibliotecari, videosorveglianza, ecc.);
- consegnare singolarmente una specifica informativa a tutti i soggetti con cui intraprende un rapporto di lavoro, anche occasionale (**GDPR-C3C-Informativa addetti**);
- pubblicare sul sito internet gli estremi ed i dati di contatto estesi del Responsabile della protezione dei dati.

11) I DIRITTI DEGLI INTERESSATI

Il GDPR, per quanto concerne il tema dei "diritti" degli interessati al trattamento, presenta diversi elementi di continuità con il D.Lgs. 196/2003 e Direttiva 95/46/CE; il legislatore europeo ha tuttavia introdotto **nuove prerogative riconosciute agli interessati al trattamento**, tenendo in considerazione l'attuale sviluppo delle nuove tecnologie che potenzialmente possono determinare nuovi pericoli e rischi per i diritti e le libertà degli stessi. Di seguito viene riportata un'elencazione dei diritti degli interessati previsti dal GDPR (par.12.1), nonché le modalità attuative implementate dal Titolare per fornire un puntuale ed esaustivo riscontro ad eventuali richieste degli interessati (par. 12.2).

11.1) Classificazione dei diritti degli interessati

La seguente tabella riporta un elenco dei diritti degli interessati previsti dal GDPR, recepiti dal Titolare e garantiti secondo le modalità di cui al paragrafo successivo

Diritto	Descrizione
ART.15 **Diritto di accesso**	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. 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. 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. Il diritto di ottenere una copia di cui al paragrafo 3 non deve ledere i diritti e le libertà altrui.
ART.16 **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.
ART.17 **Diritto di cancellazione (oblio)**	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; 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. Esclusioni: i suddetti diritti 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	Descrizione
ART.18 **Diritto di limitazione**	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.
ART.20 **Diritto alla portabilità dei dati**	L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti 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. Nell'esercitare i propri diritti relativamente alla portabilità dei dati, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile. 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. Il diritto di cui alla portabilità non deve ledere i diritti e le libertà altrui.
ART.21 **Diritto di opposizione**	L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano 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. 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. Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità. 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. 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.
ART.22 **Processi decisionali automatizzati (profilazione)**	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. Il suddetto paragrafo 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.

11.2) Procedura (modalità e strumenti) per garantire adeguati riscontri agli interessati

Il seguente schema logico identifica il processo operativo, implementato dal Fondazione Val Tidone Musica, finalizzato a garantire l'attivazione di adeguata procedura per fornire puntuali riscontri ad eventuali richieste degli interessati. La seguente procedura si applica a specifiche richieste di esercizio dei diritti previsti dagli Art.15-21 del GDPR (elencati al paragrafo precedente) ma non a richieste di accesso ad atti in riferimento alle normative sulla trasparenza specifiche per le Pubbliche Amministrazioni.

FASE DEL PROCESSO	MODALITÀ ATTUATIVE
Sensibilizzare il personale nella corretta risposta ad eventuali richieste da parte degli interessati	Diffuse adeguate istruzioni e riferimenti a tutto il personale operativo, che è tenuto a segnalare al proprio responsabile di settore qualsiasi richiesta di esercizio dei diritti da parte degli interessati Sensibilizzati i referenti interni sulla necessità di comunicare le richieste al DPO (o al coordinatore privacy interno se presente)
Definire soggetti preposti a dare riscontri e pubblicarne i riferimenti ed i contatti	Soggetto preposto a gestire le richieste: [ ] Titolare [x] DPO [ ] Altro referente ……. Pubblicazione estremi e strumenti: [x] Pubblicazione on-line [ ] Inserimento informativa / contratti [ ] Inserimento in organigramma [ ] Email dedicata [ ] Numero dedicato
Definire la modulistica per effettuare le richieste e la modalità di identificazione dell'interessato	Il DPO inviterà gli interessati ad effettuare le richieste in forma scritta, anche elettronica, utilizzando l'apposita modulistica. All'interessato sarà richiesto di allegare alla domanda una copia di un documento di identità. 📎 **GDPR-C2E-Diritti interessati M1**
Definire modalità di valutazione delle richieste	Il DPO, in relazione al merito delle singole richieste, effettuerà le opportune valutazioni per definire se la richiesta sia: • da evadere gratuitamente • oggetto di necessari approfondimenti • da evadere con contributo economico • manifestamente infondata / eccessiva 📎 **GDPR-C2E-Diritti interessati M2**
Definire tempistiche	Il DPO, in relazione al merito delle singole richieste, effettuerà le opportune valutazioni per definire i tempi di risposta: • tempestivi (senza ingiustificato ritardo) • entro 30 gg • entro 60 gg (casi complessità) • comunicazione motivi ritardo 📎 **GDPR-C2E-Diritti interessati M2**
Definire strumenti attuativi delle richieste	Il DPO suggerirà/adotterà adeguati strumenti per agevolare la gestione delle richieste, tra cui: • organizzazione ordinata banche dati • definizione adeguati tempi retention • strumenti software dedicati
Definire modalità di riscontro agli interessati	Il DPO provvederà sempre a dare riscontro alla richieste degli interessati in forma scritta, utilizzando apposito modulo: 📎 **GDPR-C2E-Diritti interessati M3**

12) VALIDITA', VERIFICA ED AGGIORNAMENTO DEL MODELLO

Il presente documento supporta il Responsabile della Protezione dei dati personali del Fondazione Val Tidone Musica, nel suo ruolo di coordinamento e supervisione del sistema di compliance:

- certifica e documenta il sistema di conformità privacy GDPR del Fondazione Val Tidone Musica;
- viene emesso alla data indicata in intestazione, recependo il contesto normativo in vigore (classificato al paragrafo 2.1);
- ha validità fino alla sua riemissione, da effettuarsi entro il termine dell'anno solare successivo alla data di emissione.

GESTIONE DOCUMENTALE
La seguente tabella identifica le modalità di gestione del fascicolo documentale privacy

GESTIONE DOCUMENTALE	
Conservazione documenti	◉ Su piattaforma digitale sicura (Datacenter certificato ISO 27.001 e protocolli di trasmissione dati muniti di SSL) ◉ Presso sede Titolare in formato cartaceo ◎ Presso sede Titolare in formato elettronico
Validazione documenti	MODELLO ACCOUNTABILITY (presente documento) ◉ Sottoscrizione in formato cartaceo originale ◉ Validazione tramite tool digitale basato su casella email personale e riservata ALLEGATI Gli allegati, in quanto format documentali da utilizzarsi in caso di eventi particolari, sono validati automaticamente mediante il processo di validazione del modello. Nel caso in cui si procedesse alla compilazione i documenti compilati saranno conservati a sistema.
Validità del modello	Il presente modello è valido fino alla successiva riemissione, da effettuarsi entro il termine dell'anno successivo alla data del presente documento. Annualmente verrà infatti riemesso il modello al fine di aggiornarlo allo scenario normativo di riferimento ed alle variazioni nell'assetto organizzativo del Titolare (ottemperando altresì ai requisiti di verifica periodica previsti dal GDPR). I moduli allegati potranno essere confermati nella validità, previa valutazione dello scenario di legge.
Documentazione pregressa	Ai sensi delle significative novità introdotte dal GDPR il Titolare ha deciso di effettuare una revisione complessiva della compliance privacy, pertanto il presente modello e relativi allegati annullano e sostituiscono la documentazione precedentemente adottata
Divulgazione	Il presente documento è da intendersi ad uso interno del Titolare e non può essere riprodotto/riutilizzato, in tutto o in parte, per fini estranei alla compliance interna; nel rispetto di tale principio, il documento può essere esibito o consegnato in copia conforme esclusivamente a: componenti degli organi di controllo per le opportune verifiche; autorità preposte a verifiche ispettive. Il documento può essere condiviso inoltre con soggetti interni coinvolti nel sistema di conformità. Qualora venisse richiesta da soggetti esterni un'evidenza del sistema di conformità privacy GDPR potrà essere realizzata una versione "divulgativa" del Modello, mediante scorporazione dei contenuti specifici/riservati.

ATTIVITA' DI VERIFICA / AGGIORNAMENTO

Gli **obblighi di verifica periodica** del sistema di conformità privacy sono sanciti in particolare dai seguenti articoli del GDPR:

- Art.5, c2 "*Il titolare del trattamento è competente per il rispetto dei principi generali applicabili al trattamento ed **in grado di comprovarlo** ("Responsabilizzazione" o "Accountability")"*
- Art.24, c1 *"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**"*
- Art.32, c1(d) *"Il Titolare implementa una procedura per **testare, verificare e valutare regolarmente** l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento."*

Il DPO, nel suo ruolo di coordinamento e controllo, effettua le seguenti attività:

1) attività di verifica/aggiornamento **specifiche sui singoli settori**, da condursi con le PO di riferimento
2) attività di verifica/aggiornamento **generali**, da condursi con un coordinatore generale
3) redazione di **evidenze di verifica**, per documentare i controlli effettuati ed ottemperare ai requisiti di legge;
4) **supporto continuativo** in corso d'anno.

ATTIVITA' DI CONSULENZA (1): VERIFICHE DI SETTORE
Attività di verifica/aggiornamento **specifiche sui singoli settori**, da condursi con le PO di riferimento

DESCRIZIONE	RIF. LEGGE	DELIVERABLE DA VERIFICARE
Verifica **assegnazione ruoli e relativi atti di nomina** a tutti i soggetti coinvolti nel trattamento (personale lavorativo che opera presso il settore di riferimento)	Art.29	• Elenco soggetti autorizzati • Nomina soggetti autorizzati • Nomina posizioni organizzative
Verifica identificazione e designazione dei **responsabili esterni del trattamento** (consulenti/fornitori che forniscono servizi al settore, con accesso a dati)	Art.28	• Elenco resp.esterni • Nomina resp.esterni
Verifica **istruzioni agli autorizzati** (verifica sottoscrizione fascicolo)	Art.29	• Fasciolo scritto istruzioni
Attività di **formazione alle PO**	Art.29	• Attestato formazione
Verifica / aggiornamento del **registro trattamenti**	Art.32	• Registro dei trattamenti
Modalità: 1 incontro on-site con il referente interno **Frequenza:** Annuale		

ATTIVITA' DI CONSULENZA (2): VERIFICHE GENERALI
Attività di verifica/aggiornamento **generali**, da condursi con un coordinatore generale

DESCRIZIONE	RIF. LEGGE	DELIVERABLE
Verifica **piano di sicurezza** (misure tecniche ed organizzative a tutela dei dati), coordinato con piano Agid	Art.32	• Piano di sicurezza
Verifica **informative** (atti di informazione da predisporre in conformità all'art.13 del GDPR)	Art.13	• Pubblicazione estremi DPO • Informativa sito web • Informative dipendenti • Informative semplificale • Ulteriori informative (es: partecipazione a bandi, concorsi, ecc.)
Verifica procedura **data breach**	Art.33,34	• Registro Data Breach
Verifica procedura **diritti interessati** (coordinata con accesso ad atti e trasparenza)	Art.15-21	• Modulo di richiesta di esercizio • Modulo di valutazione • Modulo di risposta
Verifica **nomine generali**	Art.28,29	• Nomina organi politici
Modalità: 1 incontro on-site con coordinatore/i generale **Frequenza:** Annuale		

ATTIVITA' DI CONSULENZA (3): REDAZIONE DOCUMENTI
Aggiornamento del presente Modello, per documentare i controlli effettuati

DESCRIZIONE	RIF. LEGGE	DELIVERABLE
Aggiornamento del Modello in modo da certificare e documentare, secondo il principio dell'accountability, i controlli previsti per legge su: - elementi di contesto - ruoli e responsabilità - attività di trattamento - misure di sicurezza	Art. 5, 24, 32	• GDPR-C1-Modello di conformità
Modalità: Redazione in back-office da parte del DPO **Frequenza:** Annuale		

ATTIVITA' DI CONSULENZA (4): SUPPORTO CONTINUATIVO Supporto continuativo, in corso d'anno, per mantenimento conformità e gestione eventi	
DESCRIZIONE	**NOTE OPERATIVE**
Supporto informativo per eventuali **novità normative e giurisprudenziali**	Forniti tempestivi riscontri in caso di novità normative emanate da: - Garante nazionale per la protezione dei dati personali - Board Europeo (EDPB) - Associazioni competenti in materia di privacy - Sentenze e giurisprudenza di settore
Supporto consulenziale su eventuali documenti / modulistica privacy ricevuta da **soggetti esterni**	Forniti adeguati riscontri su eventuale documentazione privacy fornita all'Ente da soggetti esterni, principalmente in caso di richiesta firma
Supporto per esercizio **diritti interessati**	Fornito adeguato supporto per la gestione e compilazione modulistica in caso di richiesta di esercizio di diritti degli interessati
Supporto per **data breach**	Fornito adeguato supporto per la gestione e compilazione modulistica in caso di evento che possa compromettere la sicurezza dei dati (data breach)
Supporto su **richieste ed approfondimenti privacy**	Forniti adeguati riscontri su eventuali dubbi o richieste di chiarimenti su profili interni a rilevanza privacy
Attivazione **piattaforma documentale**	Fornita una piattaforma digitale web-based per agevolare il controllo del sistema di conformità ed i flussi di comunicazione tra referente privacy interno e DPO
Mantenimento **carica DPO**	Mantenimento della carica di DPO, in modo coerente con le prescrizioni di cui agli art. 37-39
Modalità: Supporto su richiesta o su evento **Frequenza:** Continuativa in corso d'anno	

ESITO DEI CONTROLLI E STATO DEL SISTEMA DI CONFORMITÀ

Il presente Modello, nonché le sue riemissioni annuali, fungono pertanto da verbale dei controlli effettuati, definendo la valutazione del sistema di conformità di cui alla seguente tabella.

VALUTAZIONE COMPLESSIVA DEL SISTEMA DI CONFORMITÀ	
	Il sistema di conformità di Fondazione Val Tidone Musica risulta: • completo a livello di documentazione; • effettivo ed aggiornato rispetto ai trattamenti effettuati; • compreso ed applicato dai soggetti preposti ai trattamenti; • attuato operativamente rispetto alle misure di sicurezza indicate.