REGOLAMENTO
DEL SISTEMA DI PROTEZIONE
DEI DATI PERSONALI



00	29/05/2025	**1^ Emissione**	**D.P.O.** Ing. Enrica Marsiglio	**Presidente** GIUSEPPE CARINCI
Rev.:	**Data**	**Descrizione**	**Emesso**	**Approvato**

Parte I - AMBITO DI APPLICAZIONE DEL REGOLAMENTO, DEFINIZIONI E CRITERI DEI TRATTAMENTI

Art.1 - Ambito di applicazione

1. Il presente regolamento disciplina il trattamento da parte del Conservatorio Statale di Musica "Antonio Buzzolla" di Adria (Ro) dei dati personali ai sensi e per gli effetti del D.Lgs. 30 giugno 2003, n.196 e del Regolamento UE 2016/679.
2. Esula dalla disciplina del presente regolamento il trattamento dei dati particolari e giudiziari.
3. L'insieme dei regolamenti, dei documenti, delle disposizioni, delle procedure, delle istruzioni e degli strumenti relativi all'applicazione del sopra citato Decreto legislativo costituisce il sistema di protezione dei dati personali del Conservatorio di Musica A". Buzzolla" di Adria (Ro) (d'ora in poi sistema di protezione dei dati personali).

Art.2 - Definizioni

1. Si recepiscono ai fini del presente regolamento le seguenti definizioni di legge:
"Codice", il D.Lgs. 30 giugno 2003, n.196;

"Regolamento", il Regolamento UE 2016/679 del 27 aprile 2016;

"Codice di deontologia", il Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici di cui alla G.U. n. 80 del 5 aprile 2001;

"trattamento", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

"dato personale", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

"dati identificativi", i dati personali che permettono l'identificazione diretta dell'interessato;

"dati particolari", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

"dati giudiziari", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi

pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

"titolare", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

"responsabile", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

"incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

"interessato", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

"comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

"diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

"dato anonimo", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

"blocco", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

"banca di dati", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

"Garante", l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n.675.

"misure minime", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;

"strumenti elettronici", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

"autenticazione informatica", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

"credenziali di autenticazione", i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

"parola chiave", componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;

"profilo di autorizzazione", l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

"sistema di autorizzazione", l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

Art.3 - Principio di necessità nel trattamento dei dati

1. I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

- adotta le necessarie misure di sicurezza e le ulteriori misure ritenute idonee alla salvaguardia dell'integrità, della riservatezza e della disponibilità dei dati;
- nomina il/i responsabile/i interno/i ed esterni dei trattamenti;
- nomina gli incaricati dei trattamenti, sempre che non affidi tale compito al/i responsabile/i interno/i dei trattamenti;
- approva i programmi di istruzione e formazione degli addetti;
- assume le decisioni relative agli investimenti necessari a garantire al sistema di protezione dei dati personali la conformità alla vigente normativa;
- vigila sulla osservanza delle leggi e delle disposizioni impartite, promuove almeno una volta all'anno la riunione per la verifica della correttezza del funzionamento del sistema di protezione dei dati personali e della gestione delle risorse e approva gli aggiornamenti e/o le correzioni necessarie del sistema medesimo.

Art.4 -Modalità del trattamento e requisiti dei dati

1. I dati personali oggetto di trattamento sono:
   A. trattati in modo lecito e secondo correttezza;
   B. raccolti e registrati per scopi determinati, espliciti e legittimi, e utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
   C. esatti e, se necessario, aggiornati;
   D. pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati;
   E. conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.
2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

Parte II - RESPONSABILITA'

Art.5 -Titolare

1 Il Conservatorio di Musica "A. Buzzolla" di Adria è titolare dei trattamenti dei dati personali, sia su supporti cartacei che mediante elaboratori elettronici, effettuati da essa o per conto della medesima.

2 L'approvazione dei documenti rilevanti ai fini dell'applicazione del Codice è demandata al Consiglio di Amministrazione.

3 Nell'ambito delle strutture e dei dipendenti del Titolare l'accesso ai dati personali ed il relativo trattamento sono consentiti esclusivamente ai soggetti nominati responsabili o incaricati.

Art.6 - Responsabilità del Titolare

1 Al Titolare competono I seguenti compiti e responsabilità:

- assume le decisioni in ordine alle finalità e alle modalità dei trattamenti dei dati;
- definisce e approva il Documento Programmatico sulla Sicurezza e ogni altro documento relativo al sistema di protezione dei dati personali;

adotta le necessarie misure di sicurezza e le ulteriori misure ritenute idonee alla salvaguardia dell'integrità, della riservatezza e della disponibilità dei dati;

- nomina il/i responsabile/i interno/i ed esterni dei trattamenti;
- nomina gli incaricati dei trattamenti, sempre che non affidi tale compito al/i responsabile/i interno/i dei trattamenti;
- approva i programmi di istruzione e formazione degli addetti;
- assume le decisioni relative agli investimenti necessari a garantire al sistema di protezione dei dati personali la conformità alla vigente normativa;
- vigila sulla osservanza delle leggi e delle disposizioni impartite, promuove almeno una volta all'anno la riunione per la verifica della correttezza del funzionamento del sistema di protezione dei dati personali e della gestione delle risorse e approva gli aggiornamenti e/o le correzioni necessarie del sistema medesimo, ivi incluso l'aggiornamento o revisione del Documento Programmatico della Sicurezza da effettuare entro il 31 marzo di ogni anno.

Art.7 - Responsabilità dei responsabili interni dei trattamenti

1. Il Titolare nomina il/i responsabile/i sulla base dei requisiti di esperienza, capacità e affidabilità indicati dal Codice e dal Regolamento. L'accettazione della nomina conferma il possesso dei requisiti di cui sopra.

2. Ogni responsabile del trattamento è incaricato dal Titolare di organizzare e coordinare l'attività degli incaricati e di vigilare sul fatto che essi operino nel rispetto della legge, nonché dei regolamenti, delle disposizioni, delle procedure e delle istruzioni del sistema di protezione dei dati personali.

3. In particolare, il Responsabile deve assicurare:

- la nomina degli incaricati, in quanto a ciò incaricato dal Titolare;
- che siano rilasciate le informative e acquisito il consenso degli interessati, laddove richiesto;
- che siano osservate le misure minime di sicurezza e le altre misure di sicurezza eventualmente adottate, relative ai trattamenti con strumenti elettronici e a quelli su supporti cartacei;
- che siano osservate le disposizioni relative all'esercizio dei diritti e quelle relative al riscontro agli interessati, che deve essere fornito entro 15 giorni dal ricevimento della richiesta dell'interessato. Se le operazioni necessarie per un integrale riscontro risultino di particolare complessità o ricorra altro giustificato motivo, entro il termine di cui sopra ne deve essere fornita comunicazione all'interessato e, in tal caso, il termine per l'integrale riscontro è di 30 giorni dal ricevimento della richiesta.

4. Il Responsabile è tenuto altresì a:

- riferire tempestivamente al Titolare le condizioni o le problematiche che siano suscettibili di rendere difficile o pregiudicare la gestione o l'espletamento delle attività nel rispetto della legge e delle disposizioni del sistema di protezione dei dati personali; ed, in particolare, qualsiasi elemento oggettivo o soggettivo che abbia compromesso o possa compromettere la sicurezza, la correttezza e la legittimità dei trattamenti in ambito informatico;
- partecipare alle riunioni convocate dal Titolare per: 1) la verifica periodica del funzionamento del sistema di protezione dei dati personali; 2) l'acquisizione e l'implementazione delle correzioni e/o degli aggiornamenti di tale sistema per l'applicazione della normativa e/o in ragione delle modifiche intervenute nell'organizzazione ovvero nelle procedure dell'ente;
- proporre i programmi di istruzione, formazione e aggiornamento degli incaricati, fornire loro ogni chiarimento necessario o utile alla migliore attuazione e/o gestione del sistema di protezione dei dati personali;
- riferire tempestivamente all'organo responsabile della disciplina eventuali violazioni della legge e/o del sistema di protezione dei dati personali imputabili agli incaricati, per l'eventuale apertura di una procedura disciplinare e per gli altri provvedimenti che si rendano necessari;
- interagire - laddove richiesto - con il Garante.

5. La bozza di revisione del Documento Programmatico sulla Sicurezza è proposta dal responsabile del trattamento specificamente incaricato.

6. La custodia delle password è assicurata dal responsabile del trattamento specificamente incaricato.

7. Per l'espletamento dell'incarico sono attribuiti al/i responsabile/i i necessari poteri e supporti economici ed organizzativi.

8. Salva diversa e motivata disposizione scritta, l'attribuzione e lo svolgimento dell'incarico di responsabile del trattamento non comportano e non conferiscono al medesimo alcun diritto ad indennità o maggiorazione retributiva.

Art.8 — Responsabilità dei responsabili esterni dei trattamenti

1. Il Titolare individua e nomina i responsabili esterni dei trattamenti.

2. Il Titolare acquisisce dai medesimi l'impegno formale a trattare i dati forniti:

- ai soli fini e nei limiti dell'espletamento dell'incarico o dell'adempimento del contratto stipulato;
- nel rispetto del Codice e del Regolamento e della normativa conseguente -con particolare riferimento all'adozione delle misure minime di sicurezza - nonché di eventuali disposizioni, procedure o istruzioni ulteriormente dettate dal Titolare;
- garantendo al Titolare il diritto di verificare, in tempi e modalità da concordare, il rispetto degli obblighi di legge e delle eventuali ulteriori disposizioni e/o procedure e/o istruzioni;
- informando tempestivamente il Titolare di condizioni o problematiche che siano suscettibili di rendere difficile o pregiudicare la gestione o l'espletamento delle attività nel rispetto della legge e delle eventuali disposizioni, procedure e/o istruzioni dettate dal Titolare; e, in particolare, di qualsiasi elemento oggettivo o soggettivo che abbia compromesso o possa compromettere la sicurezza, la correttezza e la legittimità dei trattamenti in ambito informatico.

3. L'accettazione della nomina da parte del responsabile conferma il possesso dei requisiti e conferma l'assunzione degli impegni di cui al precedente comma.

Art.9 — Responsabilità degli incaricati

1. Tutti gli addetti che nello svolgimento delle proprie mansioni trattano dati personali sono nominati incaricati dei trattamenti. Il rifiuto della nomina equivale al rifiuto dello svolgimento delle mansioni affidate.

2. L'autorizzazione al trattamento dei dati personali può risultare da un atto di incarico esplicito, ovvero dalla documentata preposizione ad un'Area o Ufficio dell'Ente.

3. Ciascun incaricato è tenuto ad effettuare esclusivamente le operazioni e i trattamenti come sopra individuati e non può procedere ad operazioni e/o trattamenti diversi a meno che non sia emanata nuova disposizione scritta da parte del nominante (Titolare o responsabile).

4. Ciascun incaricato è tenuto, in particolare:

- ad eseguire o applicare le disposizioni del nominante sul rilascio dell'informativa e l'acquisizione del consenso;
- osservare scrupolosamente le misure minime di sicurezza e le altre misure definite dal Titolare;

5. Per quanto concerne le misure di sicurezza per i trattamenti mediante personal computer ciascun incaricato è edotto che:

- ad esso è associata una credenziale di autenticazione, comprensiva di una parola chiave (password) che deve, con le opportune cautele, mantenere segreta;
- tale password deve essere composta da 8 caratteri ovvero dal massimo numero di caratteri consentito; la password deve contenere caratteri alfanumerici e deve essere costruita secondo un criterio agevolmente memorizzabile; non può contenere

riferimenti riconducibili a sé o ai propri familiari, deve essere modificata almeno una volta ogni 6 mesi in totale autonomia, ovvero ogni 3 mesi se attraverso personal computer siano trattati dati particolari e/o giudiziari;

- è tenuto a trascrivere User-Id e password in un foglio, a chiuderlo in una busta e a sigillarla, a consegnare la medesima al custode delle password, che assume la responsabilità di conservarla in luogo e/o in forma sicura;
- nel caso di assenza dalla postazione durante una sessione di trattamento, deve disporre il sistema operativo in modalità "stand by" o configurare il salvaschermo protetto da password, comunque curando di non lasciare incustodito e accessibile lo strumento elettronico.
- è suo compito aggiornare il programma antivirus almeno due volte alla settimana, mentre quello degli altri programmi dovrà essere attuato almeno 1 volta ogni semestre; inoltre, almeno 1 volta a settimana è tenuto ad effettuare il c.d. "back up" dei dati contenuti nel personal computer assegnato e a custodire la copia di sicurezza in luogo protetto individuato di concerto con il responsabile del trattamento.

6. Per quanto riguarda invece i trattamenti senza strumenti elettronici, ciascun incaricato è tenuto a:

- utilizzare la documentazione contenente dati personali in modo da non renderli visibili o accessibili ai soggetti non autorizzati, durante le attività di trattamento e nelle pause dalle medesime; una particolare cautela è imposta per il caso che i documenti contengano dati particolari e/o giudiziari;
- riporre e custodire i documenti nei luoghi/schedari predisposti dopo la conclusione delle singole operazioni di trattamento, in particolare facendo uso delle serrature a disposizione per le banche dati che contengano dati particolari e/o giudiziari;
- in ogni caso, a non lasciare incustodito il proprio posto di lavoro prima di aver provveduto alla messa in sicurezza dei dati;
- assicurarsi, al termine della giornata lavorativa, che ogni documento ad esso affidato contenente dati personali sia custodito e protetto da accessi non autorizzati, il ché implica l'uso delle serrature relative agli arredi/schedari e la custodia delle chiavi in luogo idoneo - se opportuno concordato con gli eventuali colleghi di ufficio - ovvero la chiusura stessa della stanza - qualora ciò non osti ad altre attività necessarie.

7. L'incaricato è altresì edotto che è suo compito e responsabilità:

- trasmettere senza ritardo al responsabile del trattamento le notizie delle richieste degli interessati relative all'esercizio dei diritti previsti dal Codice e dal Regolamento accertando l'identità del richiedente e/o il titolo in base al quale abbia effettuato la richiesta;
- eseguire le disposizioni del responsabile e collaborare con il medesimo nelle pratiche di riscontro/risposta agli interessati;
- astenersi da fornire telefonicamente, a mezzo fax o in qualunque altro modo - a fronte delle richieste relative all'esercizio dei diritti - dati di qualunque tipo senza specifica autorizzazione e senza l'identificazione del richiedente;

Art.10 - Responsabilità specifiche degli incaricati che trattano i dati dei dipendenti e dei collaboratori

1. Oltre a quanto previsto dall'articolo precedente, gli incaricati del trattamento che trattano i dati dei dipendenti e dei collaboratori sono edotti che:

- i trattamenti devono essere effettuati nel rispetto di quanto previsto dal Codice e dal Regolamento. Specifica attenzione deve essere prestata nell'eventuale trattamento di dati particolari riferiti a familiari dei dipendenti/collaboratori - soprattutto se minori - in modo da prevenire qualsiasi lesione della loro riservatezza;
- la consegna delle buste-paga e di ogni altro analogo documento, seppur non contenente dati particolari, deve essere effettuata in modo da assicurare la riservatezza dei dati;
- la riservatezza e l'adozione di specifiche cautele in caso di sussistenza di dati particolari, concerne anche le operazioni di trattamento relative ai curricula di aspiranti dipendenti/collaboratori.

Parte III - PRINCIPI SUI TRATTAMENTI DEI DATI PERSONALI

Art.11 - Principio generale

1. Qualunque trattamento di dati personale da parte del Titolare, in quanto ente pubblico, è consentito soltanto per lo svolgimento delle funzioni istituzionali.

Art.12 — Principi applicabili al trattamento di dati diversi da quelli particolari e giudiziari

1. Il trattamento di dati diversi da quelli particolari e giudiziari è consentito, fermo restando quanto sopra, anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente.

2. La comunicazione di dati personali ad altri soggetti pubblici è ammessa quando è prevista da una norma di legge o di regolamento. In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di cui all'articolo 39, comma 2, e non è stata adottata la diversa determinazione ivi indicata La comunicazione e la diffusione di dati personali detenuti dal Titolare a soggetti pubblici, privati o ad enti pubblici economici sono ammesse nei casi e nei limiti.

3. La comunicazione di dati personali a privati o a enti pubblici economici e la diffusione sono ammesse unicamente quando sono previste da una norma di legge o di regolamento.

Art.13 - Principi applicabili al trattamento di dati particolari

1. Il trattamento dei dati particolari da parte del Titolare è consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite.

2. Nei casi in cui una disposizione di legge specifica la finalità di rilevante interesse pubblico, ma non i tipi di dati particolari e di operazioni eseguibili, il trattamento è consentito solo in riferimento

ai tipi di dati e di operazioni identificati e resi pubblici, in relazione alle specifiche finalità perseguite nei singoli casi e nel rispetto dei principi di cui all'articolo 22, con apposito regolamento adottato in conformità al parere espresso dal Garante ai sensi dell'articolo 154, comma 1, lettera g), anche su schemi tipo.

3. Se il trattamento non è previsto espressamente da una disposizione di legge il Titolare può richiedere al Garante l'individuazione delle attività, tra quelle demandate a sé dalla legge, che perseguono finalità di rilevante interesse pubblico e per le quali è conseguentemente autorizzato, il trattamento dei dati particolari. Il trattamento è consentito solo se il Titolare provvede altresì a identificare e rendere pubblici i tipi di dati e di operazioni nei modi di cui al co.2.

4. L'identificazione dei tipi di dati e di operazioni di cui ai commi 2 e 3 è aggiornata e integrata periodicamente.

Art. 14. Principi applicabili al trattamento di dati giudiziari

1. Il trattamento di dati giudiziari da parte del Titolare è consentito solo se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le finalità di rilevante interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili.

2. Le disposizioni di cui all'articolo 13, commi 2 e 4, del presente regolamento si applicano anche al trattamento dei dati giudiziari.

Art. 15. Principi applicabili al trattamento di dati particolari e giudiziari

1. Il trattamento dei dati particolari e giudiziari è effettuato secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato.

2. Nel fornire l'informativa, deve essere fornito un espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati particolari e giudiziari.

3. Possono essere trattati solo i dati particolari e giudiziari indispensabili per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa.

4. I dati particolari e giudiziari sono raccolti, di regola, presso l'interessato.

5. In applicazione delle norme del Codice e del Regolamento, il Titolare - tramite il/i responsabile/i dei trattamenti - verifica periodicamente l'esattezza e l'aggiornamento dei dati particolari e giudiziari, nonché la loro pertinenza, completezza, non eccedenza e indispensabilità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato abbia fornito di propria iniziativa. Al fine di assicurare che i dati particolari e giudiziari siano indispensabili rispetto agli obblighi e ai compiti loro attribuiti, deve essere specificamente valutato il rapporto tra i dati e gli adempimenti. I dati che, anche a seguito delle verifiche, risultino eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per la verifica dell'indispensabilità dei dati particolari e giudiziari riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni o gli adempimenti.

6. I dati particolari e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.

7. I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalità di cui al comma 6 anche quando sono tenuti in elenchi, registri o banche di dati senza l'ausilio di strumenti elettronici.

8. I dati idonei a rivelare lo stato di salute non possono essere diffusi.

9. Rispetto ai dati particolari e giudiziari indispensabili ai sensi del comma 3, si possono effettuare unicamente le operazioni di trattamento indispensabili per il perseguimento delle finalità per le quali il trattamento è consentito, anche quando i dati sono raccolti nello svolgimento di compiti di vigilanza, di controllo o ispettivi.

Parte IV - DISPOSIZIONI SULLA GESTIONE DEI DATI PERSONALI DEGLI ALLIEVI

Art.16 - Comunicazione e diffusione

1. Al fine di agevolare l'orientamento, la formazione e l'inserimento professionale e nel mondo del lavoro, anche all'estero, dei giovani studenti e diplomati, ed ove la comunicazione e/o diffusione siano necessarie al raggiungimento degli scopi istituzionali del Conservatorio o comunque a scopi non incompatibili con essi, si possono comunicare e diffondere, anche a privati e per via telematica, i dati relativi alle attività e ai soggetti, compresi i diplomati, e solo per gli scopi ivi indicati, nonché i dati relativi agli esiti scolastici, intermedi e finali, degli studenti, dei giovani diplomati e diplomandi, borsisti, specializzandi, allievi di corsi di formazione professionale o altri soggetti che comunque svolgano attività di studio e di ricerca presso il Conservatorio anche al fine di consentire l'invio ai soggetti sopra indicati, di inviti ad incontri, manifestazioni, riunioni, congressi, aventi ad oggetto tematiche connesse all'ambito del Conservatorio di Musica.

2. I predetti dati possono essere successivamente trattati per i soli scopi in base ai quali sono comunicati o diffusi.

3. Resta fermo il diritto degli interessati di opporsi per motivi legittimi.

Art.17 - Rilascio dei certificati relativi agli studenti

1. Agli uffici e alla segreteria del Conservatorio è consentito comunque il rilascio a terzi di certificati contenenti dati personali relativi a studenti o diplomati presso il Conservatorio, ivi compresi i dati riguardanti la partecipazione dello studente ai programmi Erasmus, Socrates e comunque ad altri accordi culturali, nonché la sua reperibilità all'estero, purché dietro esibizione di atto di delega con firma autenticata dell'interessato, anche inviata via fax, oppure di atto di delega, senza firma autentica, accompagnato dall'esibizione del documento d'identità del delegante e del delegato anche in fotocopia o trasmesso mediante fax.

Parte V - CRITERI E MODALITA' DI UTILIZZO DEGLI STRUMENTI INFORMATICI

Art.18 - Criteri generali e responsabilità

1. I personal computer (fissi e mobili), gli accessi a internet e le caselle di posta elettronica concessi in dotazione sono beni del Titolare e, in quanto tali, devono essere utilizzati esclusivamente per finalità istituzionali e lavorative e mai per scopi personali.

2. Detti strumenti sono affidati in custodia personale al dipendente che deve custodirli con diligenza e che dovrà tempestivamente informare il responsabile di un eventuale furto o del loro danneggiamento e smarrimento.

Art.19 - Utilizzo del personal computer

1. Onde scongiurare il rischio del danneggiamento dei dati trattati dal Titolare e/o di alterare la stabilità delle applicazioni dell'elaboratore, non è consentito installare alcuna applicazione o programma provenienti dall'esterno in quanto possibili vettori di virus informatici, salvo espressa autorizzazione del responsabile.

2. Non è consentito l'uso di programmi non distribuiti ufficialmente dai fornitori del Titolare.

3. Non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici.

4. Non è consentito modificare le configurazioni impostate sul proprio personal computer .

5. Non è consentito installare o sostituire componenti hardware o software salvo espressa autorizzazione del responsabile. In particolare non è consentita l'installazione sul proprio personal computer di mezzi di comunicazione propri (es: modem) o comunque strutture (schede hardware) non autorizzate.

6. Ai docenti che ricevano in uso personal computers è vietato, fatta salva contraria disposizione scritta a cura del nominante, il trattamento di dati particolari e/o giudiziari.

Art.20 -Utilizzo di supporti magnetici

1. Non è consentito scaricare files (cd rom, floppy, hard disk) in supporti magnetici/ottici non aventi alcuna attinenza con la prestazione lavorativa.

2. Tutti i files di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo e relativa autorizzazione all'utilizzo da parte del responsabile o, comunque, devono passare attraverso un sistema scanner antivirus (di rete) per la posta elettronica e/o un firewall.

Art.21- Utilizzo delle reti interne

1. Le unità di rete sono aree di condivisione di informazioni strettamente istituzionali e non possono, in alcun modo, essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, neppure per brevi periodi, in queste unità.

2. Il responsabile si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquisiti o installati in violazione del presente Regolamento.

Art.22 - Utilizzo della rete internet

1. Non è consentito navigare in siti non attinenti allo svolgimento delle mansioni assegnate.

2. Non è consentito lo scarico di software gratuiti prelevato da siti internet, se non espressamente autorizzato dal responsabile.

3. È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa; l'accesso e l'utilizzo con il proprio indirizzo personale è contrario alle disposizioni del presente Regolamento.

4. Non è permessa la partecipazione, per motivi non professionali, a forum, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi.

5. Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

Art.23 - Utilizzo dei servizi di posta elettronica

1. Gli incaricati accedono all'utilizzo della posta elettronica per ragioni lavorative e pertanto non è consentito utilizzare la posta elettronica (interna ed esterna) per motivi non attinenti allo svolgimento delle mansioni assegnate.

2. Non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

3. La posta elettronica diretta all'esterno della rete interna può essere intercettata da estranei e, dunque, non deve essere usata per inviare documenti di lavoro "strettamente riservati", salva espressa autorizzazione scritta del responsabile dell'ufficio.

4. Ogni comunicazione (interna ed esterna), inviata o ricevuta, che abbia contenuti rilevanti o contenga impegni per il Titolare *deve* essere visionata od autorizzata dal responsabile dell'ufficio.

5. Ogni *e*-mail in uscita dovrà contenere la seguente dicitura: "Avviso di riservatezza - Il testo e gli eventuali documenti trasmessi contengono informazioni riservate al destinatario indicato. La seguente e-mail è confidenziale e la sua riservatezza è tutelata legalmente. La lettura, copia o altro uso non autorizzato o qualsiasi altra azione derivante dalla conoscenza di queste informazioni sono rigorosamente vietate. Qualora abbiate ricevuto questo documento per errore

6. Non è consentito lo scarico di software gratuiti prelevato da siti internet, se non espressamente autorizzato dal responsabile.

7. Non è consentito utilizzare caselle postali personali tramite gli accessi derivanti dai personal computers del Titolare.

Parte V - DISPOSIZIONI FINALI

Art.22 - Controlli, verifiche e sanzioni

1. Controlli e verifiche sul rispetto del presente regolamento avverranno, nei limiti consentiti dalle norme di legge e del contratto collettivo nazionale di lavoro e nel rispetto della dignità e libertà dei lavoratori.

2. La mancata osservanza delle disposizioni del presente regolamento può comportare l'insorgere di responsabilità disciplinari, civili e penali.

Art.23 - Controlli e verifiche sull'uso delle risorse informatiche, dei servizi di posta elettronica e della rete internet

1. Il Titolare si riserva controlli e verifiche sull'uso delle risorse informatiche, dei servizi di posta elettronica e della rete internet: a) "a campione", con finalità di valutazione dell'adeguatezza dell'impianto normativo di cui al presente Regolamento e di coerenza delle condotte osservate dagli incaricati; b) con riferimento a determinate aree o uffici o singoli incaricati e correlative postazioni, laddove siano emersi fondati indizi o sospetti di commissione di atti o condotte non consentite dal presente Regolamento che, disgiuntamente o congiuntamente, possano compromettere la disponibilità e/o integrità e/o riservatezza di dati e/o banche dati ovvero la funzionalità e/o la sicurezza delle risorse informatiche, ovvero rappresentino una non irrilevante violazione degli obblighi lavorativi e/o siano penalmente rilevanti. La finalità è quella di prevenire detti atti o condotte o di impedirne la prosecuzione, sanzionare per quanto di competenza i responsabili. risolvere con tempestività ogni e qualsiasi problema procurato all'organizzazione e al suo funzionamento. tutelare i diritti del Titolare in sede giudiziaria.

2. Relativamente alla fattispecie di cui al punto b), nel momento il Titolare venga per la prima volta a conoscenza di presunti atti o condotte non conformi che non rivestano carattere di obiettiva gravità, per la loro natura o per il genere di conseguenze che ne possano derivare, e pertanto siano differibili i relativi controlli e verifiche, il Titolare emetterà, nei confronti dell'area o ufficio di pertinenza, un avviso tendente a richiamare tutti gli incaricati ad un rigoroso adempimento delle prescrizioni del presente Regolamento. Quando siano acquisite notizie o evidenze di nuovi atti o condotte non conformi, il Titolare potrà procedere a controlli e verifiche su base individuale.

3. Nell'ipotesi di controlli e verifiche "a campione" di cui alla letta) del comma precedente, quando si riscontrino atti o condotte non conformi che rivestano carattere di obiettiva gravità o per la loro natura o per il genere di conseguenze che ne sono derivate o potranno derivarne, la finalità del trattamento successivo è quella esplicitata sub b).

4. In ogni caso, laddove i riscontrati atti o condotte siano preveduti dalla legge come reati, il Titolare si riserva di informare o adire l'Autorità Giudiziaria.

5. Atteso che, quando il Titolare si appresta ad effettuare le predette attività di controllo e verifica, può imbattersi in dati personali riferiti ad uno o più incaricati, si informa tutto il personale, che:

- il trattamento è effettuato nel rigoroso rispetto delle finalità di cui al comma precedente, nel rispetto della legge - ed in particolar modo nel rispetto dei principi di pertinenza e non eccedenza - e delle norme interne all'organizzazione, mediante supporti cartacei e strumenti elettronici; le operazioni di trattamento da effettuare sono quelle e solo quelle indispensabili al raggiungimento delle finalità esplicitate, restando in ogni caso escluse l'interconnessione e la diffusione;

- il trattamento ha natura facoltativa per la fattispecie di cui alla lettera a) del comma i del presente articolo; ha natura obbligatoria per la fattispecie di cui alla lettera b) del medesimo comma, perché il Titolare è tenuto a garantire l'uniforme applicazione delle disposizioni di legge e del presente Regolamento;
- nel caso in cui l'interessato rifiuti senza giustificato motivo di consentire il controllo o le verifiche di cui si tratta, ne può rispondere per ciò stesso in sede disciplinare;
- i dati sono trattati nel rispetto della massima riservatezza anche interna, dal responsabile interno del trattamento e/o da chi - da quegli incaricato - ha effettuato il controllo, da colui o coloro - ivi compresi i competenti uffici del M.U.R. - che siano titolari del potere disciplinare, dal legale rappresentante per quanto di sua competenza, dagli incaricati dell'ufficio personale e dai superiori gerarchici dell'interessato, da ogni altro soggetto specificamente incaricato. I dati possono altresì dover essere messi a disposizione delle Forze di Polizia e/o dell'Autorità Giudiziaria;
- spettano all'interessato i diritti di cui all'art.7, ovvero in qualunque momento esso ha il diritto di ottenere la conferma dell'esistenza o meno dei medesimi dati e di conoscerne il contenuto e l'origine, verificarne l'esattezza o chiederne l'integrazione o l'aggiornamento oppure la rettificazione. Ha altresì il diritto di chiedere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, nonché di opporsi in ogni caso, per motivi legittimi, al loro trattamento;
- Titolare del trattamento è il Conservatorio di Musica "A. Buzzolla" di Adria, con sede in Adria (Ro), viale U. Maddalena, 2, telefono 042621686, E-mail: antonio.buzzolla@conservatorioadria.it nella persona del suo legale rappresentante. Responsabile del trattamento è il Direttore.

6. Il responsabile del trattamento o chi da esso incaricato all'attività di controllo e verifica, nel momento in cui riscontri anche solo la possibilità che l'incaricato abbia commesso atti o posto in essere condotte di cui alla lett b), comma 1 del presente articolo, è informato che può designare un proprio collega quale soggetto da incaricare di assistere alle operazioni successive.

7. Il dipendente così individuato è immediatamente autorizzato con lettera sottoscritta dal responsabile del trattamento.

Adria, 29/05/2025

Il presidente del Consiglio di Amministrazione

CARINCI GIUSEPPE
03.06.2025
10:09:31 UTC