Istruzioni per i soggetti autorizzati
al trattamento di dati personali

Si definisce come "soggetto autorizzato al trattamento di dati personali" la persona fisica espressamente designata che opera su dati personali sotto l'autorità del Titolare del trattamento e/o del Referente per la protezione dei dati, nel rispetto delle disposizioni del Regolamento (UE) 2016/679, "*Regolamento Generale sulla Protezione dei Dati"* (RGPD nel seguito).

In relazione alle attività svolte nell'ambito del Conservatorio di Musica di Cosenza "S. Giacomantonio", il soggetto autorizzato dovrà effettuare i trattamenti di dati personali di competenza attenendosi scrupolosamente alle seguenti istruzioni e ad ogni ulteriore indicazione, anche verbale, che potrà essere fornita dal Titolare o dal Referente per la protezione dati che lo ha nominato.

I dati personali devono essere trattati:

a. nel rispetto dei principi di liceità, correttezza, trasparenza, minimizzazione, esattezza, integrità e riservatezza;
b. per finalità determinate, esplicite e legittime, e dunque elaborati in modo che non siano incompatibili con tali finalità;
c. per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente elaborati;
d. nel pieno rispetto delle misure di sicurezza, custodendo e controllando i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Al fine di garantire la sicurezza dei dati e del trattamento, il Titolare (ai sensi dell'art. 32 del RGPD) deve mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d)

una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

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

Le misure minime di sicurezza sono distinte in funzione delle seguenti modalità di trattamento dei dati:

1. **senza l'ausilio di strumenti elettronici** (es.: dati contenuti in documenti analogici, dati in archivi cartacei);
2. **con strumenti elettronici** (es.: Personal Computer, Tablet, Smartphone).

1. TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

- I documenti contenenti dati personali devono essere custoditi in modo da non essere accessibili a persone non autorizzate al trattamento (es. armadi o cassetti chiusi a chiave).
- I documenti contenenti dati personali che vengono prelevati dagli archivi per l'attività quotidiana devono esservi riposti a fine giornata.
- I documenti contenenti dati personali non devono rimanere incustoditi su scrivanie, tavoli di lavoro o in altre aree accessibili a terzi.
- I documenti contenenti dati personali non devono essere lasciati incustoditi presso le stampanti/fotocopiatrici poste in aree o stanze condivise.
- Le misure di sicurezza applicate alle copie o alle riproduzioni dei documenti contenenti dati personali devono essere identiche a quelle applicate agli originali.
- I dati personali non devono essere condivisi, comunicati o inviati a terzi, a meno che ciò non faccia parte del trattamento per il quale si è stati autorizzati.
- Qualora sia necessario distruggere i documenti contenenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili.

2. TRATTAMENTI CON STRUMENTI ELETTRONICI

- Ciascun utente accede alla rete del Conservatorio e alle sue risorse utilizzando le proprie credenziali di autenticazione.
- Il trattamento di dati personali con strumenti elettronici è consentito solo ai soggetti in possesso di credenziali che consentano il superamento di una procedura di autenticazione relativa ai trattamenti per i quali sono stati autorizzati.
- Le credenziali di autenticazione consistono in alternativa: in un codice per l'identificazione del soggetto, associato a una parola chiave riservata conosciuta solamente dal medesimo; in un dispositivo di autenticazione in possesso e uso esclusivo del soggetto autorizzato, eventualmente associato a un codice identificativo o a una parola chiave; in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave; in un meccanismo di autenticazione multi-fattore che rispetti le migliori prassi pro-tempore.
- A ogni soggetto autorizzato possono essere assegnate o associate individualmente una o più credenziali per l'autenticazione.
- Le credenziali di autenticazione sono strettamente personali; ogni attività, condotta facendo uso delle credenziali suddette è normalmente attribuita al "titolare" delle stesse.
- La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno dodici caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili al soggetto autorizzato (es. il nome) ed è modificata da quest'ultimo al primo utilizzo.
- Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri soggetti, neppure in tempi diversi.
- Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
- Una credenziale è disattivata anche nel caso in cui un soggetto non sia più autorizzato ad effettuare uno dei trattamenti a cui tale credenziale dava accesso.

- I soggetti autorizzati possono consegnare al preposto per la custodia delle credenziali o al Referente per la protezione dei dati una busta chiusa contenente la loro credenziale di autenticazione, ovvero inviano un documento crittografato con la medesima informazione. Nel caso di documenti crittografati, sarà necessario trasmettere al destinatario la chiave necessaria a decrittografare il documento. In alternativa, ove questo sia possibile, i soggetti autorizzati possono comunicare e consegnare al Referente, nelle stesse modalità sopra descritte, una credenziale di autenticazione personale che il Referente potrà utilizzare, ove se ne ravvisi la necessità e l'urgenza, solo in caso di assenza del soggetto autorizzato.
- I soggetti autorizzati non dovranno mai lasciare incustodito e accessibile il proprio terminale durante una sessione di trattamento. Dovendosi allontanare temporaneamente avranno cura di chiudere la sessione o avviare un salvaschermo con *password*, o altre misure che richiedano per l'accesso una procedura di autenticazione di sicurezza almeno pari a quella che permette di identificare l'incaricato su quel terminale.
- I dispositivi (PC, notebook, smartphone, tablet) utilizzati dai soggetti autorizzati per il trattamento dati devono essere obbligatoriamente dotati del software antivirus/ antispyware fornito dal Conservatorio e aggiornato giornalmente.
- Il Responsabile della sicurezza informatica fornisce il software antivirus/antispyware nella sezione del portale dedicata al servizio delle licenze.
- Nel caso in cui sia necessario trattare dati personali sul proprio dispositivo deve essere utilizzato un pacchetto software per la crittografia e deve essere prevista la distruzione di quei dati personali che non occorre più trattare.
- Il Garante per la protezione dei dati personali con provvedimento del 13 ottobre 2008 (doc. n. 1571514 disponibile sul sito www.garanteprivacy.it) ha richiamato l'attenzione sulla necessità di adottare idonei accorgimenti e misure, volti a prevenire accessi non consentiti ai dati personali memorizzati nelle apparecchiature elettriche ed elettroniche destinate a essere: reimpiegate o riciclate o smaltite (si consiglia la lettura degli allegati A e B del provvedimento). A tal proposito, i supporti magnetici od ottici contenenti dati personali devono essere cancellati prima di essere riutilizzati. Qualora ciò non fosse possibile, essi devono essere distrutti.

Sui dispositivi di proprietà del Conservatorio non è consentito:

- Installare programmi non inerenti l'attività lavorativa e/o privi di licenze d'uso.
- Installare antivirus, antispyware e firewall non autorizzati.
- Modificare le configurazioni relative all'accesso alla rete del Conservatorio comunicate al momento della installazione (es. indirizzo IP).
- Attivare l'accesso dall'esterno a un sistema di calcolo se non preventivamente comunicato al Referente per la protezione dei dati o al Responsabile per la sicurezza infomatica.
- Connettere dispositivi esterni personali (chiavi usb, hard disk, ecc.) adeguatamente protetti secondo le indicazioni fornite nel presente documento.

Sui dispositivi di proprietà personale:

- E' consentito installare programmi inerenti l'attività lavorativa che prevedano il trattamento di dati personali solo nel caso in cui il dispositivo sia protetto secondo le linee già definite nel presente documento e l'attività sia autorizzata dal Referente per la protezione dei dati.
- E' obbligatorio, ove si smarrisca un dispositivo personale sul quale siano presenti programmi che prevedono il trattamento di dati personali di cui è Titolare il Conservatorio, informare immediatamente il proprio Referente, il Titolare e il Responsabile per la Protezione dei Dati.
- Il Titolare si riserva il diritto di cancellare, senza preavviso, i dati personali trattati e gli account aziendali presenti nei dispositivi personali in uso ai soggetti autorizzati.

Su Internet non sono ammesse le seguenti attività:

- navigare e/o registrarsi su siti non inerenti la propria attività istituzionale, didattica e di ricerca.
- scaricare programmi e/o file coperti da diritto d'autore se non espressamente in possesso dei diritti di licenza d'uso.
- partecipare a forum o chat line se non per motivi relativi alla propria attività istituzionale.
- tentare accessi fraudolenti a dati, programmi e sistemi altrui.

- utilizzare credenziali di accesso diverse da quelle di cui si è assegnatari individuali.

Posta elettronica istituzionale e modalità di utilizzo

La posta elettronica "@conservatoriodicosenza.it" costituisce il canale di comunicazione istituzionale del Conservatorio.

La casella @ conservatoriodicosenza.it costituisce l'indirizzo ufficiale di ogni dipendente che su questo riceve le comunicazioni relative all'attività istituzionale; il servizio è riservato esclusivamente a un uso istituzionale, nei limiti delle competenze di ogni utente.

L' utente è responsabile civilmente e penalmente dell'attività svolta tramite il proprio account.

Gli utenti si impegnano a non comunicare a terzi le proprie credenziali e si impegnano ad adoperarsi attivamente per salvaguardare la riservatezza delle proprie credenziali.

Il soggetto autorizzato, utente del servizio di posta elettronica, si impegna, nei confronti del Conservatorio, a non utilizzare il servizio per fini diversi da quelli istituzionali o non conformi alle presenti istruzioni. L'utente si assume ogni responsabilità penale e civile ed il carico di ogni eventuale onere derivante dall'uso improprio del servizio; esonera contestualmente il Conservatorio da ogni pretesa o azione che dovesse essere rivolta al Conservatorio medesimo da qualunque soggetto, in conseguenza di tale uso improprio.

L'utente, inoltre, non può utilizzare il servizio in modo da danneggiare, disattivare, sovraccaricare, pregiudicare o interferire con l'utilizzo e il godimento del servizio da parte di altri utenti. L'utente, salvo giustificabili eccezioni, di cui comunque risponde personalmente, non può utilizzare la posta elettronica per inviare, anche tramite collegamenti o allegati in qualsiasi formato (testo, fotografico, video, grafico, audio, codice, ecc.) i messaggi che contengano o rimandino a:

- pubblicità non istituzionale, manifesta o occulta;
- comunicazioni commerciali private;
- materiale pornografico o simile, in particolare in violazione della Legge 3 agosto 1998, n. 269 e successive modifiche "Norme contro lo sfruttamento sessuale dei minori degli anni 18";
- materiale discriminante o lesivo in relazione a razza, sesso, religione, ecc.;
- materiale che violi la normativa in materia di protezione dei dati personali;
- contenuti o materiali che violino i diritti di proprietà di terzi;

- altri contenuti illegali.

Viene, inoltre, fatto divieto di:

- utilizzare per le comunicazioni inerenti alle attività istituzionali caselle di posta diverse da quelle del dominio conservatoriodicosenza.it;
- inviare lettere a catena ovvero messaggi ripetuti;
- diffondere notizie non veritiere o non verificate;
- inondare di messaggi indesiderati (spamming);
- non rispettare le normative sulla proprietà intellettuale;
- diffondere consapevolmente virus.

L'elenco riportato è da intendersi non esaustivo.

L'utente prende, inoltre, atto del fatto che è vietato servirsi, o dar modo ad altri di servirsi, del servizio di posta elettronica per danneggiare, violare o tentare di violare il segreto della corrispondenza e il diritto alla riservatezza.

L'Utente accetta di essere riconosciuto quale autore dei messaggi inviati dal suo account e di essere il ricevente dei messaggi spediti al suo account.

Il Conservatorio si riserva la facoltà di segnalare alle autorità competenti, per gli opportuni accertamenti ed i provvedimenti del caso, le eventuali violazioni delle condizioni di utilizzo dell'account di posta elettronica @conservatoriodicosenza.it.

***Data Breach* (Violazione dei dati) e obbligo di notificazione.**

L'art. 4 definisce i *Data Breach* come "violazione dei dati", ossia la violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. Il Gruppo di lavoro ex Art. 29 (Ora, Comitato europeo della protezione dei dati), nelle sue linee guida dedicate al tema, ha distinto in tre macro-categorie il Data Breach: a) *Confidentiality Breach* (accesso accidentale o abusivo ai dati); b) *Availability Breach* (perdita o distruzione accidentale o non autorizzata del dato); c) *Integrity Breach*, quando vi è un'alterazione accidentale o non autorizzata del dato personale.

La notifica delle violazioni dei dati personali ricade sul Titolare del trattamento e deve essere comunicata all'autorità di controllo (Garante per la protezione dei dati personali) senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, pena pesanti sanzioni amministrative e responsabilità in sede civile e penale.

Pertanto, tutto il personale è tenuto a cooperare con il Titolare del trattamento al rispetto degli artt. 33 e 34 del RGPD, segnalando prontamente, allo stesso Titolare o al Responsabile della Protezione dei Dati (rpd@conservatoriodicosenza.it), anche potenziali circostanze idonee a prefigurare una violazione dei dati personali o della sicurezza (es. perdita di un *device* non cifrato*, device* infettato da un *ransomware*, furto di un laptop di un dipendente che contenga dati personali degli studenti o dei dipendenti del Conservatorio, perdita di disponibilità del dato personale. Si pensi, in quest'ultimo caso, a una mail contenente dati personali di terzi inviata per errore a un terzo non autorizzato), al fine di attivare tutte le procedure di cui agli artt. 33 e 34 del Regolamento (UE) 2016/679.

Il Responsabile della protezione dei dati

Avv. Sergio NIGER

NIGER SERGIO
16.12.2019
09:34:55 UTC