

ATTO DI NOMINA A RESPONSABILE ESTERNO DEL TRATTAMENTO INFORMatico

in applicazione del “Codice in materia di protezione dei dati personali” di cui all’art.29 del D. Lgs. 196/03 e s. m., e art. 28 del Regolamento UE 679/16 “Regolamento generale sulla protezione dei dati”

Oggetto: L’Associazione MITTELFEST, con sede legale a Cividale del Friuli, in Stretta San Martino 4, P.IVA 02031930304, nella persona del proprio legale rappresentante ROBERTO CORCIULO

Nomina a Responsabile esterno del trattamento informatico dei dati ai sensi dell’art. 4, c. 1, lettera g) e art. 29 del D. Lgs. 196/03 e s. m., nonché dell’art. 28 del Regolamento UE 679/16

NGUYEN FRANCESCO DIEP

:

visto il Decreto Legislativo 30 giugno 2003, n. 196 “Codice in materia di protezione dei dati personali”, di seguito definito “Codice”;

visto il Regolamento UE 679/16 “Regolamento generale sulla protezione dei dati”, di seguito definito “Regolamento”;

preso atto che l’art. 4, c. 1, lettera g) del suddetto Decreto definisce il “Responsabile” come la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal Titolare al trattamento dei dati personali;

preso atto che l’art. 4, c. 1, n. 8 del suddetto Regolamento definisce “Responsabile del trattamento” come la persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

atteso che l’art. 29, commi 2, 3, 4 e 5 del D. Lgs. 196/03 dispone che:

2. Se designato, il Responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
3. Ove necessario per esigenze organizzative, possono essere designati Responsabili più soggetti, anche mediante suddivisione dei compiti.
4. I compiti affidati al Responsabile sono analiticamente specificati per iscritto dal Titolare.
5. Il Responsabile effettua il trattamento attenendosi alle istruzioni impartite dal Titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni”;

atteso che l’art. 28 del Regolamento UE 679/16 dispone che:

1. Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest’ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantiscano la tutela dei diritti dell’interessato.
3. I trattamenti da parte di un Responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell’Unione o degli Stati membri, che vincoli il Responsabile del trattamento al

titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento”;

ritenuto che il sig. **NGUYEN Francesco Diep**, in qualità di fornitore esterno di servizi informatici, per l’ambito di attribuzioni, funzioni e competenze conferite, abbia i requisiti di esperienza, capacità ed affidabilità idonei a garantire il pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati, ivi compreso il profilo relativo alla sicurezza;
ciò premesso,

NOMINA

NGUYEN Francesco Diep, residente in Via del Sale 1/b -33100 UDINE Codice Fiscale NGFFNC89T20G317X -Partita Iva 02862240303, Responsabile esterno del trattamento per la gestione dei dati e dei sistemi informatici, svolta nell’ambito dello stesso incarico professionale di:

- pianificazione e gestione degli strumenti della comunicazione dei Social network e della newsletter attraverso una social media strategy, lavorando sul piano della gestione delle diverse piattaforme e della curatela dei contenuti editoriali rispetto agli obiettivi comunicativi e ai pubblici individuati come pertinenti per ogni piattaforma e agli obiettivi dati;
- posizionamento strategico di Mittelfest nei diversi social network rispetto ai pubblici diversi di riferimento per gli specifici spettacoli e attività;
- attività di Advertising online secondo un preciso piano editoriale e il budget assegnato a tale scopo;

Il Responsabile dovrà effettuare il trattamento dei dati nel rispetto della normativa vigente e delle misure di sicurezza adeguate ed individuate nel “Regolamento aziendale per l’utilizzo delle risorse informatiche, di internet e di posta elettronica per l’utilizzo dei servizi informatici aziendali” di Associazione Mittelfest nonché in conformità del Regolamento UE 679/16, art. 32.

Il Responsabile dovrà, inoltre, rispettare le istruzioni impartite dal Titolare del trattamento sia nel presente atto di nomina, sia in successive eventuali comunicazioni.

In particolare, nel Vostro incarico dovrete svolgere le seguenti attività:

1) gestire il sistema informatico, nel quale risiedono le banche dati personali, in osservanza all’art. 32 del Regolamento UE 679/16 attenendosi anche alle disposizioni del Titolare in tema di sicurezza e ai Regolamenti interni all’azienda;

2) predisporre ed aggiornare un sistema di sicurezza informatico idoneo a rispettare le prescrizioni dell’art. 31 e ss. del D. Lgs. 196/03 e dell’art. 32 del Regolamento UE 679/16; adottare tutte le preventive adeguate di sicurezza, ritenute idonee al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. Più specificatamente, fatte salve le successive integrazioni del Regolamento interno e in base all’art. 32 del Regolamento, il Responsabile del trattamento informatico dovrà:

- mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendano – se fosse necessario - la pseudonimizzazione e la cifratura dei dati personali, la capacità di assicurare su base permanente la riservatezza, l’integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, la capacità di ripristinare tempestivamente la disponibilità e l’accesso dei dati personali in caso di incidente fisico o tecnico ed una procedura per testare, verificare e valutare regolarmente l’efficacia delle misure tecniche e organizzative;
- assegnare e gestire il sistema di autenticazione informatica secondo le modalità indicate nel Regolamento interno e quindi, fra le altre, generare, sostituire e invalidare, in relazione agli strumenti

e alle applicazioni informatiche utilizzate, le parole chiave e i codici identificativi personali da assegnare agli incaricati del trattamento dati della Società committente, svolgendo anche la funzione di custode delle copie delle credenziali;

- procedere, più in particolare, alla disattivazione dei codici identificativi personali, in caso di perdita della qualità che consentiva all'utente o incaricato l'accesso all'elaboratore;
- adottare adeguati programmi antivirus, firewall e altri strumenti software o hardware atti a garantire la massima misura di sicurezza nel rispetto di quanto dettato dal D. Lgs. 196/03 e dal Regolamento UE 679/16 ed utilizzando le conoscenze acquisite in base al progresso tecnico software e hardware, verificandone l'installazione, l'aggiornamento e il funzionamento degli stessi;
- adottare tutti i provvedimenti necessari ad evitare la perdita o la distruzione, anche solo accidentale, dei dati personali e provvedere al ricovero periodico degli stessi con copie di backup, vigilando sulle procedure attivate in struttura. Il Responsabile del trattamento informatico dovrà anche assicurarsi della qualità delle copie di backup dei dati e della loro conservazione in luogo adatto e sicuro;
- indicare al personale competente o provvedere direttamente alla distruzione e smaltimento dei supporti informatici di memorizzazione logica o alla cancellazione dei dati per il loro reimpiego;
- cooperare nella predisposizione del Registro dei trattamenti dei dati personali (qualora la Società fosse tenuta alla sua redazione) per la parte concernente il sistema informatico ed il trattamento informatico dei dati;
- predisporre e implementare le eventuali ulteriori misure adeguate di sicurezza imposte dall'art 32 Regolamento UE 679/16 per il trattamento informatico dei dati sensibili o giudiziari per la conseguente tutela degli strumenti elettronici;

3) coordinare assieme al Titolare le attività operative degli incaricati del trattamento nello svolgimento delle mansioni loro affidate per garantire un corretto, lecito e sicuro trattamento dei dati personali nell'ambito del sistema informatico;

4) collaborare – se fosse necessario - con il Titolare per l'attuazione delle prescrizioni impartite dal Garante; interagire con i soggetti incaricati di eventuali verifiche, controlli o ispezioni, evadendo tempestivamente le richieste di informazioni da parte dell'Autorità Garante e dando immediata esecuzione alle eventuali indicazioni che pervengano dalla medesima Autorità;

5) comunicare prontamente al Titolare qualsiasi situazione di cui sia venuto a conoscenza, nell'espletamento delle attività di esecuzione dell'incarico professionale assegnato, che possa compromettere il corretto trattamento informatico dei dati personali;

6) adottare e gestire sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte di tutte le persone incaricate al trattamento dei dati. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti allo "username" utilizzato, i riferimenti temporali e la descrizione dell'evento (log in e log out) che le ha generate e devono essere conservate per un congruo periodo, concordato con il Titolare del trattamento;

7) comunicare tempestivamente al Titolare casi di accesso non autorizzato ai dati o di trattamento non consentito, o non conforme alle finalità istituzionali.

8) mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 del Regolamento e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate da Titolare del trattamento o da un altro soggetto da questi incaricato;

9) individuare, nell'ambito della propria organizzazione, le persone (dipendenti o collaboratori) munite dei necessari requisiti di esperienza, capacità ed affidabilità, cui attribuire, rispetto al sistema informatico aziendale del committente, le mansioni di amministratore di sistema definendone gli ambiti di operatività, in conformità al provvedimento 27 novembre 2008 del Garante per la protezione dei dati personali; conservare, aggiornare e mettere a disposizione del committente e/o degli organi di controllo, l'elenco con i dati (nome, cognome, funzione) degli amministratori di sistema; predisporre ed attuare un idoneo sistema di controllo periodico sull'operato dei propri amministratori, fornendo, inoltre, un rapporto periodico al committente sulla correttezza dell'attività di queste persone rispetto alle misure di sicurezza adottate ed alle mansioni attribuite;

11) mantenere la più completa riservatezza sui dati trattati e sulle tipologie di trattamento effettuate; tale obbligo è da considerarsi pienamente vigente anche nel caso di cessazione del rapporto di impiego e/o comunque di collaborazione;

Si rammenta che l'operato del Responsabile esterno per il trattamento informatico dei dati deve essere oggetto di verifica, con cadenza almeno annuale, per acclarare che le attività svolte dallo stesso siano effettivamente conformi alle mansioni attribuite.

Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

Con la sottoscrizione della presente, il Responsabile esterno accetta la nomina.

Una copia del presente atto di nomina dovrà essere restituita ad Associazione Mittelfest, debitamente firmato per accettazione.

Cividale, 10.03.2020

IL TITOLARE

Presidente del CdA e legale rappresentante
(dott. Roberto Corciulo)

IL RESPONSABILE

Compiti ed istruzioni

PER I RESPONSABILI DEL TRATTAMENTO DEI DATI PERSONALI

in applicazione del D. Lgs. 196/03 “Codice in materia di protezione dei dati personali” e del Regolamento UE 679/16 “Regolamento generale sulla protezione dei dati”

PRINCIPI GENERALI DA OSSERVARE

Ogni *trattamento* di dati personali deve avvenire, nel rispetto primario dei seguenti principi di ordine generale:

Ai sensi dell’art. 11 del Codice Privacy, che prescrive le “*Modalità del trattamento e requisiti dei dati*”, nonché ai sensi dell’art. 5 del Regolamento UE che prescrive i “*Principi applicabili al trattamento di dati personali*”, per ciascun trattamento di propria competenza, l’incaricato deve fare in modo che siano sempre rispettati i seguenti presupposti:

- i dati devono essere trattati:

secondo il principio di **liceità**, vale a dire conformemente alle disposizioni del Codice e del Regolamento, nonché alle disposizioni del Codice Civile, per cui, più in particolare, il trattamento non deve essere contrario a norme imperative, all’ordine pubblico ed al buon costume;

secondo il principio fondamentale di **correttezza**, il quale deve ispirare chiunque tratti qualcosa che appartiene alla sfera altrui;

secondo il principio di **trasparenza**, che impone che le informazioni e le comunicazioni relative al trattamento dei dati siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro;

- i dati devono essere raccolti solo per **scopi**:

determinati, vale a dire che non è consentita la raccolta come attività fine a sè stessa;

espliciti, nel senso che il soggetto interessato va informato sulle finalità del trattamento;

legittimi, cioè, oltre al trattamento, come è evidente, anche il fine della raccolta dei dati deve essere lecito;

compatibili con il presupposto per il quale sono inizialmente trattati, specialmente nelle operazioni di comunicazione e diffusione degli stessi;

- i dati devono, inoltre, essere:

esatti, cioè, precisi e rispondenti al vero e, se necessario, **aggiornati**;

pertinenti, ovvero, il trattamento è consentito soltanto per lo svolgimento delle funzioni istituzionali, in relazione all’attività che viene svolta;

completi: non nel senso di raccogliere il maggior numero di informazioni possibili, bensì di contemplare specificamente il concreto interesse e diritto del soggetto interessato;

non eccedenti in senso quantitativo rispetto allo scopo perseguito, ovvero devono essere raccolti solo i dati che siano al contempo strettamente necessari e sufficienti in relazione al fine, cioè la cui mancanza risulti di ostacolo al raggiungimento dello scopo stesso;

conservati per un periodo non superiore a quello necessario per gli scopi del trattamento e comunque in base alle disposizioni aventi ad oggetto le modalità ed i tempi di conservazione degli atti amministrativi. Trascorso detto periodo i dati vanno resi anonimi o cancellati e la loro comunicazione e diffusione non è più consentita.

Ciascun trattamento deve, inoltre, avvenire nei limiti imposti dal principio fondamentale di **riservatezza** e nel rispetto della dignità della persona dell'interessato al trattamento, ovvero deve essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi.

Se il trattamento di dati è effettuato in violazione dei principi summenzionati e di quanto disposto dal Codice Privacy e dal Regolamento è necessario provvedere al "blocco" dei dati stessi, vale a dire alla sospensione temporanea di ogni operazione di trattamento, fino alla regolarizzazione del medesimo trattamento (ad esempio fornendo l'informativa omessa), ovvero alla cancellazione dei dati se non è possibile regolarizzare.

In merito alla **responsabilità civile**, si fa rinvio all'art. 15 del Codice Privacy, che dispone relativamente ai danni cagionati per effetto del trattamento ed ai conseguenti obblighi di risarcimento, implicando, a livello pratico, che, per evitare ogni responsabilità, l'operatore è tenuto a fornire la prova di avere applicato le misure tecniche di sicurezza più idonee a garantire appunto la sicurezza dei dati detenuti.

Inoltre, il Regolamento europeo all'art. 82 in riferimento al diritto al risarcimento prevede espressamente la responsabilità civile del responsabile del trattamento per inosservanza dei propri obblighi e o delle istruzioni fornite dal Titolare. Il responsabile viene esonerato dall'obbligo di risarcire i danni solo se dimostra che l'evento dannoso non gli è in alcun modo imputabile.