Oggetto: **Nomina a responsabile del trattamento e amministratore di sistema** di FLOR INFORMATICA S.R.L., ai sensi degli artt. 28 e 32 del Regolamento europeo sul trattamento dei dati personali n 679/2016 e Provvedimento a carattere generale del Garante per la protezione dei dati personali di data 27 novembre 2008.

IL TITOLARE

visto il Regolamento europeo sulla protezione dei dati 27 aprile 2016, n. 679;

visto il Decreto legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali" come modificato dal decreto legislativo 8 agosto 2018, n. 101;

visto il Provvedimento a carattere generale del Garante per la protezione dei dati personali di data 27 novembre 2008, avente ad oggetto "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema";

vista la Circolare dell'Agenzia per l'Italia Digitale (AgID) 18 aprile 2017, n. 2, che detta le misure minime di sicurezza ICT per le Pubbliche Amministrazioni nel rispetto del Codice per l'Amministrazione Digitale;

visto il punto 8) del paragrafo 1 dell'art. 4 del Regolamento UE 2016/679 che definisce «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;

visto il paragrafo 1 dell'art. 28 del Regolamento UE 2016/679 che prevede che "qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato";

visto il paragrafo 3 dell'art. 28 del Regolamento UE 2016/679 che prevede che "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";

considerato che per capacità, esperienza ed affidabilità FLOR INFORMATICA s.r.l. fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, con particolare riferimento al profilo relativo alla sicurezza nel trattamento dei dati personali;

in data 24/11/2023 tra l'Ente COMUNITA' DELLA VALLE DI CEMBRA e il fornitore FLOR INFORMATICA s.r.l. è stato stipulato il contratto avente ad oggetto il servizio di assistenza e consulenza informatica, di gestione della sicurezza informatica e di gestione delle misure minime di sicurezza informatica (CIG ZEF3C76368);

per lo svolgimento di tale attività e/o servizio, FLOR INFORMATICA S.R.L. tratta dati personali di cui è titolare l'Ente;

visto il Codice degli Enti Locali della Regione autonoma Trentino-Alto Adige approvato con Legge regionale 3 maggio 2018 n. 2;

visto lo Statuto comunale;

NOMINA
FLOR INFORMATICA S.R.L.
QUALE
RESPONSABILE DEL TRATTAMENTO E AMMINISTRATORE DI SISTEMA
per lo svolgimento del servizio di assistenza e consulenza informatica, di gestione della sicurezza informatica e di gestione delle misure minime di sicurezza informatica dell'ente
effettuato con strumenti elettronici o comunque automatizzati o con strumenti diversi a decorrere dal 01/10/2023 e fino alla cessazione del contratto

L'elenco completo dei soggetti autorizzati a prestare le attività di assistenza informatica all'Ente è riportato nell'allegato A, parte integrante del presente atto di nomina.
In relazione a tale incarico, il fornitore dovrà opportunamente autorizzare, istruire e monitorare i soggetti indicati nell'Allegato A, che avranno il compito di sovraintendere e gestire le risorse del sistema informativo e del sistema di basi di dati dell'Ente, in base alle prescrizioni e indicazioni date dal Titolare.
In qualità di amministratore di sistema e responsabile del trattamento, il fornitore può accedere ed effettuare il trattamento dei dati gestiti nel sistema informatico unicamente per finalità di gestione, manutenzione e limitando le operazioni a quelle necessarie a tali fini, trattando i dati personali di cui viene a conoscenza nell'ambito dello svolgimento delle operazioni di manutenzione in modo lecito, con assoluta riservatezza e secondo correttezza.
In particolare, nell'effettuare operazioni di gestione e manutenzione:

- se è necessario eseguire stampe per controllare il funzionamento di stampanti o per verificare il funzionamento di strumenti o programmi installati, quando non strettamente necessario relativamente al test in oggetto, si devono utilizzare files di prova privi di dati personali;
- eventuali stampe di prova di dati personali vanno immediatamente distrutte, così come vanno cancellate o restituite le registrazioni di dati personali su supporti di registrazione;
- se è strettamente necessario accedere a files già esistenti contenenti dati personali (ad esempio files di log o per il recupero di un testo) trattare tutti i dati personali di cui viene a conoscenza nell'ambito dello svolgimento delle operazioni di manutenzione in modo lecito e secondo correttezza ed ai soli fini della gestione e manutenzione;
- se vi è necessità è consentito prelevare e trasferire presso il proprio centro di assistenza tecnica apparecchiature elettroniche, parti di esse o supporti contenenti i dati oggetto della manutenzione ed assistenza. Se l'oggetto della manutenzione ed assistenza non sono i dati stessi o il loro recupero, e se tecnicamente possibile, i supporti di registrazione devono essere cancellati prima dell'asporto (verificando se è necessario o utile consegnare un backup agli addetti). Ove prevista, la password di accesso è comunicata dall'incaricato il quale provvede a cambiarla al termine delle operazioni di manutenzione;
- i dati sono consegnati al solo fine della manutenzione ed assistenza e non devono essere utilizzati per scopi diversi da quelli per i quali è stato richiesto l'intervento;
- l'accesso per la tele-assistenza deve avvenire esclusivamente se motivato da oggettive necessità dipendenti dall'oggetto dell'incarico e richiede che l'incaricato attivi il programma che consente la teleassistenza.

È compito del fornitore implementare una misura idonea alla registrazione degli accessi compiuti dai propri autorizzati al sistema informativo (access log) dell'Ente, che comprenda i riferimenti temporali e la descrizione dell'evento e che consenta di conservare tali registrazioni in maniera completa e inalterata per un periodo minimo di sei mesi.

Collaborando con il Titolare del trattamento, il fornitore deve osservare e adempiere alle seguenti prescrizioni:

- impostare e gestire un sistema di autenticazione informatica per i trattamenti di dati personali effettuati con strumenti elettronici, conforme a quanto previsto dall'art. 32 del Regolamento europeo 679/2019; in particolare, deve:
  1. attribuire a ciascun incaricato del trattamento le credenziali univoche di autenticazione composte da codice per l'identificazione dell'incaricato e password per l'utilizzazione del sistema e, dove previsto, dei singoli applicativi o sistemi componenti;

2. prevedere password composte, ove tecnicamente possibile, da almeno otto caratteri;
3. prevedere che uno stesso codice non possa, neppure in tempi diversi, essere riassegnato a persone diverse;
4. prevedere un sistema che obblighi gli incaricati alla modifica delle credenziali univoche di autenticazione con una cadenza trimestrale;
5. operare la disattivazione delle credenziali di autenticazione non utilizzate da almeno sei mesi o in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

- impostare e gestire un sistema di autorizzazione informatica per gli incaricati dei trattamenti di dati personali effettuati con strumenti elettronici, conforme dall'art. 32 del Regolamento europeo 679/2019; in particolare deve:
  1. configurare d'intesa con il titolare un sistema di autorizzazione;
  2. configurare i profili di autorizzazione degli incaricati e dei responsabili prima dell'inizio del trattamento;
  3. periodicamente e almeno annualmente verificare le condizioni per la conservazione dei profili di autorizzazione da parte degli incaricati e dei responsabili
  4. verificare costantemente che l'Ente abbia adottato le misure minime di sicurezza per il trattamento dei dati personali, previste dalla Circolare dell'Agenzia per l'Italia Digitale (AgID) 18 aprile 2017, n. 2, che detta le misure minime di sicurezza ICT per le Pubbliche Amministrazioni nel rispetto del Codice per l'Amministrazione Digitale provvedendo senza indugio agli adeguamenti eventualmente necessari e supportarlo nel loro aggiornamento;
- suggerire l'adozione e l'aggiornamento delle misure di tecniche e organizzative adeguate a garantire il livello di sicurezza adeguato al rischio atte a realizzare quanto previsto all'art. 32 del Regolamento europeo 679/2016;
- curare l'adozione e l'aggiornamento delle eventuali misure adeguate di cui al punto precedente;
- attivare e aggiornare con cadenza almeno semestrale idonei strumenti elettronici atti a proteggere i dati trattati attraverso gli elaboratori del sistema informativo contro il rischio di intrusione e contro l'azione dei virus informatici;
- aggiornare periodicamente, con frequenza almeno semestrale, i programmi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti;
- adottare procedure per la custodia delle copie di sicurezza dei dati e per il ripristino della disponibilità dei dati e dei sistemi (operazioni di backup e recovery dei dati);
- predisporre un piano di controlli periodici, da eseguirsi con cadenza almeno semestrale, dell'efficacia delle misure di sicurezza adottate;
- consegnare copia delle credenziali di autenticazione quale Amministratore di sistema al Titolare, incluse le password di accesso al server e alle risorse informatiche.

È compito del fornitore riferire periodicamente, ed in ogni caso con cadenza almeno annuale al Titolare sullo svolgimento dei propri compiti, mediante presentazione di dettagliata relazione degli interventi effettuati corredata dalla dimostrazione necessaria per dimostrare conformità a tutti i propri obblighi.
Il fornitore è tenuto a fornire piena collaborazione al Titolare nello svolgimento delle verifiche periodiche circa il rispetto delle disposizioni di legge e l'adeguatezza delle misure di sicurezza adottate.
Il fornitore è tenuto ad assistere il Titolare nell'adempimento dell'obbligo di rispondere alle richieste di esercizio dei diritti degli interessati e delle istanze del Garante per la protezione dei dati personali.

L'amministratore di sistema, nell'espletamento delle sue funzioni, ha l'obbligo di rispettare anche le disposizioni e prescrizioni di cui all'art. 28 del Reg. Ue 679/2016, destinate ai responsabili del trattamento in quanto per il servizio di assistenza e consulenza informatica, di gestione della sicurezza informatica e di gestione delle misure minime di sicurezza informatica dell'ente si configura anche quale responsabile "esterno" del trattamento; in particolare:

<u>Subresponsabili:</u>

Il fornitore, per l'erogazione delle attività affidate e dei relativi trattamenti di dati personali non è legittimato a ricorrere a un altro responsabile senza previa specifica autorizzazione scritta. La richiesta deve indicare le specifiche attività di trattamento affidate all'altro responsabile.

Istruzioni

Il fornitore ha l'obbligo di osservare le istruzioni che sono e saranno impartite dal titolare del trattamento con il presente atto e con comunicazioni successive in materia di trattamento dei dati personali.
Il fornitore ha l'obbligo di osservare la normativa speciale in materia di trattamento dei dati relativa al servizio oggetto del contratto.

Incaricati al trattamento

Il fornitore ha l'obbligo di individuare, secondo idonee modalità, i soggetti incaricati al trattamento che agiscono sotto la sua autorità.
Il fornitore ha l'obbligo di impartire le disposizioni organizzative e operative e fornire ai soggetti autorizzati le istruzioni per il corretto, lecito, pertinente e sicuro trattamento dei dati, eseguendo gli opportuni controlli.

Misure di sicurezza

Il fornitore si impegna ad adottare e attuare, in via autonoma, le misure di sicurezza tecniche e organizzative più adeguate a garantire un livello di tutela dei dati adeguato al rischio, tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento effettuato in esecuzione del Contratto.
Il fornitore provvede affinché vengano rigorosamente adottate tutte le misure idonee a garantire la disponibilità, l'integrità e la riservatezza dei dati; vale a dire misure che permettano di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati trattati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità per le quali i dati sono stati raccolti e di modifiche o cancellazioni a seguito di errori o di azioni volontarie, ma anche a seguito di malfunzionamenti o danni dei sistemi tecnologici.
Il fornitore verifica periodicamente lo stato di applicazione del D.lgs. 30 giugno 2003 n. 196 e del Regolamento Europeo 2016/679, nonché la corretta applicazione, il buon funzionamento dei sistemi e, ai sensi dell'art. 32 del GDPR, delle misure adottate per la tutela dei dati personali e la conformità alle indicazioni dell'Autorità Garante e del Titolare.
I dati personali, trattati in esecuzione del contratto, devono essere tenuti separati rispetto a quelli eventualmente trattati per conto di altre terze parti applicando una segregazione fisica e logica, ove possibile.
Il fornitore garantisce la stretta osservanza dell'incarico ricevuto, escludendo qualsiasi trattamento o utilizzo dei dati personali che esuli dalle attività previste nel Contratto.
Il fornitore ha l'obbligo di provvedere alla formazione e tenuta del registro delle di attività di trattamento svolte per conto del Titolare, se previsto dall'art. 30 del Regolamento UE 2016/679.
Il fornitore ha l'obbligo di designare un Responsabile della protezione dei dati, se previsto dall'art. 37 del Regolamento UE 2016/679 e di comunicarne il nominativo e riferimento al Titolare entro 10 giorni dalla nomina.
Il fornitore si impegna a supportare il titolare nella predisposizione e aggiornamento della valutazione di impatto del trattamento sui diritti e sulle libertà delle persone.

Trasferimento dati extra UE

Se i dati contenuti nelle banche dati vengono trasferiti in Paesi extraeuropei il fornitore deve verificare che il Paese extraeuropeo sia destinatario di una decisione di adeguatezza della Commissione Europea oppure, in mancanza, il fornitore deve offrire garanzie adeguate e verificare che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi ai sensi dell'art. 46 GDPR.
In quest'ultimo caso, il fornitore deve verificare, caso per caso se la legge o la prassi del Paese terzo incidono sull'efficacia delle garanzie adeguate contenute negli strumenti di trasferimento.
Il fornitore dovrà, se necessario, attuare misure supplementari che andranno identificate, caso per caso, conformemente alle raccomandazioni adottate dall'European Data Protection Board (raccomandazioni 01/2020; raccomandazioni 02/2020) e ne dovrà fornire puntuale rendicontazione nei termini del paragrafo Controlli e ispezioni.

Assistenza

- esercizio dei diritti dell'interessato

Il fornitore ha l'obbligo di prestare la propria collaborazione al Titolare nella predisposizione, ai sensi degli artt. 13 e 14 Regolamento UE 2016/679, dell'informativa agli interessati, della modulistica e delle altre forme idonee di informazione, inerenti al proprio servizio.

Il fornitore ha l'obbligo di assistere il Titolare del trattamento con misure tecniche e organizzative adeguate al fine di soddisfare l'obbligo dello stesso di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III del Regolamento UE 2016/679.

Il fornitore ha l'obbligo di prestare la propria collaborazione per consentire al Titolare di rispondere in modo esaustivo e tempestivo alle richieste e prescrizioni delle Autorità di controllo e dell'Autorità Giudiziaria.

- misure di sicurezza

Il fornitore notifica al Titolare del trattamento ogni violazione di dati a carattere personale nel termine massimo di 36 ore dopo esserne venuto a conoscenza. Tale notifica è accompagnata da ogni documentazione utile per permettere al Titolare del trattamento, se necessario, di notificare la violazione all'autorità di controllo competente.

Spetta solo al Titolare decidere di non effettuare la notifica all'Autorità di controllo competente, in presenza di semplice incidente che non ha comportato perdita, distruzione, diffusione o modifica dei dati e/o, nonostante la violazione dei dati personali, sia improbabile che essa comporti un rischio per i diritti e le libertà degli Interessati. Il fornitore provvederà a fornire al Titolare del trattamento tutte le informazioni di propria competenza al fine di consentire a quest'ultimo di effettuare tale valutazione.

Previo accordo con il Titolare del trattamento, il fornitore comunica, in nome e per conto del Titolare del trattamento, la violazione di dati a carattere personale alla persona interessata al più presto, qualora, in base alla valutazione del Titolare, tale violazione sia suscettibile di generare un rischio elevato per i diritti e le libertà di una persona fisica.

- informazioni accountability (responsabilizzazione)

Il fornitore ha l'obbligo di mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 del Regolamento UE 2016/679 e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzati dal Titolare del trattamento o da un altro soggetto dallo stesso incaricato.

Il fornitore ha l'obbligo di informare il Titolare del trattamento di ogni comunicazione o attività di controllo o ispettiva dell'Autorità di controllo.

Controlli e ispezioni

Il fornitore ha l'obbligo di permettere al Titolare del trattamento di porre in essere controlli periodici finalizzati ad accertare l'adeguatezza delle misure di sicurezza, l'osservanza delle istruzioni impartite e in generale il rispetto della normativa in materia. Queste verifiche possono essere condotte mediante preavviso scritto di minimo 7 giorni lavorativi.

Il Titolare garantisce che:

- i controlli, le ispezioni e le verifiche di cui al paragrafo che precede avranno luogo durante il normale orario di lavoro e senza ostacolare l'attività del fornitore e di altri clienti del fornitore;
- tutte le informazioni ottenute o generate dal Titolare o dal/i proprio/i auditor in relazione a tali controlli, ispezioni e verifiche saranno mantenute strettamente confidenziali (salvo richieste da parte delle Autorità di controllo o, se altrimenti richiesto, dalla legge applicabile);
- conviene che il costo di siffatti controlli, verifiche o ispezioni, sarà a proprio carico, a meno che dai predetti accertamenti, controlli o ispezioni non risultino inadempimenti e/o violazioni del fornitore agli obblighi su di lui incombenti.

Manleve

Il fornitore s'impegna a risarcire, manlevare e tenere indenne il Titolare per qualsiasi danno, pretesa, risarcimento, sanzione e/o pregiudizio che possa derivargli dalla mancata osservanza degli obblighi di cui al presente atto, delle istruzioni impartite e della normativa vigente.

Il fornitore è altresì responsabile per ogni pregiudizio cagionato al Titolare .

Qualora il fornitore eroghi ulteriori servizi o espleti ulteriori attività per conto del Titolare del trattamento che non rientrano nel contratto oggetto della presente nomina, il medesimo sarà nominato con separato atto di nomina quale responsabile del trattamento.

Cembra Lisignago, 27 novembre 2023

FLOR INFORMATICA

Bruno Flor
2023.11.27 09:43:43
CN=Bruno Flor
C=IT
O=NON PRESENTE
2.5.4.46=20111116151363

IL PRESIDENTE DELLA COMUNITA' DELLA VALLE DI CEMBRA

Simone Santuari

santuari simone
27.11.2023 14:26:19 GMT+00:00