

Atto di nomina di Responsabile di Trattamento Dati e Amministratore di Sistema Informatico

Nell'ambito del presente contratto, l'Associazione Banca del Tempo TEMPO-TREZZO A.P.S. di Trezzo sull'Adda, in quanto titolare del trattamento dei dati inseriti dai singoli soci o importati in maniera massiva sul www.portaledeltempo.it designa:

SORINT.lab Spa

Responsabile del trattamento dei dati personali

Ai sensi dell'articolo 28 REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO (in seguito GDPR) del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

e

Amministratore del sito web www.portaledeltempo.it

Ai sensi del provvedimento Generale del Garante per la Protezione dei Dati Personali del 27 novembre 2008 e nell'ambito di quanto stabilito nel presente contratto l'Amministratore di Sistema viene designato quale figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti di dati personali.

La figura dell'Amministratore di sistema non è espressamente prevista dal GDPR e tale norma supera quanto previsto il D. Lgs. 30 giugno 2003 n. 196 e relativo Allegato B, che saranno comunque considerati come base di riferimento per una corretta gestione del sistema.

Materia disciplinata

La seguente nomina è valida ai fini di quanto previsto nel contratto.

Durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati.

Le parti danno atto e accettano quanto segue:

1. l'oggetto del trattamento è limitato ai Dati Personali che rientrano nell'ambito di applicazione del GDPR;
2. la durata del trattamento coinciderà con quanto stabilito in precedenza nel contratto. Il trattamento durerà inoltre fino a quando tutti i Dati Personali non saranno stati eliminati o restituiti in conformità alle istruzioni della Società o alle disposizioni riportate nel contratto;
3. la natura e lo scopo del trattamento consisteranno nell'erogare il Servizio contrattuale come stabilito in precedenza;
4. i tipi di Dati Personali trattati includono quelli espressamente indicati all'Articolo 4 del GDPR;
5. le categorie di interessati sono i rappresentanti e gli utenti finali della Banca del Tempo, ad esempio i soci, dipendenti, appaltatori, collaboratori e clienti.

In particolare, si chiede che come responsabile del trattamento, SORINT.lab, nella gestione del portale in oggetto:

- a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
- b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- c) adotti tutte le misure richieste ai sensi dell'articolo 32 del GDPR, prevedendo le misure minime come riportate di seguito;
- d) Il responsabile del trattamento è autorizzato a ricorrere a un altro responsabile del trattamento previa informazione al titolare del trattamento, comunicando anche nel seguito eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche;
- e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato previsti dal GDPR;
- f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli 32 e 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
- g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;
- h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

SORINT.lab nella qualità di Amministratore di Sistema ha il dovere di compiere quanto in suo potere nell'ambito del contratto e segnalare alle Banche del Tempo tutto quanto si renderà necessario ai fini del rispetto e della corretta applicazione del GDPR con particolare riferimento al profilo relativo alla sicurezza nella custodia e nel trattamento dei dati personali.

La designazione di SORINT.lab avviene in ragione del possesso in capo a quest'ultima dei requisiti di capacità tecniche, professionali e di condotta.

Nell'ambito dell'incarico ricevuto e limitatamente ai sistemi ed alla parte del processo di trattamento sotto suo controllo, all'amministratore di sistema spetta il compito di mettere in atto misure tecniche informatiche per garantire un livello di sicurezza adeguato al rischio (art. 32 del Regolamento UE 27 aprile 2016 n.679) sulla base delle indicazioni ricevute dal titolare dei trattamenti.

Le "misure adeguate" sono definite sulla base di un'analisi del rischio da effettuare con il responsabile di trattamento sulla base dei rischi.

Ove possibile si implementeranno o si consiglierà l'implementazione per Software di terze parti di tecniche di cifratura dei dati, tecniche di ripristino in caso di incidenti e verifiche periodiche delle misure tecniche

adottate con soluzioni "privacy by design" e "privacy by default" – di cui all'art. 25 del medesimo Regolamento UE.

In accordo con le singole Banche del Tempo si definiranno e gestiranno le procedure per l'eventuale violazione o perdita dei dati, accidentale od intenzionale prevedendo sistemi di controllo per la sicurezza informatica volte a garanzia della struttura.

Specificatamente, l'Amministratore di Sistema sarà tenuto a gestire le seguenti attività:

1. Importazione dei dati utente delle nuove banche del Tempo (da foglio di calcolo Excel).
2. Accesso all'anagrafica utenti per reset password in seguito a eventuali problematiche di accesso.
3. Accesso all'elenco delle transazioni effettuate al fine di conciliare eventuali cancellazioni non registrate.

Garantendo i seguenti standard di sicurezza dei dati:

1. Connessione all'applicazione protetta da crittografia SSL/TLS.
2. Accesso alle utenze controllato e subordinato all'immissione delle credenziali di accesso (indirizzo e-mail e password).
3. Le credenziali di accesso degli utenti sono immagazzinate in modo sicuro nel database (password sotto forma di hash crittografico con salt casuale).
4. Backup giornaliero dei dati. I backup vengono conservati per 7 giorni.

L'Amministratore di Sistema si impegna inoltre a:

1. Predisporre in contraddittorio con il Titolare dei trattamenti, un piano di controlli periodici, da eseguirsi con cadenza almeno semestrale, atti a verificare l'efficacia delle misure di sicurezza adottate.
2. Coadiuvare, se richiesto, il Titolare del trattamento nella Valutazione dei Rischi e nella Valutazione d'Impatto (DPIA)

Comunicazione di Eventi Imprevisti relativi alla Protezione (DATA BREACH)

Qualora SORINT.lab venga a conoscenza di un inadempimento della sicurezza con conseguente distruzione, perdita, alterazione accidentale o illegale, divulgazione non autorizzata dei Dati della Società o dei Dati Personali oppure accesso ad essi non autorizzato durante il trattamento da parte di SORINT.lab (ciascuno un "Evento Imprevisto relativo alla Protezione"), SORINT.lab adotterà tempestivamente e senza ingiustificato ritardo le seguenti azioni:

1. comunicherà alla Banca del Tempo l'Evento Imprevisto relativo alla Protezione;
2. analizzerà l'Evento Imprevisto relativo alla Protezione e fornirà alla Società informazioni dettagliate riguardo ad esso;
3. adotterà misure ragionevoli per mitigare gli effetti e ridurre eventuali danni derivanti da esso.

Le notifiche degli Eventi Imprevisti relativi alla Protezione verranno trasmesse alle Banche del tempo inviando una e-mail all'indirizzo: bdt@tempotrezzo.it.

SORINT.lab porrà in essere ogni sforzo ragionevole per aiutare la Banca del tempo ad adempiere all'obbligazione ai sensi dell'Articolo 33 del GDPR o di altra legge o altro regolamento applicabile, di comunicare all'autorità di controllo e agli interessati specifici tale Evento Imprevisto relativo alla Protezione.

L'obbligo di SORINT.lab di segnalare un Evento Imprevisto relativo alla Protezione o di rispondere ad esso ai sensi del presente Articolo non costituisce un'ammissione di responsabilità rispetto a tale evento.

La Banca del tempo dovrà comunicare tempestivamente a SORINT.lab eventuali utilizzi impropri degli account o delle credenziali di autenticazione oppure eventuali Eventi Imprevisti riguardanti un Servizio Online.

Monitoraggio

È compito dell'Amministratore di Sistema monitorare costantemente lo stato di sicurezza di tutti i processi di elaborazione dati di cui sopra, mantenendo aggiornati tutti i supporti hardware e software e, se del caso, comunicando al Titolare tutte le attività da porre in essere al fine di garantire un adeguato livello di sicurezza in proporzione alla tipologia e quantità dei dati personali trattati.

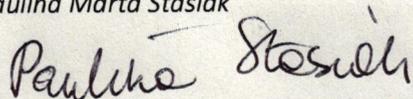
L'operato dell'Amministratore di Sistema sarà oggetto, con cadenza annuale, ad una attività di verifica da parte del cliente, tesa a controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previsti dalle norme vigenti.

BANCA DEL TEMPO TEMPO-TREZZO A.P.S.



Il Rappresentante pro tempore

Paulina Marta Stasiak



Trezzo sull'Adda, 20/11/2020

Per Accettazione

dell'Atto di nomina di Responsabile di Trattamento Dati e Amministratore di Sistema informatico.



Il Rappresentante

Luogo,

Data: .../.../.....