SIRIO Informatica s.a.s.
V.le A. De Gasperi, 98
63074 San Benedetto del Tronto
C. FISC. e P. IVA 01.565.770.441
http://www.SIRIOInformatica.it
info@SIRIOInformatica.it

TGSPEEDY: DICHIARAZIONE DI CONFORMITÀ AL GDPR

REGOLAMENTO EUROPEO SULLA PROTEZIONE DEI DATI 679/2016

REV. 3 DEL 12/12/2020

Il Regolamento Europeo GDPR 679/2016 costituisce la normativa di riferimento dello Stato italiano per la regolamentazione del trattamento dei dati personali ed impone una serie di obblighi, in capo a chi tratta informazioni riferite ad altri soggetti, al fine del rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Il presente documento costituisce la dichiarazione di conformità del software *TGSpeedy* prodotto da *SIRIO Informatica sas* alla normativa europea *GDPR*.

La *SIRIO Informatica sas* si avvale di un team trasversale di specialisti della protezione dei dati composto da consulenti legali, professionisti della sicurezza e della conformità. Il nostro team ha quindi completato una valutazione completa delle nostre attuali pratiche di sicurezza e protezione dei dati rispetto alle disposizioni del GDPR.

CONTROLLI: procedure interne

Adottiamo misure esaustive per proteggere la nostra infrastruttura, la nostra rete e le nostre applicazioni, formare i dipendenti sulle pratiche in ambito di sicurezza e privacy e costruire una cultura in cui conquistare la fiducia dei clienti è la massima priorità. Di seguito sono descritte in dettaglio alcune delle nostre misure di controllo.

Formazione

Parte della garanzia di protezione dei dati personali dei nostri utenti consiste nel diffondere e favorire la conoscenza delle nozioni di sicurezza e privacy. A questo proposito, ai dipendenti viene richiesta l'accettazione delle norme di sicurezza, incluse le Norme sulla privacy dei dati, prima ancora di ottenere l'autorizzazione ad accedere ai sistemi. Inoltre, i dipendenti partecipano a corsi di formazione obbligatori sulla sicurezza e sulla privacy per i nuovi assunti, oltre alla formazione annuale di follow-up e a una

sensibilizzazione continua su tali temi mediante e-mail informative, conferenze, presentazioni e risorse disponibili sulla *Rete Internet*.

Richieste di accesso a dati personali

Gli interessati, come previsto dal Regolamento Europeo, hanno la possibilità di richiedere l'accesso o la cancellazione dei dati personali raccolti su di loro. Ulteriori informazioni su questo processo sono disponibili facendone richiesta.

Soggetti terzi e collaboratori esterni

La nostra azienda gestisce in prima persona le attività relative alla fornitura dei propri servizi e alla relativa manutenzione. Eventuali necessità di accesso ai dati da parte di soggetti terzi la cui autorizzazione è prevista dal Regolamento Europeo, viene regolamentata attraverso la stesura di un documento di impegno di responsabilità e viene comunicato al Titolare dell'Informazione l'evento necessario. L'accesso viene sempre compiuto in conformità alle nostre procedure interne, assicurando la massima trasparenza e sicurezza dell'intervento.

MODELLO ORGANIZZATIVO

1 **Gestione e sicurezza delle informazioni organizzative**

1.1 **Gestione del rischio**: L'azienda ha individuato un processo per identificare, valutare e gestire i rischi legati alla sicurezza delle informazioni, e garantisce che i rischi sulla sicurezza delle informazioni vengano valutati e gestiti correttamente. Prima di stabilire il livello di protezione necessario l'azienda, ha controllato i dati personali che raccoglie e tratta in modo da valutare i rischi legati a queste informazioni.

1.2 **Politica di sicurezza**: un documento interno consente al personale di adottare le migliori procedure su tematiche tecniche legate alla sicurezza delle

informazioni in base alle esigenze aziendali, alle leggi e regolamenti in vigore. L'informativa consente di affrontare in modo coerente i rischi legati alla sicurezza e fa parte di una politica generale di protezione dei dati personali

1.3 **Responsabilità della sicurezza dell'informazione**: la *SIRIO Informatica sas* ha definito e assegnato le responsabilità legate alla sicurezza delle informazioni e ha individuato chi si occuperà del coordinamento e revisione dell'implementazione dell'informativa sulla sicurezza dei dati.

1.4 **Outsourcing**: consulenza e revisione degli accordi con fornitori di servizi di terze parti, che prevedono condizioni di sicurezza adeguate al trattamento dei dati personali. In questo modo l'azienda può garantire la protezione dei dati personali accessibili da fornitori terzi.

1.5 **Gestione degli incidenti**: la *SIRIO Informatica sas* ha individuato un processo adeguato a segnalare e recuperare le informazioni in caso di una violazione della sicurezza dei dati. Possiamo garantire la gestione adeguata delle violazioni alla sicurezza dei dati, inclusa la comunicazione di eventi che mettono a rischio la sicurezza delle informazioni. Le violazioni della sicurezza dei dati possono derivare da un furto, un attacco ai sistemi, l'uso non autorizzato di dati personali da parte di un membro dello staff, da perdita accidentale o guasto di una apparecchiatura.

2 Consapevolezza del personale sulla sicurezza delle informazioni

2.1 **Formazione e sensibilizzazione del personale anche tramite campagne interne di promozione**: l'azienda organizza corsi di formazione sulla sicurezza dei dati, inclusi i corsi dedicati al personale. Ci assicuriamo che dipendenti e fornitori rispettino e siano consapevoli delle loro responsabilità in materia di sicurezza dei dati. Il personale con responsabilità specifiche in materia di

sicurezza o con accesso privilegiato ai sistemi di sicurezza aziendali è adeguatamente formato e qualificato.

3 Sicurezza Fisica

3.1 *Protezione edifici e locali fisici*: l'azienda ha individuato determinati controlli di accesso per limitare l'accesso a locali e attrezzature, in modo da impedire l'accesso fisico, il danneggiamento e l'interferenza con i dati personali.

3.2 *Misure fisiche in atto negli uffici*: nelle sedi operative sono attive le seguenti misure di sicurezza relative alla intera struttura, per contrastare le minacce e i possibili impatti:

Accesso fisico dall'esterno	Custode – Sistemi di allarme – Sistemi di Video Sorveglianza – Identificazione biometrica – Sistemi fisici di anti-intrusione
Incendio	Estintori – Sistemi di Allarme – Ambienti *tagliafuoco*
Guasto Impianto Elettrico	Gruppo i continuità - Messa a terra con revisione - Revisione periodica
Guasto impianto condizionamento	Manutenzioni periodiche – Sistemi di allarme
Accessi interni	Uffici presidiati – politiche interne vietano la trascrizione su carta di informazioni che possono mettere a rischio la sicurezza del sistema
Perdita o distruzione dati	Procedure Disaster Recovery – Backup e ridondanze cluster

3.3 *Smaltimento sicuro*: l'azienda ha individuato un processo per cancellare in modo sicuro i dati e le attrezzature quando non sono più necessari. Tutto il personale dispone di attrezzature che consentono la cancellazione permanente delle informazioni e la distruzione irreversibile di materiale fisico.

4 Misure di sicurezza *Cloud* e Applicativo Client *TGSpeedy*

4.1 Gli incaricati vengono identificati da un codice utente ed una password. In particolare: la password è modificata dall'incaricato al primo utilizzo e, successivamente, per un tempo programmabile dall'utilizzatore. Viene fornita all'utente la possibilità di imporre password complesse in conformità a quanto stabilito dal GDPR.

4.2 E' possibile procedere alla disattivazione automatica degli account dopo un periodo di inutilizzo prolungato degli stessi.

4.3 Il sistema prevede la notifica all'amministratore di sistema di tentativi di accesso non andati a buon fine, o che vengono eseguiti al di fuori delle restrizioni di indirizzi IP consentiti.

4.4 E' possibile creare restrizioni di utilizzo delle varie funzioni del software, in modo da discriminare l'accesso alle informazioni personali in base al principio di competenza.

4.5 In seguito ad un periodo di inutilizzo dell'interfaccia utente, è possibile prevedere il blocco automatico della postazione di lavoro, con l'oscuramento delle eventuali finestre aperte.

4.6 Essendo *TGSpeedy* un sistema in *Cloud*, i dati vengono archiviati e resi disponibili attraverso i nostri DataCenter. La nostra Server-Farm, è suddivisa tra la sede operativa di Arezzo (AR) e quella di *San Benedetto del Tronto (AP)*. Sistemi di ridondanza e di backup periodici garantiscono la conservazione dei dati in conformità a quanto stabilito dal *GDPR*.

4.7 La comunicazione tra postazione di lavoro del Cliente e Server-Farm di *TGSpeedy*, avviene attraverso l'utilizzo di un algoritmo di crittografia proprietario

ed appositamente concepito da *SIRIO Informatica sas* e tramite il protocollo *HTTPS SSL.* Informazioni sensibili come password o codici fiscali vengono archiviate in modo crittografato SHA256.

4.8 Le informazioni personali inviate dal sistema *TGSpeedy* tramite allegati email, possono essere protette facendo uso di collegamenti il cui accesso è protetto da password, nel rispetto della normativa prevista dal *GDPR*.

SIRIO Informatica sas

Marcello Colucci