Policy di gestione e conservazione dei dati di proprietà dei clienti

In questo documento vengono illustrate le policy e le procedure che utilizza Tempo srl per la conservazione e la gestione dei dati di proprietà dei clienti, durante il periodo di servizio.

Modalità in cui i dati vengono conservati ed eventualmente archiviati

I dati presenti all'interno degli applicativi, gestiti in modalità SaaS, messi a disposizione da parte di Tempo srl sono sempre salvati sul cloud di Aruba (https://www.cloud.it/), a meno di esplicita indicazione concordata nel contratto. In quest'ultimo caso sono definite separatamente anche le procedure di eliminazione.

I suddetti dati possono essere contenuti in:

- Tabelle di Database (es.: Microsoft SQL Server) o analogo (es.: DynamoDB, Redshift, etc.);
- File (es. nel caso delle fatture elettroniche o dei log delle chiamate ricevute dai WS);

Nello specifico per quanto riguarda il database dell'applicativo Easy:

1. Sono presenti backup giornalieri mantenuti per 14gg monitorati con procedura automatica;
2. Sono presenti backup orari dalle ore 9 alle ore 19 (periodo tipico di attività dei ns clienti)
3. Ogni cliente accede ad un proprio database. Non esistono database condivisi;
4. I log degli applicativi memorizzati all'interno dello stesso database che contiene i dati operazionali.
5. I backup giornalieri vengono anche replicati settimanalmente, previa criptazione, su Amazon Glacier.

Misure di sicurezza predisposte in caso di accesso non autorizzato

Per prevenire accessi non autorizzati vengono utilizzate accessi personali, distinti per ogni dipendente della Tempo Srl, per l'accesso ai server, che per ogni cliente per l'accesso ai servizi. Gli operatori di Help Desk possono accedere ai dati per verificare eventuali richieste di assistenza ricevute dai clienti.

1. Ogni server possiede un log degli accessi utilizzabile per un'indagine iniziale;
2. Ogni giorno in maniera automatizzata viene recapitata via mail il log degli accessi falliti ai referenti tecnici della Tempo Srl per la verifica di anomalie.
3. Tempo srl programma periodici Application Penetration test e Network Penetration test (sia dall'interno che dall'esterno della rete) per garantire la sicurezza dell'infrastruttura.

Presenza di strumenti per monitorare i livelli di sicurezza dei dati

La sicurezza del dato è garantita tramite versioning su S3 e backup su EBS. In aggiunta è in essere una Procedura di verifica annuale dei backup. Per DSpace in particolare i dati vengono monitorati tramite procedura automatica per la verifica della consistenza tra i Bucket S3 e l'hash precedentemente salvato su database.

Tutte le macchine virtuali del Private Cloud di Tempo Srl sono protette dal firewall pfSense, il quale produce log automatizzati per il monitoraggio della sicurezza dei dati.

Periodicamente vengono effettuate analisi dei log prodotti dai dispositivi di monitoraggio per il rilevamento di pattern sospetti e/o eventi ripetuti, che possano evidenziare attività malevoli.

Lo staff tecnico di Tempo srl ha accesso completo ai dati per poter erogare i servizi concordati con il cliente. É inoltre possibile, tramite i vari applicativi, definire il livello di accesso esterno ai dati utilizzando funzionalità specifiche.

Tempistiche e modalità con cui vengono gestite e comunicate le eventuali violazioni dei dati

- *Se vi è un data breach interno* (se la violazione avviene internamente all'impresa, quindi sui dati che Tempo srl tratta direttamente): In questo caso il soggetto autorizzato deve dare tempestiva comunicazione per scritto al titolare del trattamento, descrivendo anche ciò che ha rilevato, la tipologia di breach e la quantità di dati coinvolti, le circostanze in cui il breach si è verificato e di come ne è venuto a conoscenza e le azioni da lui adottate al fine di limitare i danni o interrompere il breach. L'avviso è, quindi, tempestivo, avviene non appena l'autorizzato scopre la violazione. Il titolare poi comunica al Garante, qualora ne ricorrano i presupposti, entro 72 ore dal momento in cui è venuto a conoscenza della violazione.
- *Se vi è un data breach esterno* (se la violazione avviene su dati di cui noi siamo titolari, ma sono affidati ad un responsabile esterno): Il responsabile esterno del trattamento è obbligato a comunicare tempestivamente e senza ingiustificato ritardo (non più tardi di 12 ore) la violazione al titolare del trattamento, sia tramite e-mail che tramite pec.

Modalità attraverso cui è possibile restringere l'accesso ai dati

Le politiche di sicurezza per restringere l'accesso ai dati sono gestite a livello applicativo.

Esiste un pannello di configurazione a cui può accedere il gruppo degli utenti che per il cliente ha i diritti amministrativi. Quando il cliente richiede gestioni personalizzate per la restrizione dell'accesso ai dati è possibile creare dei filtri realizzati attraverso un linguaggio di scripting like-Sql in modo da rendere l'accesso ai dati parametrico in base alle condizioni definite d'accordo con il cliente.

Coperture assicurative in relazione al rischio privacy

La Società è munita di assicurazione R.C. Professionale "Rischi Diversi" che comprende, in particolare:

"*L'assicurazione si obbliga a tenere indenne Tempo srl di quanto questi sia tenuto a risarcire quale civilmente obbligato ai sensi di legge, a titolo di risarcimento del danno cagionato a terzi in conseguenza dell'attività professionale esercitata. Quest'ultima è relativa alla fornitura di soluzioni integrate nel campo dell' IT, nell'offerta di soluzioni, prodotti e/o servizi di sicurezza, di integrazione e di centralizzazione delle applicazioni; nonché nell'offerta di prodotti consulenziali nell'area dello sviluppo software, nella fornitura di servizi e di consulenza per l' e-commerce, il datawarehouse e per la realizzazione di applicazioni internet.*”