Misure di sicurezza di un’applicazione web per essere conformi al GDPR

Nella gestione della privacy di un’organizzazione talvolta ci si trova a valutare la conformità al GDPR (Regolamento UE 2016/679) di una applicazione web o *web application* fornita, spesso con modalità SaaS (Software As A Service) da un fornitore esterno.

Da un lato l’art. 28 del GDPR ci chiede di affidarci solo a **responsabili del trattamento** che garantiscano **adeguate misure di sicurezza** e la conformità al GDPR stesso, dall’altro l’art. 25 ci chiede che gli applicativi software che trattano dati personali siano “***privacy by design***” e “***privacy by default***”, ma cosa significa tutto ciò? Cosa dobbiamo realmente chiedere al fornitore di una *web application*? Anzi cosa dobbiamo pretendere per garantirci la conformità al GDPR?

Al di là degli obblighi del GDPR, molti imprenditori si pongono queste domande:

1. Dove sono conservati i miei dati?
2. Chi li può visionare?
3. Saranno sempre nella mia disponibilità?

Le responsabilità in capo al Titolare del trattamento in caso di violazione dei dati personali gestiti attraverso un sito web sono pesanti se esso non ha provveduto, da un lato a garantirsi contrattualmente la conformità del responsabile del trattamento e dall’altro ad assicurarsi che l’applicazione web sia adeguatamente sicura. In pratica il titolare rischia di essere accusato di “*culpa in eligendo*” e “*culpa in vigilando*”, relativamente al rapporto con il responsabile del trattamento.

Il più elevato livello di garanzie che un titolare del trattamento può ottenere è la certificazione ai sensi dell’articolo 42 (e 43) del gdpr del fornitore responsabile del trattamento per il prodotto utilizzato. Al momento tale certificazione non è

ancora pienamente disponibile, ma manca veramente poco perché i primi schemi di certificazione ai sensi dell'articolo 42 del GDPR siano abilitati da Accredia (o da altri enti di accreditamento europei mutuamente riconosciuti nella UE) attraverso l'accreditamento dei primi Organismi di Certificazione ai sensi della norma ISO 17065 per la certificazione del GDPR. Ad esempio, lo schema ISDP©10003 è l'unico schema di certificazione italiano accreditato e, quindi, potrà costituire uno strumento per poter **certificare processi, prodotti o servizi** sotto **accreditamento ISO 17065** e, quindi, **certificare la conformità di un prodotto software** come un applicativo web al Regolamento Europeo sulla Protezione dei Dati Personali 679/2016.

Ma in assenza di un prodotto software certificato quali sono i requisiti di sicurezza che possiamo ragionevolmente richiedere ad una *web application* si tratta dati personali di dipendenti, clienti e fornitori dell'organizzazione titolare del trattamento?

Vediamo un elenco non esaustivo di possibili misure di sicurezza, suddivise per categorie.

1. Controllo degli accessi: il sistema web deve prevedere un'autenticazione mediante credenziali del tipo *username* e *password* univoche (o rese tali). Devono essere implementati criteri di sicurezza per le password come ad esempio una lunghezza minima (almeno 8 caratteri sono indispensabili), una complessità minima della password (ad esempio potrebbe essere richiesta la presenza di almeno un carattere alfabetico maiuscolo, alfabetico minuscolo, un numero ed un carattere speciale), la password dovrebbe essere cambiata al primo accesso dell'utente e a frequenza prestabilita, sebbene la variazione della password non sia più un *must* della sicurezza informatica; infatti sistemi come l'autentificazione a due fattori richiesta anche saltuariamente (ad esempio in caso di collegamento da un nuovo dispositivo) potrebbe rendere maggiormente sicuro il portale web. Poi dovrebbe comunque essere impedito l'accesso contemporaneo con il medesimo codice utente da due dispositivi differenti. Inoltre, l'utente dovrebbe essere automaticamente scollegato dalla sessione dopo un certo periodo di tempo. Infine, le password dovrebbero essere mantenute in forma cifrata nel database dell'applicativo per evitare hacker possano appropriarsi delle credenziali degli utenti.
2. Anti-malware: il portale web dovrebbe implementare sistemi antivirus attivi e firewall per contrastare eventuali attacchi dall'esterno.
3. Profilazione degli utenti: tutti gli utenti dovrebbero avere accesso alle sole risorse di cui necessitano e le utenze amministrative ovvero quelle di amministratore di sistema dovrebbero essere utilizzate soltanto per necessità specifiche.
4. Log degli accessi: dovrebbe essere implementato un sistema di raccolta di *log* degli accessi degli amministratori di sistema (mantenuti almeno sei mesi in formato non modificabile come richiesto dal provvedimento del Garante Privacy) e degli utenti.
5. Aggiornamento software: dovrebbero essere mantenuti costantemente aggiornati

contro minacce alla sicurezza i sistemi operativi ed i software di base della piattaforma nella quale opera l'applicativo web; dunque aggiornamenti costanti delle versioni di mySQL, PHP ed Apache nella piattaforma open source LAMP, aggiornamenti di MSSQL e relativi componenti software della piattaforma Microsoft, ecc..

6. Comunicazioni sicure: le connessioni fra client e web devono essere crittografate (protocollo SSL/TLS) con certificati validi, prassi ormai consolidata per siti web che applicano le connessioni "https".
7. Politica di backup: dovrebbe essere attuata una *policy* di backup adeguata alle esigenze di disponibilità dei dati, in termini di tempi di ripristino dei dati e massima perdita dei dati ammissibile. I tempi di *retention* dei backup dovrebbero essere coerenti con le esigenze di ripristino di dati passati ed eventuali cancellazioni. Le copie di backup dovrebbero essere protette contro il *ransomware*, attraverso cifratura, conservazione off-line, esecuzione dei backup con profili utente separati. Per garantirsi contro disastri ambientali e causati dall'uomo almeno una copia di backup periodica dovrebbe essere conservata in un'ubicazione remota (oltre 50-100 km dal datacenter).
8. Disaster recovery: il fornitore dei servizi cloud dove è installato l'applicativo dovrebbe fornire un piano di *disaster recovery* adeguato alle esigenze dell'organizzazione cliente.
9. Piano di Business Continuity: il fornitore dei servizi cloud deve prevedere un piano di continuità operativa che contempli, oltre al piano di DR, contromisure per garantire la disponibilità dei servizi a fronte di disastri ed altre situazioni di crisi non legate all'infrastruttura IT (come ad es. una pandemia, un incendio, un'alluvione, un terremoto, ecc.).
10. Monitoraggio di log di accesso e sistemi antintrusione: dovrebbero essere implementate attività di monitoraggio dei log di accesso degli utenti e degli amministratori e di sistemi antintrusione (*Intrusion Prevention System*) e dei relativi log.
11. Sicurezza fisica ed ambientale del datacenter: il datacenter ove risiede il cloud dell'applicativo dovrebbe essere dotato di misure di sicurezza fisica ed ambientale come impianti antincendio e antiallagamento, sistemi di allarme e di videosorveglianza, controllo degli accessi fisici del personale, ecc..
12. Sicurezza informatica del datacenter: devono essere previste, a protezione dei dati ,misure quali firewall e anti-malware, gestione delle utenze amministrative/privilegiate e MFA sulla piattaforma cloud, monitoraggi/audit sulla sicurezza, censimento degli asset, ecc..
13. Sicurezza delle apparecchiature e dei servizi accessori: l'infrastruttura del datacenter deve essere dotata di adeguati sistemi di raffreddamento, sicurezza fisica dei cablaggi, misure di alimentazione di emergenza quali gruppi elettrogeni, ecc..
14. Conformità al GDPR dell'ubicazione del datacenter: i dati personali conservati in cloud dovrebbero comunque risiedere all'interno della UE o in un Paese per il quale esistono adeguate garanzie secondo quanto previsto dal Reg. UE 679/2016 e dalla Commissione Europea.

In sé la *web application* dovrebbe essere progettata con maschere video e funzioni che permettano di gestire il minor numero di dati personali possibile, consentendo agli utenti di visionare solo i dati effettivamente necessari per operare e prevedere la pseudonimizzazione dei dati nelle tabelle del database, separando i dati più sensibili dagli altri e rendendoli associabili all'individuo attraverso codici anonimi. Questi aspetti richiedono, però, una progettazione dell'applicativo già orientata alla protezione dei dati personali ed ai principi del GDPR, cosa non certo comune.

Naturalmente ognuna di queste misure di sicurezza potrà rivestire un'importanza diversa a seconda del tipo di dati gestiti nell'applicativo in cloud e della loro importanza o valore in termini di Riservatezza, Integrità e Disponibilità.

In conclusione, prima di adottare un software web per trattare dati riservati occorre esaminare bene anche questi aspetti per non trovarsi cattive sorprese in futuro.