DIGITAL HEALTH ITALIA

MAGGIO 2018 - POV

Conformità alla normativa GDPR per Start-up Digital Health

PERCHÈ LE STARTUP DIGITAL HEALTH SI DEVONO PREOCCUPARE DELLA GDPR?

Per la loro stessa natura, le applicazioni nel Digital Health raccolgono una categoria di dati speciali (anche detti sensibili), la quale è strettamente regolamentata, e implica un'importante responsabilità legale, per esempio: **la responsabilità criminale per i rappresentati aziendali**.

È dunque di fondamentale importanza per le aziende operanti in questo settore essere conformi a tutti quei requisiti amministrativi e tecnici, definiti dalla normativa sulla protezione dei dati (UE GDPR), in modo da non incorrere nel rischio di violazione e perdite di dati, o altre invasioni della privacy dell'utente.

Alcuni fatti:

Sanzioni: Il mancato rispetto delle regole GDPR in Europa può costare alle aziende fino al 4% del loro fatturato globale o 20 milioni di euro. La regolamentazione americana HIPAA prevede, invece, una sanzione di 225 dollari per ogni documento violato.

L'avanguardia: Negli ultimi 3 anni, studi hanno dimostrato che gli sviluppatori hanno faticato ad adeguarsi alla norma: un 85% non sono conformi e un 66% non usa ancora l'HTTPS. Queste mancanze mettono a rischio i dati personali delle persone, gli eHealth business e l'affidabilità riposta in essi.

QUALI SONO I DATI SANITARI?

L'Art. 4(15) della GDPR definisci i dati sanitari come "i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute".

Oltre ai quelli sanitari, la categoria dei dati sensibili ne include altri, fra i quali quelli che riguardano: la razza o l'origine etica, l'idea politica, religiosa o di altre credenze, l'appartenenza ad un sindacato, le biometriche che definiscono una persona, la genetica e le informazioni relative ai reati o condanne.

In alcuni casi è difficile mettere in pratica questa definizione con applicazioni reali, che siano differenti da quelle puramente sanitarie, ma legate piuttosto al benessere, alla salute, alla gestione della dieta o dell'attività fisica.

In questi frangenti gli sviluppatori posso avvalersi di un consulto specialistico per capire se trattano con dati sensibili oppure no.

Per avere più informazioni al riguardo puoi dare un occhio a questo eBook:
https://chino.io/static/content/Chino.io-Decision-Tree-on-Sensitive-Data.pdf

PERCHÈ PER LE STARTUP DIGITAL HEALTH È DI VITALE IMPORTANZA DIMOSTRARE LA CONFORMITÀ?

Il sistema sanitario è caratterizzato da un insieme molto complesso di parti interessate. Tipicamente l'utente finale non è il cliente stesso, il quale può essere un ospedale, un'assicurazione, una casa farmaceutica, o un altro servizio pubblico o privato.

Per ognuno di essi le start-up devono dimostrare sicurezza, qualità, conformità e affidabilità. Ospedali, assicurazioni o altri partner si rifiutano di lavorare con aziende che non dimostrano sufficiente sicurezza e maturità su questo argomento. Inoltre, recenti studi hanno dimostrato che al 59% delle persone non piace condividere i propri dati online, mentre altri hanno criticato l'incapacità di alcune applicazione nel mantenere i benefit promessi.

Infine, gli investitori e le autorità incaricate della protezione dei dati possono richiedere documenti aggiuntivi nel caso di violazione degli stessi o in caso di negligenza nel processo di trattamento.

QUALE È IL PROCESSO NECESSARIO DA PARTE DELLE AZIENDE DIGITAL HEALTH PER GARANTIRE LA CONFORMITÀ ALLA NORMA?

La maggior parte dei requisiti della norma GDPR si applicano alle aziende Digital Health nella stessa maniera di altri tipi di business (e-commerce, Finanziario, etc.), tuttavia, **alcuni di essi risultano essere più impegnativi da rispettare per gli sviluppatori**.

IL CONSENSO

Secondo la norma, il trattamento dei dati sanitari è proibito, a meno che essi non vengano trattati secondo uno dei sei metodi che ne determinano la conformità. Fra questi, quello più utilizzato nel processo è il "**consenso esplicito**", il quale è tipicamente integrato attraverso le caselle di spunta nel sito web o nella app, durante la fase di registrazione.

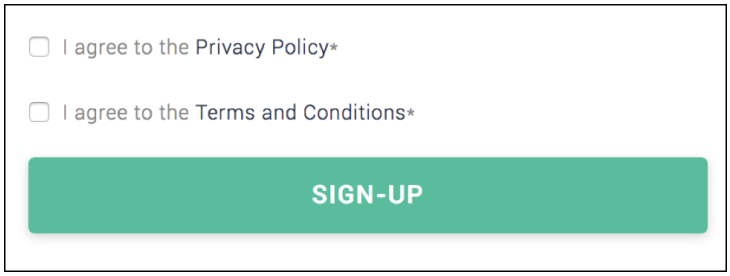
Le Aziende devono prestare particolare attenzione in questo processo e nell'implementazione del metodo con il fine di ottenere un consenso valido, che viene definito come specifico, informato, granulare, ricevuto liberamente ed esplicitamente indicato nell'accordo per il trattamento dei dati dell'interessato.

Questo qui presente è un esempio calzante (preso da un sito web italiano) di un **consenso non valido**, né tantomeno con la vecchia direttiva.

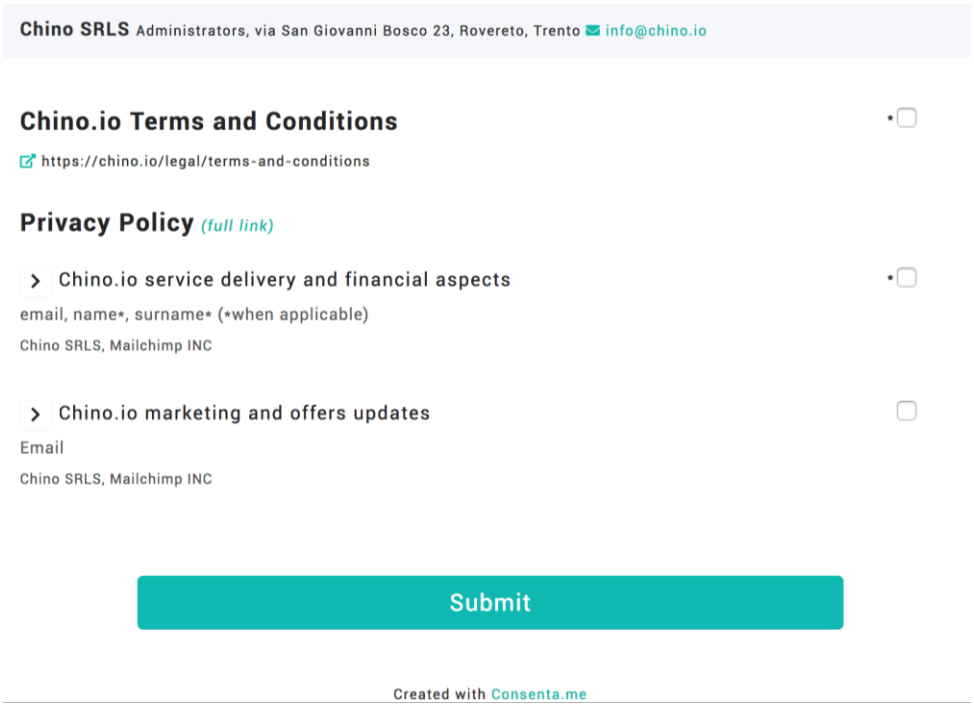
Il seguente esempio è migliore, ma non completo e dunque non valido in quanto:

+ Non è granulare, dato che è necessario accettare tutti i termini e policy per l'utilizzo del servizio, compreso quelli di marketing.

+ Non è informato, dato che è necessario cliccare sul policy link e leggere la terminologia legale per capire come verranno trattati i tuoi dati.



Conformemente alle migliori prassi, il modulo di consenso deve contenere le informazioni complete riguardanti il preposto al trattamento dei dati e deve essere strutturato come quanto segue:



Oltre a mostrare correttamente le informazioni, gli sviluppatori devono fornire una prova del fatto che le persone interessate abbiano dato il loro consenso legalmente. Ciò significa che devono tenere traccia di consensi, aggiornamenti, prelievi ed essere in grado di dimostrare la loro conformità se richiesto dall'autorità di vigilanza.

VALUTAZIONE D'IMPATTO DELLA PROTEZIONE DEI DATI (DPIA)

La valutazione d'impatto (detta anche DPIA, acronimo del nominativo inglese "Data Protection Impact Assessment") è un documento che dimostra che sia stata compiuta una valutazione del rischio e che siano state identificate le misure necessarie per la conformità con le disposizioni del GDPR e che dunque il business non rappresenti un rischio per l'utente.

Seguendo un approccio basato sul rischio e analizzando la natura, l'ambito, il contesto e lo scopo del processo di gestione, saremo in grado di determinare quale sia il livello di rischio del business e quali siano i potenziali effetti sulla protezione dei dati e, più in generale, sui diritti e le libertà dei cittadini dell'UE.

La miglior risorsa che offre una linea guida ufficiale e chiara riguardo la DPIA è l'Art. 29 "Gruppo di lavoro". Esso definisce i requisiti necessari per la valutazione d'impatto (in quanto non tutte le aziende sono tenute a eseguirla) e come eseguirla. Si consiglia di leggere il documento e consultare uno specialista per capire se sia il caso di eseguire la DPIA.

Se essa dovessero essere condotta dall'azienda, si esegua una DPIA che sia basata sui rischi specifici dell'azienda. La stessa può essere eseguita da qualsiasi persona o organizzazione interna o esterna, se esplicitamente nominata..

IL RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO)

Il responsabile della protezione dei dati (detto anche DPO, acronimo del nominativo inglese "Data Protection Officer") è una nuova figura professionale introdotta dal GDPR, egli è responsabile della direzione e della supervisione delle attività di protezione dei dati in un'organizzazione. La comanda di un DPO all'interno dell'azienda è obbligatoria se:

+ le attività principali del processo di gestione richiedono un monitoraggio regolare e sistematico su larga scala del soggetto dei dati;
+ le attività principiali riguardo l'elaborazione su larga scala di speciali categorie di dati, esempio quelli sanitario (Art. 9 GDPR).

Alcuni dei compiti del responsabile della protezione dei dati:

+ Formare sul tema della privacy; informare e consigliare il controllore o il responsabile e i lavoratori riguardo alla questione della privacy; identificare i requisiti attuali per la conformità alla privacy, esempi: legge, giurisprudenza, codice, etc.
+ Fornire consigli dove richiesto sulla valutazione d'impatto della protezione dei dati e monitorare la sua prestazione ai sensi dell'Art. 35; conservare le line guida e i modelli della DPIA.
+ Mantenere le registrazioni del meccanismo di trasferimento utilizzato per i flussi dati transfrontalieri: clausole contrattuali standard, regole aziendali vincolanti e approvazioni dei regolatori.

Come azienda sanitaria che elabora dati sensibili per la salute potrebbe essere necessario nominare un DPO.

Ulteriori linee guida potrebbero essere fornite dalle interpretazioni più recenti su questo aspetto, che considerano le dimensioni dell'azienda ed altri. Pertanto, si consiglia di controllare le linee guida o contattare uno o più avvocati per le ultime interpretazioni.

MISURE TECNICHE E DI SICUREZZA

L'aspetto **più importante e allo stesso tempo più difficile** da attuare per dimostrare la conformità con la GDPR e la vecchia direttiva è l'implementazione di misure tecniche e di sicurezza.

In particolare, le applicazioni sanitarie richiedono la massima sicurezza possibile a causa della sensibilità dei dati gestiti e della complessità del settore.

Questi sono alcuni dei principi e suggerimenti da cui cominciare:

+ Privacy e sicurezza in base alla progettazione e per impostazione predefinita
+ Crittografia
+ Pseudonimizzazione

La privacy e la sicurezza secondo i principi di progettazione sono approcci di ingegneria di sistema che tengono conto della privacy e della sicurezza durante l'intero sviluppo di un progetto, servizio o prodotto (articolo 25, paragrafo 1, del GDPR).

La privacy e la sicurezza in base alla progettazione richiedono agli sviluppatori "l'implementazione di appropriate misure tecniche e organizzative" (come **crittografia** e **pseudonimizzazione**) in modo efficace "al momento della determinazione dei mezzi per il trattamento e al momento dell'elaborazione stessa". L'obbiettivo finale è quello di attuare "l'implementazione dei principi di protezione dei dati" dall'inizio del concepimento del progetto, servizio o prodotto.

La privacy per impostazione predefinita è identificata dall'art. 25 (2) GDPR, che richiede le stesse misure tecniche e organizzative da applicare "per garantire che, per impostazione predefinita, vengano elaborati solo i dati personali necessari per ogni specifico scopo del trattamento" (noto anche come **minimizzazione dei dati**).

Pseudonimizzazione e crittografia sono tecniche che gli sviluppatori **devono implementare** per assicurare la protezione dei dati sanitaria, e per ridurre il potenziale danno causato da potenziali violazioni.

La crittografia è la migliore strategia in termini di sicurezza e responsabilità legale dal momento in cui **i dati protetti in questo modo non sono privati** e, dunque, qualora persi, non sussiste il rischio di incorrere in sanzioni e non è necessario notificarlo.

Tuttavia, i dati crittografati non sono rintracciabili e dunque gli sviluppatori devono ricercare alternative e scendere a complessi compromessi, come la pseudonimizzazione, la quale, se implementata correttamente, può ridurre drasticamente i rischi per gli utenti.

L'approccio più tipico alla pseudonimizzazione (obbligatorio secondo la legge Italiana per la protezione dei dati) è quello di separare l'identificatori personali e documenti sanitari.

VALUTAZIONE DEL CONTRATTO DEL FORNITORE DI SERVIZI (PIATTAFORMA CLOUD)

Frequentemente, le startup implementano le loro applicazioni sanitarie utilizzando servizi e piattaforme di cloud non adatti alla complessità del settore. Fra gli errori più comuni nella scelta ci sono: Google Firebase e Heroku, i quali, sebbene, possano essere molto utili alle applicazioni standard, non sono adeguati a fornire le sufficienti garanzie nella gestione dei dati sanitari e nello sviluppo delle applicazioni. La scelta inziale corretta è fondamentale per non dover fare successivamente modifiche o migrazione fra piattaforme.

Gli aspetti importanti del contratto che gli sviluppatori devono controllare:

+ Che il fornitore di servizi sia conforme alla normativa HIPAA, in altri termini che fornisca garanzie sufficienti per le applicazioni sanitarie negli Stati Uniti. Anche se l'HIPAA non è una legge dell'UE, questo è un parametro affidabile per valutare se gli sviluppatori possano utilizzare un prodotto dedicato agli Stati Uniti anche nell'UE. Firebase e l'offerta standard di Heroku non sono HIPAA conformi. Inoltre, nota che, sebbene Google Cloud Platform, Amazon AWS e altri provider IaaS sono conformi, devono ancora implementare aspetti tecnici come: crittografia del documento, controllo degli accessi, e requisiti GDPR come il diritto all'oblio, etc.
+ Che il fornitore di servizi assicuri garanzie sull'ubicazione dei dati. Al giorno d'oggi la maggioranza dei servizi cloud fornisce tali garanzie, piattaforme come Firebase non lo fanno. In questo caso affidarsi agli accordi di Privacy Shield (vecchio porto sicuro) potrebbe essere una scelta rischiosa, dato il diffuso timore che i dati sulla salute vengano inviati al di fuori dell'UE.
+ Che il fornitore di servizi offra garanzie esplicite sulla privacy e sulla sicurezza dei dati. È responsabilità degli sviluppatori scegliere i fornitori di servizi adeguati. Se i fornitori di servizi non forniscono definizioni chiare delle loro responsabilità nella gestione dei dati sensibili, questo dovrebbe essere un avvertimento molto importante.

ALTRE REGOLAMENTAZIONI RILEVANTI

É importante notare che la GDPR fornisce solo framework di alto livello e solo un punto di partenza per gli sviluppatori Digital Health. In altri termini, la GDPR provvedere alla definizione dei diritti degli utenti e agli obblighi degli sviluppatori, mentre l'implementazione tecnica di questi requisiti è delegata alle migliori prassi di sicurezza, agli amministratori di sistema, ad alcune line guide definite da enti più competenti (Art 29 Gruppo di lavoro, ENISA), standard di sicurezza internazionale (NIST, ISO 270XX) e leggi degli Stati Membri (l'accordo francese HDS, la Linea Guida tedesca per le Applicazioni Sanitarie).

Si noti che le leggi degli Stati membri sono ancora valide ai sensi del GDPR e avranno il potere di introdurre ulteriori restrizioni, che potrebbero fornire ulteriori ostacoli per gli sviluppatori.

RISORSE CONSULTATE

- https://www.dataprotection.ie/docs/10-09-14-Global-Privacy-Sweep-raises-concerns-about-mobile- apps/1456.htm
- http://bmcmedicine.biomedcentral.com/articles/10.1186/s12916-015-0444-y
- http://ec.europa.eu/justice/data-protection/reform/index_en.htm

@chino_api
@zidia

Jovan Stevovic

Jovan Stevovic, CEO e co-fondatore di **Chino.io**. Jovan ha ottenuto un PhD in Computer Science all'Università di Trento sul tema privacy e condivisione dati sanitari sensibili.
Ha lavorato 5 anni nei dipartimenti R&D di aziende che sviluppano software sanitari. Jovan ha fondato Chino Srls nel 2015 assieme a Stefano Tranquillini, con cui hanno vinto diversi premi a livello Europeo come all'EIT Digital Challenge competition on Cyber Security and Privacy.
Attualmente Chino.io aiuta piu' di 50 digital health startups e aziende in EU a risolvere problemi legati alla sicurezza dei dati sanitari e compliance con le normative privacy come GDPR.

Author: Jovan Stevovic, Chino.io CEO and co-founder.