  - Scegliere il tipo di crittografia (simmetrica o asimmetrica) in base al contesto e ai rischi individuati.
  - Adottare soluzioni di crittografia basate su algoritmi pubblici notoriamente robusti.
  - Definire opportune misure per garantire la disponibilità, l'integrità e la riservatezza delle informazioni necessarie al recupero delle informazioni perse (incluse le password di amministratore e dati di ripristino).
- **Anonimizzare i dati personali -** *Eliminare le caratteristiche che identificano i dati personali.*
  - Determinare ciò che deve essere anonimo in base al contesto, alla forma in cui vengono memorizzati i dati personali (compresi i campi del database o estratti dai testi) e rischi individuati.
  - Anonimizzare permanentemente i dati che richiedono tale criterio di protezione in base alla loro forma (inclusi database e record testuali) e i rischi individuati.
  - Se questi dati non possono essere anonimizzati in modo permanente, scegliere strumenti che rispondano innanzitutto alle esigenze funzionali.

5.8.5 Linee guida per lo sviluppo di applicazioni sicure conformi al GDPR

L' introduzione della legge europea sulla privacy dei dati online è destinata ad avere un grande impatto sul modo in cui le organizzazioni dovranno trattare e gestire i dati personali dei propri utenti. Per le organizzazioni che trattano regolarmente i dati dei propri utenti o i dati personali elaborati dai servizi ai cittadini europei, sorgono questioni relative alle implicazioni tecniche riguardo le loro applicazioni e operazioni web online.
La direttiva principale di questa regolamentazione conferisce alle persone fisiche il potere di controllare i propri dati. Ciò significa che gli enti che richiedono informazioni personali online devono informare l'utente su cosa esattamente accadrà ai loro dati, dal momento in cui questi vengono forniti.
Gli aspetti più importanti del regolamento sono i seguenti:

- **Un accesso più facile ai dati personali**: gli individui dovranno avere maggiori informazioni sul trattamento dei loro dati e tali informazioni dovranno essere disponibili in modo chiaro e comprensibile.
- **Il diritto alla portabilità dei dati**: dovrà essere più facile per i soggetti trasferire i propri dati personali tra i vari fornitori di servizi.
- **Un "diritto all'oblio" più chiaro**: se non si desidera più che i propri dati vengano trattati e se non vi sono motivi legittimi per la loro conservazione, questi dovranno essere cancellati.
- **Il diritto di sapere quando i propri dati vengono violati**: ad esempio, le aziende e le organizzazioni devono informare quanto prima possibile l'autorità nazionale di controllo in merito ad eventuali gravi violazioni dei dati personali, affinché gli utenti interessati possano prendere le opportune misure.

Pertanto, in che modo si realizza un'applicazione conforme alla direttiva di cui sopra, tale da fornire un controllo completo dei dati personali degli utenti? Quelle che seguono possono essere considerate le best practices, sulla base delle linee guida sulla privacy indicate dall'OWASP Top Ten:

- **Determinare se l'applicazione ha realmente bisogno di tutti i dati personali richiesti**: l'implementazione ottimale della privacy consente di salvare il minor numero possibile di dati personali, come data di nascita, nome, paese di residenza, ecc. Ciò non è sempre possibile; alcune entità potrebbero aver bisogno di maggiori informazioni. Tuttavia, gli sviluppatori e il management devono definire esattamente quali dati sono assolutamente necessari e quali no.
- **Crittografare tutti i dati personali e informarne gli utenti**: Se un'applicazione ha bisogno di salvare informazioni personali, tali dati devono essere cifrati con algoritmi di crittografia robusti e appropriati, includendo anche l'hashing. Inoltre, dovrebbe essere esplicitamente indicato agli utenti che tutti i loro dati personali, compresi i numeri di telefono, il paese di residenza e l'indirizzo, verranno criptati e verrà calcolato il valore di hash per prevenire qualsiasi forma di estrazione e

manipolazione dei dati in oggetto che porterebbe ad una potenziale esposizione in caso di violazione di quest'ultimi.

- **Considerare l'utilizzo dell'OAUTH per la portabilità dei dati**: I protocolli per l'accesso singolo come OAUTH[53] consentono agli utenti di creare account semplicemente fornendo un altro account, ma al contempo assicurano la non memorizzazione di dati personali diversi dall'ID di autenticazione dell'altro servizio. In altre parole, trattasi di uno standard di autenticazione online open source che consente ad un utente di dare l'accesso alle sue informazioni archiviate nei sistemi di un determinato service provider ad un altro servizio senza tuttavia condividere le sue credenziali.
- **Garantire comunicazioni sicure tramite HTTPS**: Molti siti web non utilizzano l'HTTPS perché non lo ritengono necessario. Ad esempio, se l'applicazione non richiede alcun tipo di autenticazione, l'HTTPS potrebbe sembrare non necessario. Ma è facile ignorare alcuni aspetti. Ad esempio, alcune applicazioni raccolgono dati personali tramite i loro form "contattaci". Se tali informazioni vengono inviate in chiaro, queste potrebbero essere visualizzate su Internet. Inoltre, è necessario assicurarsi che il certificato SSL sia stato distribuito correttamente e non sia esposto a vulnerabilità a cui i protocolli SSL sono soggetti.
- **Informare gli utenti e crittografare i dati personali provenienti dai form 'Contattaci'**: Le applicazioni non raccolgono informazioni solo tramite autenticazione o sottoscrizione, bensì anche attraverso moduli di contatto. La maggior parte di queste informazioni sono personali, tra cui indirizzo e-mail, numero di telefono e paese di residenza. Gli utenti devono essere informati su come e per quanto tempo questi dati verranno conservati. E' altamente raccomandato l'uso di crittografia forte per la memorizzazione di tali informazioni.
- **Assicurarsi che le sessioni e i cookie abbiano una scadenza e che vengano poi distrutti dopo il logout**: Gli utenti devono avere una visibilità adeguata sull'uso dei cookie da parte dell'applicazione. Essi devono essere informati del fatto che l'applicazione sta utilizzando i cookie, l'applicazione deve fornire la possibilità agli utenti di accettare o negare i cookie, e i cookie devono essere adeguatamente distrutti dopo un periodo predefinito di inattività o il logout.
- **Non tenere traccia delle attività degli utenti ai fini della business intelligence**: Molte applicazioni e-commerce su web tracciano le attività degli utenti per determinare le loro preferenze attraverso le ricerche effettuate o i prodotti da loro acquistati. Spesso aziende come Amazon e Netflix utilizzano questo tipo di informazioni per sponsorizzare le loro piattaforme. Poiché i gusti e le scelte personali degli utenti vengono monitorati e conservati ai fini commerciali, gli utenti devono poter accettare o rifiutare tale opzione. Se gli utenti decidono di accettare il tracciamento, questi devono essere informati su come e per quanto tempo i loro dati verranno salvati nel sistema. Ovviamente, tutto ciò che riguarda le informazioni personali deve essere cifrato.
- **Informare gli utenti riguardo l'attività di logging svolta, che riguarda la memorizzazione della posizione o degli indirizzi IP**: Molte applicazioni utilizzano indirizzi IP o posizioni di geo localizzazione come parametro per controllare l'autenticazione e le autorizzazioni, e registrano queste informazioni nel caso in cui qualcuno tenti di aggirare i controlli di autenticazione. Gli utenti devono essere informati di ciò, così come della durata della storicizzazione di tali informazioni nei log del sistema. Non memorizzare mai nei registri di log informazioni significativamente sensibili come le password.
- **Conservare i dati di log in un luogo sicuro, preferibilmente in formato cifrato**: Conservare in un luogo sicuro tutti i dati di log che contengono le informazioni degli utenti e informare quest'ultimi su come tali informazioni vengono trattate: come vengono memorizzati e per quanto tempo vengono conservati. I log stessi devono essere cifrati.
- **L'uso di domande relative alla sicurezza non devono esporre i dati personali degli utenti a possibili violazioni**: In molte applicazioni, le domande di sicurezza vengono usate per confermare l'identità di un utente. Queste domande non dovrebbero includere dati personali come il nome da ragazza della mamma o il colore preferito dell'utente. Se possibile, sostituire tali domande con l'autenticazione a

[53] Protocollo aperto, sviluppato da Blaine Cook e Chris Messina a partire dal novembre 2006: https://oauth.net/