Mauro Giannandrea

Sicurezza e privacy

Dati Personali

Sono dati personali le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le abitudini, lo stile di vita, le relazioni personali, lo stato di salute, la situazione economica, ecc..

Particolarmente importanti sono:

I dati che permettono l'identificazione diretta - come i dati anagrafici , le immagini, ecc. - e i dati che permettono l'identificazione indiretta, come un numero di identificazione (ad esempio, il codice fiscale, l'indirizzo IP, il numero di targa)	I dati rientranti in particolari categorie come i dati c.d. "sensibili", cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i dati genetici e i dati biometrici.	I dati relativi a condanne penali e reati definiti dati "giudiziari", quelli cioè che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (articolo 10) comprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Con l'evoluzione delle nuove tecnologie, altri dati personali hanno assunto un ruolo significativo, come quelli relativi alle comunicazioni elettroniche (via Internet o telefono) e quelli che consentono la geolocalizzazione, fornendo informazioni sui luoghi frequentati e sugli spostamenti.

Perchè gli ottici raccolgono dati

Fidelizzazione
Supporto clienti
Scheda cliente
Servizi personalizzati
Gestione appuntamenti
Reminder appuntamenti
Newsletter

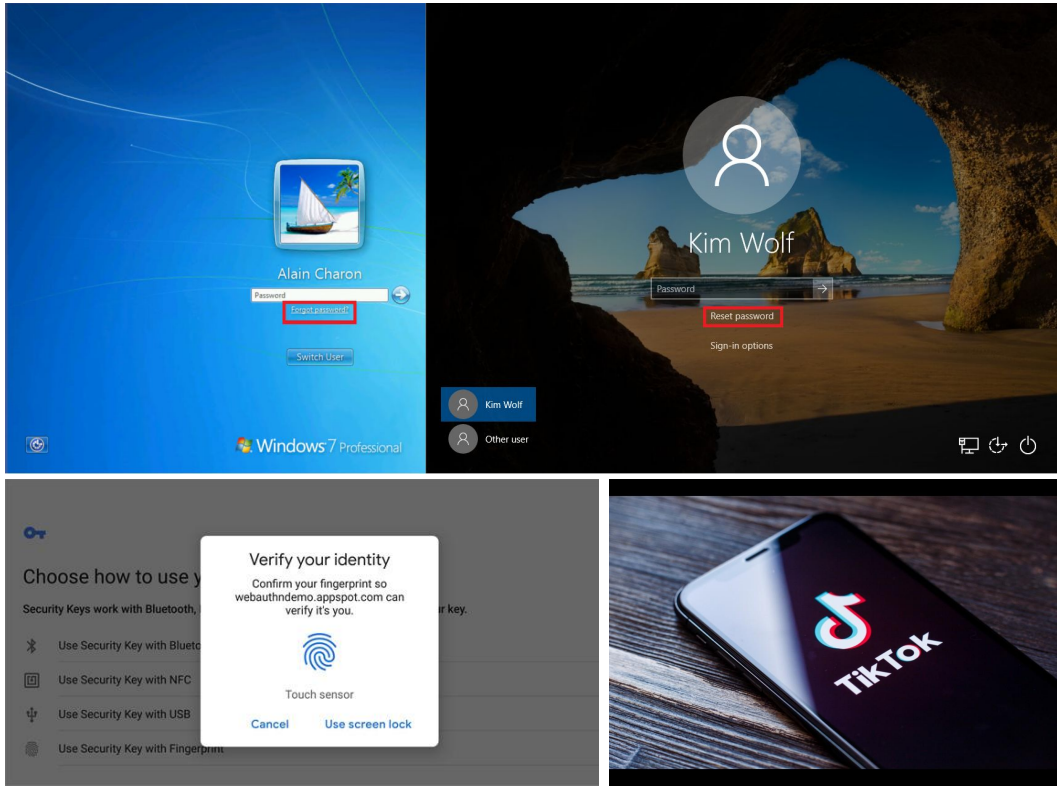
Per fare ciò L'ottico deve ricevere dal cliente un il consenso alla raccolta dei dati che deve essere libero e deve essere specifico, informato e inequivocabile. Il consenso non può provenire dal silenzio, da caselle preselezionate o dell'inattività.

Il consenso sarà anche necessario per qualsiasi e-mail inviata. Per le e-mail commerciali ai non clienti è necessaria una conferma implicita. Le e-mail non commerciali o le e-mail ai clienti richiederanno solo un opt-out (l'opzione di annullare l'iscrizione).

Anche la classica fidelity card dove presente, richiede informative specifiche e consensi ancora più specifici.

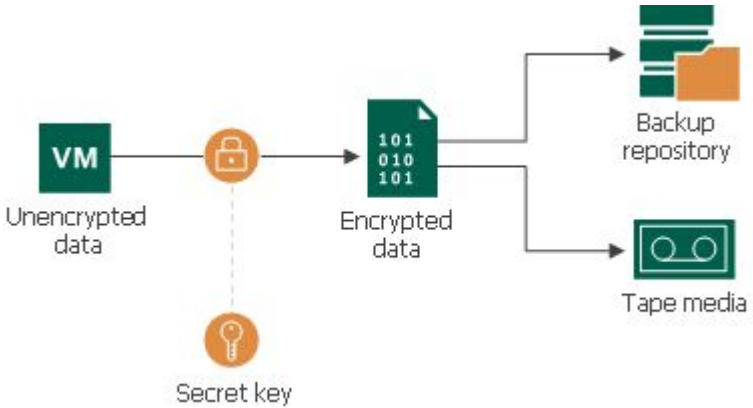
Procedura operativa – le procedure di accesso

I vostri server, computer, smartphone e i dati personali che conservate devono essere inaccessibili a chiunque non sia in possesso delle credenziali giuste. Inoltre gli interessati avranno il diritto di accedere a tutti i loro dati personali, rettificare le inesattezze, opporsi al trattamento in determinate circostanze o cancellare i loro dati; il tutto entro un termine di 30/45 giorni.
L'accesso deve essere personale e le credenziali mai condivise.



Crittografia dei dati

Il GDPR impone la segnalazione tempestiva di qualunque data breach che coinvolge i dati degli utenti. La notifica può avvenire in varie modalità ma con l'obiettivo di raggiungere tutti gli utenti coinvolti o il più ampio pubblico nel caso non si disponga più della lista utenti.



Nel caso i dati utente siano crittografati con algoritmi sufficientemente robusti da impedirne la lettura la notifica non è più obbligatoria.

Full disk encryption

La crittografia completa del disco è un metodo crittografico che applica la crittografia dell'intero disco rigido, compresi dati, file, sistema operativo e programmi software. A differenza delle passate versioni di cifratura del disco, il processo attuale è diventato abbastanza semplice ed è supportato da tutti i principali fornitori. Ad esempio, Apple offre la crittografia integrata sia per IOS che per OS X, Microsoft Windows offre il proprio BitLocker, come anche Android ha la sua alternativa.
La password da sola non è sufficiente a per la protezione dei dati in quanto il contenuto del disco rimane non criptato ed è possibile fare il boot da una chiavetta usb ed accedere alla partizione.

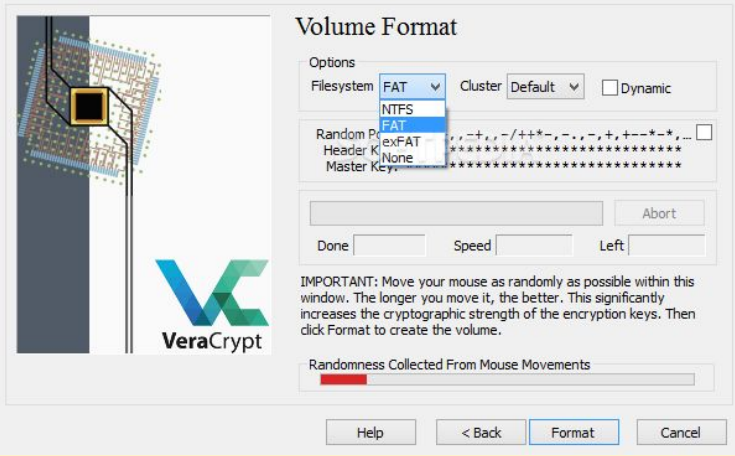
Cancer Care Group: E' stato rubato un portatile che conteneva informazioni di 55.000 ex e attuali pazienti. Di conseguenza, il Cancer Care Group ha finito per pagare 750.000 dollari di danni.

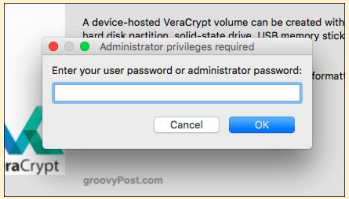
Lahey Hospital: Nel 2011 è stato rubato un portatile contenente le informazioni personali di 599 pazienti da una stanza di trattamento non chiusa a chiave. L'ospedale ha pagato 850.000 dollari come risarcimento.

Crittografia parziale

Per crittografia parziale si intende la crittografia di un solo volume. Tale volume può essere una partizione del pc, una pennetta usb, un archivio o anche un singolo file.
Ci sono software che permettono di creare dei volumi criptati, questi volumi sono portabili e possono essere letti soltanto se si possiede la password per decifrare il contenuto.

Il più famoso di questi software è Veracrypt, opensource, installabile su qualsiasi piattaforma e gratuito anche per usi aziendali.
Sono in commercio anche dispositivi usb con criptografia integrata nel chip, così da avere zero footprint.





Altre valutazioni

Connessioni: Le attività devono dimostrare di aver fatto tutto il necessario per mettere in sicurezza la rete dove risiedono i dati utente. La wifi deve avere criteri di accesso sufficientemente sicuri prevedendo magari opzioni di username/password o filtro dei mac address. Bisognerebbe anche evitare collegamenti di hotspot e strumenti personali. Reti per ospiti fruibili quindi dai clienti o fornitori dovrebbero essere isolate.

Se l'azienda ha un sito web, occorre prevedere un'**informativa privacy** sull'uso dei dati di navigazione nel sito e sui **cookies**;

Se l'azienda ha un **circuito di videosorveglianza** deve redigere un'informativa privacy per i soggetti che potrebbero essere ripresi dalla videocamera.