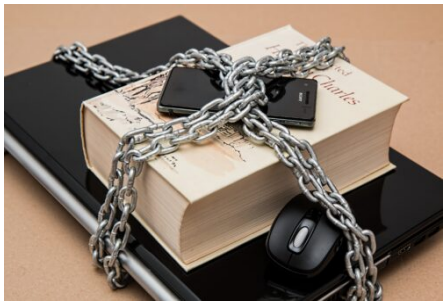
Si fa presto a dire “Misure di Sicurezza adeguate”



Come noto il Regolamento UE 679/2016 (GDPR) non prevede più – a differenza del previgente D.Lgs 196/2003 – di attuare delle **misure “minime” di sicurezza”** a protezione dei dati personali trattati da un’organizzazione (titolare o responsabile del trattamento), bensì **misure di sicurezza adeguate**, stabilite a fronte di una **valutazione dei rischi** sui trattamenti.

In particolare, all’Articolo 32 del GDPR: Sicurezza del trattamento (Considerando 83), si riporta quanto segue:

> 1. Tenendo conto dello stato dell’arte e dei costi di attuazione, nonché della natura, dell’oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
>
> a) la pseudonimizzazione e la cifratura dei dati personali;
>
> b) la capacità di assicurare su base permanente la riservatezza, l’integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
>
> c) la capacità di ripristinare tempestivamente la disponibilità e l’accesso dei dati personali in caso di incidente fisico o tecnico;
>
> d) una procedura per testare, verificare e valutare regolarmente l’efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
>
> 2. Nel valutare l’adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non

> autorizzata o dall’accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

In altri articoli di questo blog abbiamo esaminato varie misure di sicurezza, tecniche ed organizzative, che ogni titolare o responsabile del trattamento dovrebbe adottare e non è l’obiettivo di questo articolo fare un’elencazione delle possibili misure di sicurezza. Si veda al proposito Misure di sicurezza di un’applicazione web per essere conformi al GDPR, Prime esperienze di applicazione del GDPR, Come gestire il Responsabile del trattamento ai sensi del GDPR, Come gestire il Responsabile del trattamento ai sensi del GDPR.

In questo articolo vorrei invece soffermarmi su un aspetto, **la valutazione di “adeguatezza” di una misura di sicurezza** e la possibilità di un’organizzazione di dimostrare a terzi (soggetti di cui tratta dati personali in qualità di titolare, altri titolari del trattamento per i quali svolge il ruolo di responsabile del trattamento, Garante per la Protezione dei Dati Personali a fronte di eventuali ispezioni) di aver fatto tutto quello che poteva per proteggere i dati personali, ovvero di **dimostrare *l’accountability***.

Molte organizzazioni chiedono ai consulenti privacy ed ai loro DPO (o RPD, Responsabile della Protezione Dati) quali misure di sicurezza minime devono adottare, oppure se le misure adottate sono sufficienti. Ma è difficile rispondere a questa domanda in quanto il panorama delle misure di sicurezza, soprattutto sul fronte ICT, è profondamente mutato dal 2004 quando entrò in vigore il vecchio D. Lgs 196/2003 ed in particolare il suo Allegato B (ora abrogato).

Occorre fare una **valutazione dei rischi** che incombono sul trattamento, basata sulla valutazione della **probabilità** e della **gravità** dell’impatto che determinati eventi negativi, rispettivamente, si verifichino e delle conseguenze che possono portare ai dati personali trattati. Inoltre, nella determinazione delle misure di sicurezza, occorre contestualizzare (l’art. 25 del GDPR cita: «*Tenendo conto dello stato dell’arte e dei costi di attuazione, nonché della natura, dell’ambito di applicazione, del contesto e delle finalità del trattamento*…») e non tutte le misure di sicurezza sono uguali a sé stesse in tutti i contesti.

Cerchiamo di capire meglio, partendo da una domanda che un *auditor o consulente*

privacy formula normalmente al responsabile di un'organizzazione – di medio-piccole dimensioni – per la quale deve svolgere un *assessment* sullo stato di adeguatezza rispetto al GDPR.

Auditor: «Quali misure di sicurezza tecnologiche avete adottato per proteggere i dati trattati su supporto e lettronico?»

Responsabile organizzazione: «Abbiamo tutte le misure richieste dalla normativa: antivirus, firewall, backup, password…»

I problemi per il bravo auditor o consulente privacy iniziano a questo punto: bisogna capire quali di queste misure specifiche sono implementate e come, ovvero come sono configurate. Infatti, il GDPR ci chiede di considerare lo **stato dell'arte** della tecnologia, ma anche delle minacce apportate ai dati personali dai "cattivi", ovvero gli hacker, il personale infedele, i malintenzionati in genere. Inoltre ci sono da considerare anche i rischi di origine ambientale, quali catastrofi naturali, terremoti, ecc.. Purtroppo, anche in questo ambito lo "stato dell'arte" negli ultimi 10-15 anni ha fatto aumentare la probabilità di eventi quali terremoti ed alluvioni in zone nelle quali non si erano mai verificati eventi gravi (vedi ad es. Emilia – Romagna). Anche la pandemia Coronavirus, sebbene non abbia portato ad aumentare i rischi diretti di perdita di dati o di perdita di riservatezza degli stessi, ha comportato – essenzialmente attraverso il lavoro a distanza – a cambiare il "perimetro" entro il quale i dati vengono trattati, generando nuove vulnerabilità presto sfruttate da malintenzionati che hanno prontamente creato nuove minacce per attaccare i dati delle aziende.

Prendendo spunto da provvedimenti e sanzioni già comminate dal Garante Privacy relativamente alle misure di sicurezza non adeguate, a fronte di una violazione (*data breach*) verificatasi, vorrei esaminare alcune misure di sicurezza implementate da quasi tutte le organizzazioni.

Premesso che il GDPR ci chiede di scegliere le misure di sicurezze anche in base al **costo di attuazione**, dunque non può chiedere ad una piccola organizzazione (ad es. uno Studio Professionale o una piccola Società di servizi che tratta anche dati particolari) le stesse misure di sicurezza adottate da un'azienda a livello Enterprise – ad es. sistemi antintrusione molto evoluti, appliance di sicurezza informatica o altri strumenti "top di gamma" – è comunque necessario dimostrare di non aver trascurato il problema, per noncuranza oppure per eccessiva riduzione dei

costi.

Partiamo dall'antivirus, ormai meglio denominato **anti-malware**, il cui obiettivo è prevenire virus informatici, tra cui i tanto temuti *ransomware*, ma anche *syware* (programmi spia che raccolgono dati a fini pubblicitari, quando va bene) e simili.

Ci sono antivirus gratuiti (ma attenzione che molti di essi non sono *freeware* per uso commerciale, per cui si rischia di incorrere in sanzioni per assenza di licenza) che offrono una discreta protezione, ma non certamente ottimale come quella fornita dalle corrispondenti versioni a pagamento. Tra gli anti-malware gratuiti c'è anche Microsoft Defender (o Windows Defender), incluso e preinstallato in Windows 10 che offre anch'esso una discreta protezione, ma non ha performance eccellenti nella protezione dal *ransomware* e non costituisce una scelta ottimale per chi tratta dati particolarmente critici (ad es. dati sanitari).

La scelta di non adottare una soluzione a pagamento è sostenibile? Se tutto va bene non ci sono problemi, ma se siamo colpiti da un *ransomware* che ci blocca l'attività e ci costringe a segnalare la violazione dati al Garante Privacy (difficile nascondere la violazione se, come nel caso di una Farmacia lombarda bisogna stare chiusi e mettere un cartello in strada nel quale si informa la gentile clientela che si resta chiusi per problemi informatici…) è difficile sostenere che le nostre misure di sicurezza erano adeguate. Come si giustifica la scelta di non spendere per un antivirus commerciale? A fronte del costo di circa una cinquantina di euro l'anno per la protezione di 3 PC è difficile sostenere la motivazione economica.

Ma acquistare un antivirus professionale non basta, occorre configurarlo correttamente.

Pensate che un software di sicurezza completo di anti-malware, firewall ed altri *tool* di sicurezza accessori (aggiornamento applicazioni, analisi vulnerabilità, protezione webcam, ecc.) tra i più noti, come Kaspersky Internet Security, presenta oltre una quarantina di parametri da configurare per ottenere un giusto compromesso fra prestazioni del computer e delle applicazioni e livello di protezione, con la necessità di configurare opportunamente alcuni parametri per poter utilizzare determinate applicazioni. Ad esempio, per poter utilizzare una semplice chiavetta per la firma digitale al fine di accedere al portale di accesso del Processo Civile Telematico (necessario per avvocati e CTU come il sottoscritto) occorre disabilitare il controllo delle connessioni crittografate, impostata per default dall'antivirus come attiva. L'utilizzo di applicazioni web – dal semplice *home-banking* ai siti di *e-commerce*, ai portali specifici utilizzati da alcune organizzazioni per determinate attività lavorative – richiedono talvolta impostazioni specifiche, anche dipendenti dai browser usati, relativamente ad anti-banner, cookie, navigazione in incognito e così via.

Naturalmente in caso di diversi PC collegati in rete con un server che accede a internet la situazione si complica. In sostanza bisogna saper configurare

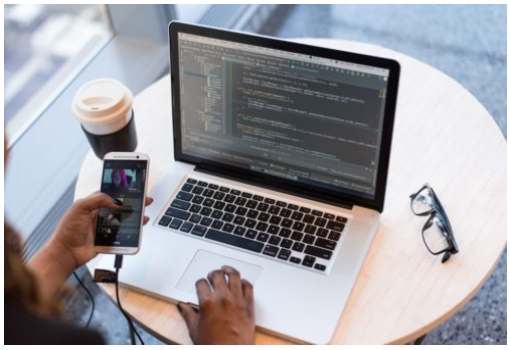
correttamente i *tool* di protezione oppure ricorrere ad un consulente informatico esterno.

Per il **firewall** vale il discorso fatto per l'antivirus, sia per quanto riguarda le soluzioni gratuite, sia per quanto riguarda la corretta configurazione. Come ulteriore complicazione si aggiunge il firewall hardware offerto ormai da quasi tutti i modem/router delle compagnie telefoniche, che deve essere configurato in modo da evitare incompatibilità con il firewall software e la struttura informatica interna. Tra l'altro spesso le incompatibilità riscontrate da utenti non esperti portano ad eliminare alcune misure di sicurezza per evitare problemi. Anche in questo caso spesso è difficile rinunciare ad un tecnico esperto esterno, in particolare per le piccole organizzazioni che non hanno un vero responsabile ICT interno in grado di gestire e risolvere la maggior parte dei problemi.

Se poi l'organizzazione deve accedere ad applicazioni web o ha installate sul proprio server applicazioni gestionali che devono essere fruibili anche esternamente, c'è l'esigenza di esporre servizi ed applicazioni all'esterno per renderle visibili e/o rendere visibili dall'esterno a determinate risorse (PC o server) interne.

In tutti questi casi occorre ancora l'intervento di uno specialista e spesso non basta un intervento "una tantum". Purtroppo, molte organizzazioni di piccole dimensioni, che magari trattano dati particolari (di cui all'art. 9 del GDPR), scelgono di spendere per servizi professionali esterni solo quando strettamente necessario, mentre spesso ci sarebbe bisogno di una manutenzione costante dei sistemi informatici, almeno dal punto di vista sistemistico. Infatti, col tempo le configurazioni degli strumenti di protezione cambiano, oppure cambiano le modalità di fruizione delle applicazioni e gli strumenti di protezione non vengono riconfigurati di conseguenza.

Qui andiamo ad introdurre l'argomento dell'**Amministratore di Sistema**, figura tanto discussa a causa del provvedimento del Garante per la Protezione Dati Personali di ormai 10 anni fa (cfr. Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema – 27 novembre 2008; aggiornato in base al provvedimento del 25 giugno 2009).



Da un punto di vista puramente formale è bene precisare che tale Provvedimento NON è

stato abrogato, sebbene in talune situazioni può essere derogata la nomina dell'Amministratore di Sistema (AdS) e il GDPR non citi questa figura. Da un punto di vista sostanziale non si può negare che la nomina formale – con compiti e responsabilità precise – dell'AdS costituisca una misura di sicurezza di tipo organizzativo. Al di là di questo il fatto di delegare il controllo dei propri sistemi informatici ad uno o più AdS in modo continuativo garantisce il Titolare (o Responsabile) del trattamento che i sistemi informatici siano ben configurati.

Ricordiamo la definizione di AdS, secondo l'Autorità Garante:

«Con la definizione di "amministratore di sistema" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente provvedimento vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.»

Purtroppo, queste regole sono sovente disattese per due ragioni fondamentali:

1. Molte organizzazioni si rivolgono a consulenti informatici e tecnici sistemisti esterni solo "alla bisogna", ovvero quando c'è da installare una nuova risorsa hardware o un nuovo software, oppure quando si verifica un problema. Già questo non va proprio bene alla luce dei discorsi fatti sopra: il titolare del trattamento potrebbe non avere sotto controllo le misure di sicurezza implementate "una tantum".
2. Altre organizzazioni hanno un rapporto continuativo con un soggetto esterno che, di fatto, svolge il ruolo di AdS (spesso nominato Responsabile ICT esterno) in quanto detiene continuativamente le credenziali di *system administrator* (usiamo il termine inglese per distinguerlo dal termine italiano che rievoca il provvedimento del Garante) e svolge manutenzione periodica sui sistemi informatici dell'organizzazione, ma non è stato formalmente nominato Amministratore di Sistema. Perché? Spesso perché non ha il controllo completo sui sistemi, in quanto altri soggetti possono operare con le credenziali di *system admin* (talvolta le medesime) sui sistemi dell'organizzazione, perché non tutte le risorse hardware ed i software vengono installati e configurati dal Responsabile ICT esterno, il quale, quindi, non vuole garantire determinate misure di sicurezza perché non è in grado di assicurarlo. Altre volte è la stessa Direzione dell'organizzazione che desidera eludere alcune misure di sicurezza ritenute "adeguate" dall'AdS ed addirittura le c.d. misure minime di sicurezza di cui al Disciplinare tecnico (allegato B) del vecchio Codice Privacy. Altre volte, infine, è solo questione di soldi.

In molte situazioni – che rientrano in ambedue le casistiche sopra citate – come aggravante c'è il problema dei *log* e della loro conservazione. Infatti, il provvedimento impone che siano conservati i *log* degli AdS, in formato non

modificabile dagli stessi, per almeno sei mesi. Poiché per realizzare ciò normalmente occorre un applicativo a ciò dedicato (oppure occorre sviluppare apposite procedure informatiche), talvolta la Direzione dell'organizzazione non vuole spendere per acquistare tale applicativo e, dunque, il candidato AdS (in questo caso può essere anche interno all'organizzazione, ovvero un dipendente) non accetta la nomina perché non è in grado di adempiere ai propri compiti relativamente alla conservazione dei log.

In entrambe le tipologie di situazioni i Titolari (o Responsabili) del trattamento devono solo pregare di non subire un *data breach* importante, perché nel caso la sanzione dell'Autorità Garante è assicurata in quanto non si riuscirebbe ad assicurare *l'accountability* del Titolare (o Responsabile) del trattamento.

Altro caposaldo delle misure di sicurezza è il **backup**, che – rimanendo strettamente nell'ambito del GDPR, ovvero nel trattamento di dati personali – può avere livelli di importanza molto diversi. Infatti, garantire la disponibilità dei dati ha un impatto differente per un Ospedale oppure per un'azienda manifatturiera.

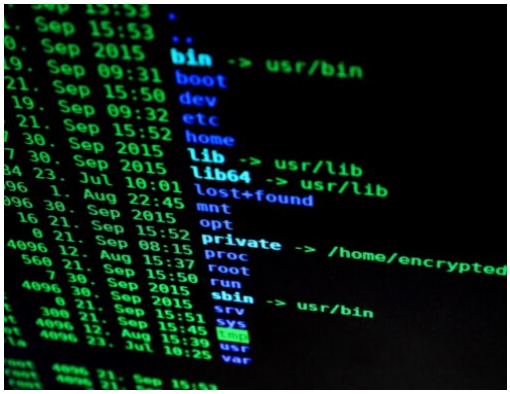
Anche in questo caso non basta dire avere il backup, ma bisogna porsi altre domande:

- Viene fatto un backup sempre completo? Oppure viene fatto un backup incrementale o differenziale?
- Qual è la frequenza del backup?
- Su quali e quanti supporti viene salvato il backup?
- Dove e come vengono conservati i supporti?
- Il backup è accessibile on-line? È cifrato?
- Qual è la *retention* dei backup (ovvero fino a quanto tempo nel passato riesco a recuperare i file)?
- Vengono eseguite prove di ripristino (*restore*) complete o parziali?
- E così via.

Una regola sui backup è quella del "**3-2-1**", ovvero mantenere almeno **3** copie dei dati (compreso l'originale), su **2** supporti, almeno **1** in una *location* remota.

È inutile aggiungere che anche se il backup può essere eseguito automaticamente (salvo poi gestire i supporti off-*line* e portarli con una certa frequenza in un'ubicazione remota), la configurazione dello stesso deve essere eseguita da personale un minimo esperto; e quindi ci riallacciamo al discorso fatto in precedenza.

L'ultimo elemento della domanda iniziale sulle misure di sicurezza è costituito dalle **password**, ovvero dalle credenziali di autenticazione, meglio descritte dall'espressione "**controllo degli accessi logici**" ai sistemi informatici.



Molti ritengono di essere a norma dotandosi di accessi con password di almeno 8 caratteri, da cambiare periodicamente. Sulla variazione periodica della password molti sorvolano, ma se da un lato esistono tesi valide che ritengono che la variazione periodica, soprattutto con frequenza breve (mensile o trimestrale) della password sia non solo inutile, ma anche controproducente, dall'altro molte organizzazioni hanno sposato questa tesi in modo inconsapevole, direi quasi incosciente.

Come al solito bisogna avere una visione completa del problema: si può eliminare il cambiamento della password a condizione di adottare una strategia di sicurezza adeguata come usare password complesse (caratteri alfanumerici, numerici e simboli, ecc.) ed introdurre l'autenticazione a due fattori. Questo è molto più importante se stiamo parlando dell'autenticazione ad un'applicazione web alla cui pagina di *login* potrebbero facilmente accedere anche soggetti esterni malintenzionati.

C'è poi il principio del **minimo privilegio** che andrebbe soddisfatto, ovvero ogni utente dovrebbe poter accedere esclusivamente alle risorse di cui ha bisogno per lavorare. Purtroppo, invece, molte piccole organizzazioni concedono a tutti di vedere tutto, basandoci sulla fiducia che tutti i collaboratori si comportino correttamente, anche al fine di evitare problemi di accesso in caso di assenza di personale.

Da un lato questa prassi può essere pericolosa perché, pur credendo alla buona fede di tutti, nel caso in cui un utente clicchi su un allegato malevolo o su una pagina web contenente malware, si rischia di compromettere tutte le risorse del sistema informatico portandosi in casa un *ransomware*. Analogamente se le credenziali di accesso di un utente venissero compromesse (per attacchi informatici o tramite attività di *social engineering*) un malintenzionato avrebbe accesso a tutte le risorse dei sistemi.

Dall'altro lato le esigenze della Direzione e/o della proprietà dell'organizzazione possono essere soddisfatte da sistemi informatici adeguatamente configurati, acquisendo gli strumenti giusti, da parte di un tecnico esperto. Dunque, anche in questo caso, spesso è questione di costi.

Da ultimo vorrei brevemente affrontare il problema delle **comunicazioni elettroniche**, tra cui la **mail** riveste un ruolo principe.

È facile vedere che molte piccole organizzazioni e singoli professionisti utilizzano indirizzi di posta elettronica gratuiti (le estensioni vanno da @libero.it a @tin.it a @gmail.com e così via). Chiaramente questi servizi di posta sono gratis a discapito della privacy, pertanto sono spesso origine di *spam* perché i provider rivendono gli indirizzi ed i dati di profilazione a terzi.

Visto il costo di 10-15 euro l'anno di un indirizzo di posta elettronica a pagamento, è difficile giustificare un soggetto che utilizza la posta elettronica anche per trasmettere e ricevere dati particolari (ex dati sensibili). In caso di *data breach* del gestore (per "libero.it" è già successo) o dell'utente, ad esempio per aver subito l'intercettazione della posta, trasmessa con protocolli non cifrati (ad es. "tin.it" non utilizza i protocolli SSL o TLS), anche in questo caso, non ci sono giustificazioni plausibili.

Altre possibili misure di sicurezza non implementate, quali l'impiego di protocolli di comunicazione obsoleti o deprecati per comunicazioni di dati particolari, l'invio di buste paga o altre informazioni personali che ricadono fra le particolari categorie di dati attraverso e-mail in chiaro (non cifrate) e così via, dovrebbero essere prese in considerazione.

Si ribadisce che occorre comprendere che una determinata misura di sicurezza tecnica non è, di per sé, adeguata o meno in assoluto. A seconda del contesto in cui si opera, della natura dei dati trattati, del costo (nell'ottica che abbiamo esplicitato sopra) e dei vincoli che esistono per svolgere una determinata attività, una certa scelta dell'imprenditore – adeguatamente documentata – può essere ritenuta accettabile in una realtà e reputata inadeguata in un'altra, magari semplicemente perché non si ravvisa una scelta consapevole, supportata da ragionamenti ed evidenze oggettive da parte del titolare (o responsabile) del trattamento.

Il consiglio è, quindi, di farsi documentare dal consulente informatico esterno o amministratore di sistema, in un'apposita relazione sulle misure di sicurezza dei sistemi informatici, tutte le misure di sicurezza effettivamente implementate e di mantenere aggiornato tale documento.

Il campo delle misure di sicurezza tecniche ed organizzative a protezione dei dati personali è molto ampio: esistono le norme ISO 27001 e soprattutto i controlli della ISO 27002 sui sistemi di gestione della sicurezza delle informazioni, integrate dalla ISO 27701 specifica sulla protezione dei dati personali, le Linee Guida ENISA, il *Cybersecurity Maturity Model*, le Linee Guida NIST, le Misure di Sicurezza AGID (specifiche per la P.A.) e così via. Facendo riferimento a documenti normativi riconosciuti o *best practice* consolidate si riesce a dimostrare l'adeguatezza delle proprie misure di sicurezza nei confronti di terzi.

Qualcuno obietta sempre: «*Ma se gli hacker sono riusciti a violare Enti governativi molto importanti ed aziende molto grandi e strutturate, che volete che possa fare io nella mia piccola organizzazione?*». Naturalmente i malintenzionati cercano sempre di

“pescare” i pesci più grossi, anche se alle volte vanno “a strascico” per cui anche i più piccoli devono difendersi facendo quello che è nelle loro possibilità.

In conclusione, le piccole organizzazioni devono stare molto attente a non ritenere che la privacy possa essere risolta con qualche adempimento formale e dichiarando di applicare alcune misure di sicurezza minimali per essere conformi; in altre parole con la compilazione/redazione di qualche documento da firmare e tenere nel cassetto, come certe soluzioni “preconfezionate” vorrebbero far credere.