ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI TORINO

Testata: Il Giornale dell'Ingegnere Data: luglio 2018 Pagina: 9

GDPR **SICUREZZA** | TRATTAMENTO DATI

Il GDPR e il principio di accountability

Tra responsabilità, trasparenza e compliance

DI LUCA GIOPPO*

Il principio di accountability, originato nel mondo anglosassone, va oltre il semplice concetto di "essere chiamato a rendere conto delle proprie azioni", riferendosi a una responsabilità incondizionata, formale o non, in capo a un soggetto o a un gruppo di soggetti (accountors), del risultato conseguito da un'organizzazione (privata o pubblica), sulla base delle proprie capacità, abilità ed etica. Tale responsabilità richiede giudizio e capacità decisionale, e si realizza nei confronti di uno o più portatori di interessi (account-holders o accountees), con conseguenze positive (premi) o negative (sanzioni), a seconda che i risultati desiderati siano raggiunti o disattesi. Nel contesto del GDPR, il corretto trattamento dei dati e le misure di sicurezza adottate.

Insieme al concetto di responsabilità, presuppone quelli di trasparenza e di compliance.
Per rispondere adeguatamente a questo principio non solo gli adempimenti devono essere con-

caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Cosa devono pertanto fare i professionisti per implementare un set minimo di soluzioni informatiche "adeguate" alla propria realtà?
Un elemento importante è essere sempre consapevoli delle minacce informatiche/tecnologiche ed essere pronti a intervenire. Soprattutto, occorre essere consapevoli dell'intera area di esposizione che si ha oggi: spesso si tende a limitarsi a prassi semplici, pensando che sia necessario proteggere unicamente il proprio personal computer. Oggi la principale porta d'ingresso è lo smartphone, tramite cui diventa possibile entrare in possesso delle informazioni necessarie a operare altri tipi di attacchi.

Cosa fare, quindi, nel concreto?

cretamente svolti ("sostanza"), ma tutto ciò che viene svolto deve essere anche formalmente verificabile ("verificabilità"), sia dall'interno, sia da eventuali operazioni di auditing esterno. Ciò comporta la necessità di tenere traccia di qualsiasi operazione effettuata in un'ottica di protezione dei dati al fine di poter ripercorrere in maniera obiettiva, in ogni momento, il percorso seguito e di valutare i risultati.

L'articolo 32 del GDPR specifica l'implementazione di misure di sicurezza vere e proprie, intese nel senso stringente del termine, stabilendo come (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 e il Responsabile del trattamento debbano mettere in atto misure tecniche e organizzative idonee per garantire un livello di sicurezza adeguato al rischio.

L'articolo fornisce alcuni esempi che sono rappresentativi di macro requisiti minimi, utili a verificare una congruità del proprio sistema di sicurezza:

- la "pseudonimizzazione" e la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in
- adottare politiche di backup affidabili, ossia utilizzare storage affidabili e non direttamente o permanentemente collegati ai sistemi primari, facendo periodiche verifiche di ripristino per essere certi del corretto funzionamento. Non solo, per rispondere alle necessità di dimostrare l'integrità e la capacità di ripristinare i dati ai fini GDPR, ma anche per offrire la possibilità di mettere effettivamente in sicurezza ciò che rappresenta uno degli asset strategici dell'attività professionale;
- utilizzare soluzioni di cifrature delle informazioni, soprattutto laddove si utilizzano device portatili che possono essere rubati;
- "securizzare" l'accesso ai device – tutti, smartphone compreso – tramite l'utilizzo di password adeguate o soluzioni che impediscano l'utilizzo di chiavette USB, se non autorizzati;
- prestare particolare attenzione alle credenziali utilizzate per i diversi servizi o social network, avendo cura di utilizzare password diverse per ogni servizio; esistono strumenti per la conservazione delle password e la digitazione automatica nel browser che facilitano l'utilizzo di password complesse;
- utilizzare caselle di posta e/o numeri di cellulare dedicati esclusivamente alla registrazione e/o gestione degli account. Infatti, si va diffondendo oggi il fenomeno del phone porting, tramite il quale

l'hacker riesce a "migrare" il nostro numero di telefono grazie a tutte le informazioni che abbiamo sparso sul web e, tramite questo escamotage, è in grado di usufruire di un telefono che, grazie alla nuova SIM ricevuta dall'operatore, può farsi inviare dai vari account dei servizi da noi utilizzati i link per cambiare la password in base alla funzionalità che consente di recuperare una password persa; il link arriverà sul telefono dell'hacker che avrà, quindi, la possibilità di entrare nei nostri account e "tagliarci letteralmente fuori". Dati i costi dei contratti telefonici e la facile disponibilità di caselle e-mail, può essere consigliabile per alcuni soggetti dotarsi di contratti dedicati alla sola gestione dei propri account con numeri telefonici e caselle di posta elettronica che non verranno mai resi noti a nessuno;

- fare una valutazione accurata del danno e del rischio: a quanto ammonterebbe il danno economico o di immagine a seguito della perdita dei dati dei propri clienti, progetti, account social, account di home banking o di criptovalute? A seconda della risposta, adottare una strategia di riduzione del rischio più o meno aggressiva, ma commisurata.

Diventa evidente che il GDPR deve essere inteso come un'opportunità per aumentare il livello di sicurezza complessiva per la nostra attività, consentendoci di svolgere la professione in maniera più serena, non solo perché abbiamo adempiuto a obblighi normativi, ma perché abbiamo consolidato delle prassi che sono funzionali al nostro lavoro in sicurezza.

* **Tesoriere Ordine degli Ingegneri della Provincia di Torino e Specialista di tecnologie**