PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 18 - numero 3877 di mercoledì 19 ottobre 2016

La Privacy Impact Analysis (PIA)

Prima di affrontare qualunque attività è necessario dedicare la giusta attenzione alla protezione dei dati personali: come fare la valutazione dell'impatto sulla protezione dati prevista dal regolamento 679/2016? Di Paola Limatola e Sebastiano Plutino.

Il Regolamento in materia di trattamento dei dati personali promuove una nuova modalità di approccio alla protezione dati personali, sulla falsariga delle "prassi" utilizzate per i sistemi di gestione (cfr. ISO 9001:2015, ISO 14001:2015, ISO 27001:2013 ...): prima di affrontare qualunque attività è necessario dedicare la giusta attenzione alla protezione dei dati personali, tenendo conto delle tecnologie utilizzate per il trattamento dei dati e dei rischi cui l'organizzazione si espone con un trattamento.

I rischi da analizzare possono esterni o interni e devono essere attentamente valutati e pesati, poiché gli, eventuali, interventi di mitigazione dovranno essere adeguati al contesto e non inutilmente onerosi rispetto alla effettiva "pericolosità" del trattamento.

Pubblicità
<#? QUI-PUBBLICITA-SCORM1-[EL0143] ?#>

La PIA - Valutazione dell'impatto sulla protezione dati ? è definita dall'art. 35 del Regolamento e deve essere svolta dal Titolare del Trattamento con il supporto del Responsabile della Protezione Dati (DPO) ove presente.

Anche se il Regolamento individua i casi in cui lo svolgimento di tale analisi è indispensabile e obbligatorio (trattamenti automatizzati e profilazione, trattamento su larga scala di particolari categorie di dati...) e anche se l'Autorità Garante pubblicherà probabilmente un elenco esaustivo delle situazioni in cui la PIA dovrà essere effettuata, riteniamo che tutti i Titolari del Trattamento, a prescindere dall'obbligatorietà, potrebbero trarre dei benefici da una valutazione ex-ante degli aspetti legati al trattamento dei dati personali per valutarne i rischi e verificare il rispetto della normativa.

L'ampiezza dell'analisi sarà legata alla complessità dell'organizzazione e, in molti casi, potrà essere affrontata anche dalle realtà più piccole con un impegno ragionevole.

L'utilizzo di strumenti già utilizzati nei sistemi di gestione, come ad esempio, il metodo Plan-Do-Check-Act (PDCA), permetterà di valutare il trattamento alla stregua di un processo e quindi inserirlo nel piano degli altri processi aziendali e di sottoporlo ad analisi, facendo emergere eventuali rischi connessi al nuovo processo sia da solo che nel rispetto degli altri già monitorati (secondo le linee guida della ISO 9001:2015).

Il Titolare inserendo il trattamento fra i processi aziendali e trattandolo come un qualunque altro processo ne ricaverebbe l'indubbio vantaggio di includere una componente importante e spesso sottovalutata nel quadro generale dei rischi aziendali e di avere una rappresentazione completa del proprio rischio imprenditoriale.

Alcune metodologie in uso per la PIA individuano con precisione i passi da compiere:

senza entrare in un livello di dettaglio eccessivo, il tema del trattamento dati deve essere affrontato con lo stesso approccio che ogni imprenditore utilizza prima di intraprendere un nuovo progetto qualificando cioè il quadro dei rischi.

Per i dati personali si tratta di valutare: il tipo di informazioni relative alle persone fisiche che l'organizzazione intende raccogliere, stabilire:

- se tali informazioni saranno comunicate a terze parti o saranno memorizzate in paesi non Europei,

- se la tecnologia utilizzata per il trattamento sarà innovativa e potrà essere percepita come intrusiva (riconoscimento facciale, biometria...);

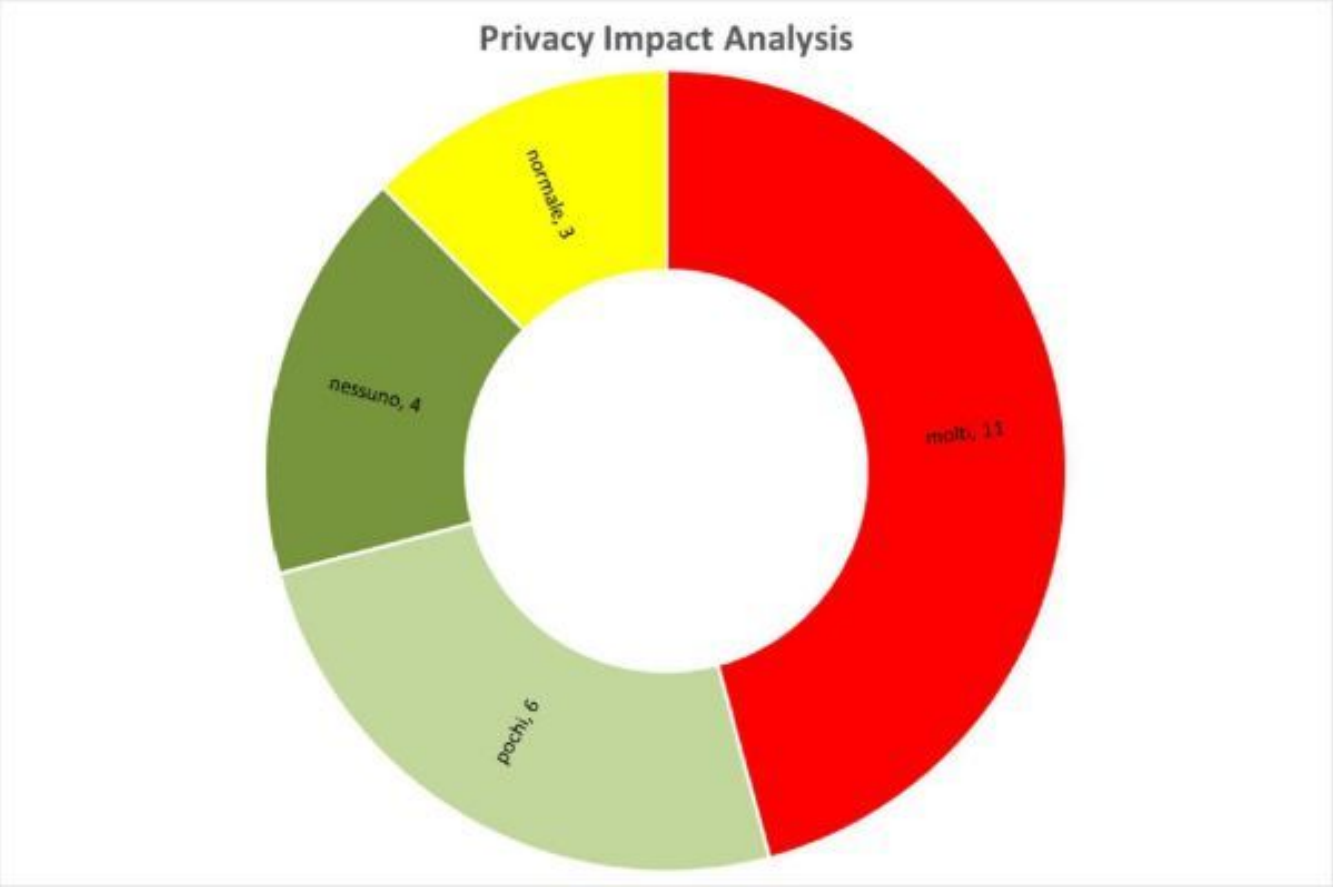
- bisognerà valutare se l'infrastruttura tecnologica utilizzata sarà efficacemente protetta da intromissioni esterne che possano pregiudicare la sicurezza dei dati o la continuità operativa;

- considerare l'opportunità di attivare meccanismi di crittografia, pseudonimizzazione o altre "disgiunzioni" che possano proteggere i dati e, se del caso, renderli disponibili per soli fini statistici;

- sarà inoltre necessario analizzare l'efficacia della comunicazione, interna ed esterna, e chiedersi se tutti i collaboratori e le persone autorizzate al trattamento siano state correttamente informate sui comportamenti da adottare nell'espletamento delle loro mansioni.

- ...

Questo percorso permetterà di definire un profilo di rischio e, utilizzando opportuni algoritmi. rappresentarlo in forma grafica: il giallo e il rosso, nell'esempio sotto, individuano le aree di rischi sui quali si dovrà intervenire attraverso opportune mitigazioni.



Nel caso di implementazione di un nuovo progetto (ad esempio un nuovo prodotto o un nuovo servizio che si intende offrire alla propria clientela) questa analisi preventiva potrà consentire di operare scelte coerenti con l'approccio "privacy by default" caldeggiato dal Regolamento.

Il Titolare avrà così la possibilità di valutare correttamente tutti gli elementi di rischio e di mitigarli in modo efficace a tutela della redditività del progetto e degli interessi dell'organizzazione, prendendo decisioni consapevoli.

Qualora la PIA evidenziasse fattori di rischio molto elevati in merito al trattamento dei dati personali, potrà essere necessario rivedere il progetto per elaborare nuove strategie che mitighino, ex-ante, il rischio. Una possibilità sarà il coinvolgimento del Garante per avere un parere che dia chiarezza definitiva sulla fattibilità dell'iniziativa che si intende portare avanti.

In conclusione, la PIA deve essere vista come uno strumento di analisi iniziale del progetto che evidenzia le opportunità e permette di individuare i rischi.

Rischi che, grazie al Regolamento, potranno essere analizzati e risolti attraverso meccanismi tecnici o autorizzazioni specifiche.

Paola Limatola

Sebastiano Plutino

Regolamento (Ue) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

 Questo articolo è pubblicato sotto una Licenza Creative Commons.

---

www.puntosicuro.it