NUNZIANTE • MAGRONE

Alert
Privacy - Review

Cybersecurity e Privacy

FOCUS: DATA PROTECTION COMPLIANCE

Continua l'approfondimento sulla cybersicurezza, questa volta osservata dalla prospettiva della *compliance data protection*, concentrando quindi l'attenzione sui rischi sanzionatori nei quali possono incorrere le imprese, vittime di cyberattacco, che non avessero implementato le misure adeguate a gestire il rischio, e sulle misure integrative atte far fronte ai rischi di sicurezza aggravati dalla pandemia.

Prosegue quindi l'esame iniziato nella precedente newsletter dove venivano esaminate le correlazioni tra il repentino incremento della digitalizzazione connesso alla pandemia da Covid-19 e l'aumento degli attacchi cybercriminali, spostando ora il focus dai costi e responsabilità delle imprese dal punto di vista contrattuale e assicurativo a quelli connessi alla *compliance privacy*.

Obblighi di sicurezza GDPR

In una prospettiva *data protection* infatti l'impresa, che agisca in qualità di Titolare o di Responsabile del trattamento, ha l'obbligo, ai sensi dell'art. 32 del Regolamento UE 679/2016 (il "GDPR"), di "*mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*" che proteggano "*da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali*" (art. 5.1 lett. f) GDPR).

La formulazione normativa è volutamente flessibile e non indica misure di sicurezza fisse e tassative, in ossequio al principio di accountability che permea il GDPR e ripudia l'approccio "*one size fits all*".

L'art. 32 del GDPR privilegia infatti al contrario un approccio di *self-assessment* individuale, per cui ogni impresa è tenuta ad assumersi la responsabilità di compiere una disamina specifica di tutte le caratteristiche e circostanze del trattamento dei dati effettuato nella propria azienda nonchè del relativo rischio e approntare le misure di sicurezza più adeguate "*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*".

Alert
Privacy - Review

Rischio sanzionatorio in caso di attacco *cyber*

Nella fase "patologica" del trattamento, ovverosia quando si verifica un *data breach* (che include le ipotesi di *cyber attack*), i medesimi criteri di analisi di adeguatezza vengono applicati *ex post* dall'autorità di settore (in Italia il Garante Privacy) - eventualmente coinvolta in quanto destinataria di notifica della violazione ove si verifichino i requisiti di necessità *ex* art. 33 GDPR - onde stabilire se sul verificarsi del *data breach* possa aver influito la carenza di misure di sicurezza adeguate, secondo le conoscenze allo stato dell'arte (anche tecnico-informatica oltre che organizzativa), per la singola specifica azienda violata.

Ove l'istruttoria condotta accerti tale responsabilità in capo all'impresa/ente oggetto di attacco informatico, l'autorità potrà adottare nei confronti di quest'ultima oltre alle misure prescrittive anche una sanzione amministrativa fino a 10 milioni di Euro o fino al 2% del fatturato mondiale totale dell'esercizio precedente, ai sensi dell'art. 83.4, lett. a) GDPR, ovvero fino a 20 milioni di Euro o fino al 4% del fatturato mondiale totale dell'esercizio precedente, ai sensi dell'art. 83.5, lett.a) GDPR, laddove venga contestata anche la violazione dell'art. 5.1 lett. f) GDPR.

È quel che è accaduto ad esempio - volendo dare uno sguardo all'attualità internazionale - nei noti casi trattati dall'autorità garante inglese (l'"ICO") di attacchi hacker al gruppo alberghiero Marriott (provv. 30.10.2020) e a British Airways (provv. 16.10.2020), che hanno portato alla comminazione di sanzioni record alle due imprese pari rispettivamente a 18.4 e 20 milioni di sterline, sanzioni peraltro erogate in ammontare ridotto per tener conto dei danni economici prodotti dall'emergenza Covid-19.

In Italia non si registrano ancora sanzioni di tale portata, tuttavia un segnale di rigore è stato lanciato anche dal Garante italiano con la sanzione a Unicredit (provv. 10.06.2020) pari a 600.000 euro, sanzione che, seppur relativa a una violazione precedente all'entrata in vigore del GDPR, si è approssimata molto al massimo edittale comminabile secondo la legge applicabile *ratione temporis*.

Nella gran parte dei casi di *data breach* notificati (dal 25 maggio 2018 al 30 giugno 2020 risultano notificati 2759 casi di *data breach*, ma solo i principali sono stati pubblicati e rappresentano comunque la punta dell'*iceberg* rispetto al totale di cyber attack "*sommersi*") il Garante ha ritenuto di poter archiviare l'istruttoria nei confronti dell'impresa notificante oppure è intervenuto con provvedimenti prescrittivi di correzione e implementazione di misure di sicurezza adeguate, salvi alcuni casi di sanzioni nell'ordine di diverse decine di migliaia euro (ad es. provv. Università degli studi di Roma La Sapienza del 23 gennaio 2020).

NUNZIANTE • MAGRONE

Alert
Privacy - Review

Smart working in tempi di pandemia e gestione rischio cyber

Come noto, uno degli effetti della pandemia nella vita delle imprese è stato il diffuso ricorso allo *smart-working* onde poter consentire la prosecuzione dell'attività lavorativa degli impiegati al di fuori dai locali aziendali, che è avvenuto - almeno durante la prima ondata – con una tempistica pressoché improvvisa che non sempre ha dato tempo alle imprese, che non vi facevano regolare ricorso prima, di farsi trovare pronte.

E' evidente che consentire in tempo di pandemia ai propri dipendenti di lavorare in modalità *smart working*, soprattutto se la prestazione lavorativa viene svolta attraverso *devices* personali (in modalità c.d. "*Bring your own device – BYOD*") non dotati delle misure di sicurezza aziendali e quindi, con alta probabilità, scarsamente *compliant* con l'art. 32 GDPR, esponga il patrimonio informativo aziendale (ivi compresi i dati personali di terzi trattati dallo *smart worker* per conto della propria impresa) al rischio di accessi indebiti e di *cyber attack* e indirettamente pertanto al rischio sanzionatorio cui sopra si è accennato. L'impresa infatti, come si è visto, risponde della *compliance* in qualità di Titolare o Responsabile del trattamento, anche se la violazione è avvenuta a livello dei sistemi IT in uso al singolo dipendente.

Appare senz'altro opportuno anzitutto che le imprese che ricorrono a tale modalità lavorativa aggiornino l'analisi di rischio conformemente alle previsioni di cui all'art. 32 GDPR, affinché questa prenda in considerazione le specificità dello *smart working* nella singola impresa, così che i nuovi rischi nascenti da tale modalità di lavoro vengano analizzati e mitigati con misure adeguate, non solo sotto il profilo tecnologico, ma anche organizzativo.

Imprescindibile in tale ottica quindi non solo l'adozione di misure di sicurezza da applicare a dispositivi e connessioni remote adeguate ai nuovi rischi (da valutare oltre che ovviamente sotto il profilo tecnico-informatico anche sotto il profilo legale-laburistico ove dall'applicazione di filtri, tecniche e *alert* specifici possa derivare un rischio di controllo remoto della prestazione lavorativa) ma anche l'integrazione degli atti di designazione degli autorizzati al trattamento *ex* art. 2-*quaterdecies* del D.Lgs. 196/2003 (il "Codice Privacy Italiano") così da fornire istruzioni più specifiche e formazione adeguata ai dipendenti, indicando i comportamenti più idonei da adottare anche in relazione alle misure di sicurezza integrative adottate dalla propria impresa di appartenenza.

09.12.2020

Laura Sini, Associate
E: l.sini@nmlex.it
T.: +39 02 657 5181

www.nunziantemagrone.it

Per chiarimenti o informazioni potete contattare l'autore oppure il Vostro Professionista di riferimento all'interno dello Studio