Civile

Trasformazione digitale: perché Privacy, Data Protection e Cybersecurity giocano un ruolo fondamentale

*di Giovanna Boschetti**
19 Aprile 2022

La trasformazione all'interno delle aziende riflette il profondo mutamento del sistema di interazione e connessione tra le persone fisiche, c.d. *smart system*, un sistema fluido in cui, nelle abitudini di vita e di consumo, sfumano sempre più i confini tra fisico e virtuale

NT+ Contenuto esclusivo Norme & Tributi Plus

Il fenomeno della trasformazione digitale è un processo che coinvolge aspetti materiali ed organizzativi del mondo delle aziende: Machine Learning, Cloud Technology, Internet of Things, Artificial Intelligence, Big Data diventano i termini protagonisti di un nuovo vocabolario, di un nuovo modello di business, di un nuovo approccio al lavoro.
La trasformazione all'interno delle aziende riflette il profondo mutamento del sistema di interazione e connessione tra le persone fisiche, c.d. *smart system*, un sistema fluido in cui, nelle abitudini di vita e di consumo, sfumano sempre più i confini tra fisico e virtuale.
In tale contesto, la corretta applicazione della normativa di Privacy/Data Protection e Cybersecurity costituisce un pilastro centrale per la corretta impostazione e protezione del sistema di *Digital Transformation* nel suo complesso.

Stampa

È noto a tutti che il mancato rispetto del Regolamento 679/2016 ("GDPR") da parte delle aziende comporta elevati rischi non soltanto in termini di sanzioni da parte dell'Autorità Garante della Privacy (fino a 20milioni di euro o al 4% del fatturato), ma anche in termini di inutilizzabilità del database, di danno reputazionale, di calo dei profitti e di perdita di quote di mercato.
Non solo: la normativa in materia di cibersicurezza internazionale e nazionale ha avuto importanti sviluppi soprattutto nell'ultimo biennio, definendo precisi requisiti per determinate categorie di fornitori e di sistemi tecnologici, nell'ottica di offrire alle aziende concrete garanzie di riservatezza, integrità e disponibilità dei dati aziendali; sussiste peraltro un accordo di collaborazione tra dell'Autorità Garante della Privacy e l'Agenzia per la Cibersicurezza Nazionale.
Oggi l'adozione un corretto modello di Privacy/Data Protection e Cybersecurity è indispensabile non soltanto per la conformità normativa ma per la concreta efficacia del processo di trasformazione digitale: quali, dunque, i focus?
1) **Valutazione dei processi nella fase di progettazione lato privacy by design e privacy by default**
Gli aspetti di trattamento di dati personali devono essere incorporati nel processo di trasformazione tecnologica sin dall'inizio secondo i principi di privacy by design (definizione dell'architettura

informatica, verifica dell'interazione dei flussi in considerazione della tipologia dei dati trattai) e privacy by default (attivazione dei processi per impostazione predefinita). In difetto, taluni aspetti del processo possono risultare in corso d'opera superflui o dannosi.

2) **Valutazione della sicurezza dell'infrastruttura tecnica e dei flussi di lavoro**

La sicurezza è un aspetto fondamentale dei sistemi su cui si regge la trasformazione tecnologica e costituisce sinonimo di business continuity: la normativa interna ed internazionale è in costante evoluzione e ogni sistema deve essere verificato secondo più aggiornati requisiti normativi di sicurezza dei sistemi tecnologici e dei provider. Una valutazione non attenta sul punto espone a gravi responsabilità e conseguenze anche dirette sotto il profilo del risarcitorio.

3) **Acquisizione delle necessarie garanzie/certificazioni da parte dei fornitori**

La verifica dei contratti con i fornitori di servizi permette di ottenere tutte le opportune attestazioni di conformità che sono richieste dalle normative vigenti e di avere, in concreto, le necessarie garanzie in riferimento alle prestazioni della tecnologia implementata. In assenza di questa valutazione, effettuare correttivi in un secondo momento determina ingenti costi per le aziende.

4) **Mappatura dei flussi dei dati**

La mappatura dei flussi di dati garantisce il controllo delle attività di processo svolte in azienda e permette la corretta redazione del registro delle attività di trattamento, che costituisce il cardine del sistema di rendicontazione per l'Autorità Garante della Privacy. In difetto di tale mappatura i processi di business non possono dirsi validati.

5) **Valutazione del rischio e valutazione d'impatto del trattamento nei confronti degli interessati**

La valutazione del rischio determina la misura di responsabilità del titolare; la valutazione d'impatto si estende alla misurazione del rischio del trattamento per i diritti e le libertà sulle persone fisiche interessate dal trattamento. Omettere tale valutazione significa, in concreto, non effettuare una corretta programmazione e quantificazione dei vantaggi del processo

6**) Implementazione di tutti gli opportuni meccanismi di garanzia nei confronti dei consumatori/utenti/social users**

La "Carta dei Diritti" dei consumatori e degli utenti, e di tutti gli stakeholders, che costituisce un requisito fondamentale delle informative, non è lettera morta: occorre avere implementato gli opportuni meccanismi atti a garantire l'esercizio dei diritti ed il tempestivo riscontro agli interessati in azienda. La mancata implementazione di tali meccanismi espone a concreti rischi nell'incapacità dell'azienda di far fronte a istanze o segnalazione di interessati, che costituiscono la prima fonte di innesco delle attività ispettive dell'Autorità Garante della Privacy.

7) **Adozione di un modello di organizzazione e gestione dei dati personali**

Il modello di organizzazione e gestione dei dati personali permette di analizzare, pianificare e strutturare in azienda un sistema efficace che preveda la corretta attribuzione dei ruoli e l'allocazione delle responsabilità interne. In assenza di tale modello, il titolare del trattamento non è in grado di controllare il processo e di valutare gli eventuali gap.

8) **Implementazione dei controlli e delle procedure a presidio del sistema**

Nessun sistema è utilmente concepito senza un sistema di controlli e di procedure che possa costituire presidio del sistema. L'assenza di un sistema di controllo e presidio espone l'azienda a danni derivanti dall'inosservanza delle regole tecniche e operative di sistema.

9) **Formazione delle nuove competenze in azienda**

La formazione del personale in azienda, con particolare riguardo anche alla formazione privacy, data protection e cybersecurity integra una misura di sicurezza ai sensi del GDPR. Un'azienda priva delle necessarie competenze perde una fondamentale leva di sviluppo e competitività.

Il processo di trasformazione digitale costituisce una priorità strategica per qualsiasi azienda: questo processo non può limitarsi a toccare gli strumenti operativi aziendali ma deve necessariamente includere un corretto modello organizzativo di Privacy, *Data Protection* e Cybersecurity.

**a cura dell' Avv. Giovanna Boschetti, Counsel, Studio CBA*

Il Sole 24 ORE aderisce a The Trust Project

P.I. 00777910159 | © Copyright Il Sole 24 Ore Tutti i diritti riservati

Il Sole 24 ORE