LA RIVISTA DEI DIRETTORI AMMINISTRATIVI E FINANZIARI

4 Anno 14 - n. 4
Ottobre 2017
Trimestrale
Copia omaggio

ANDAF magazine

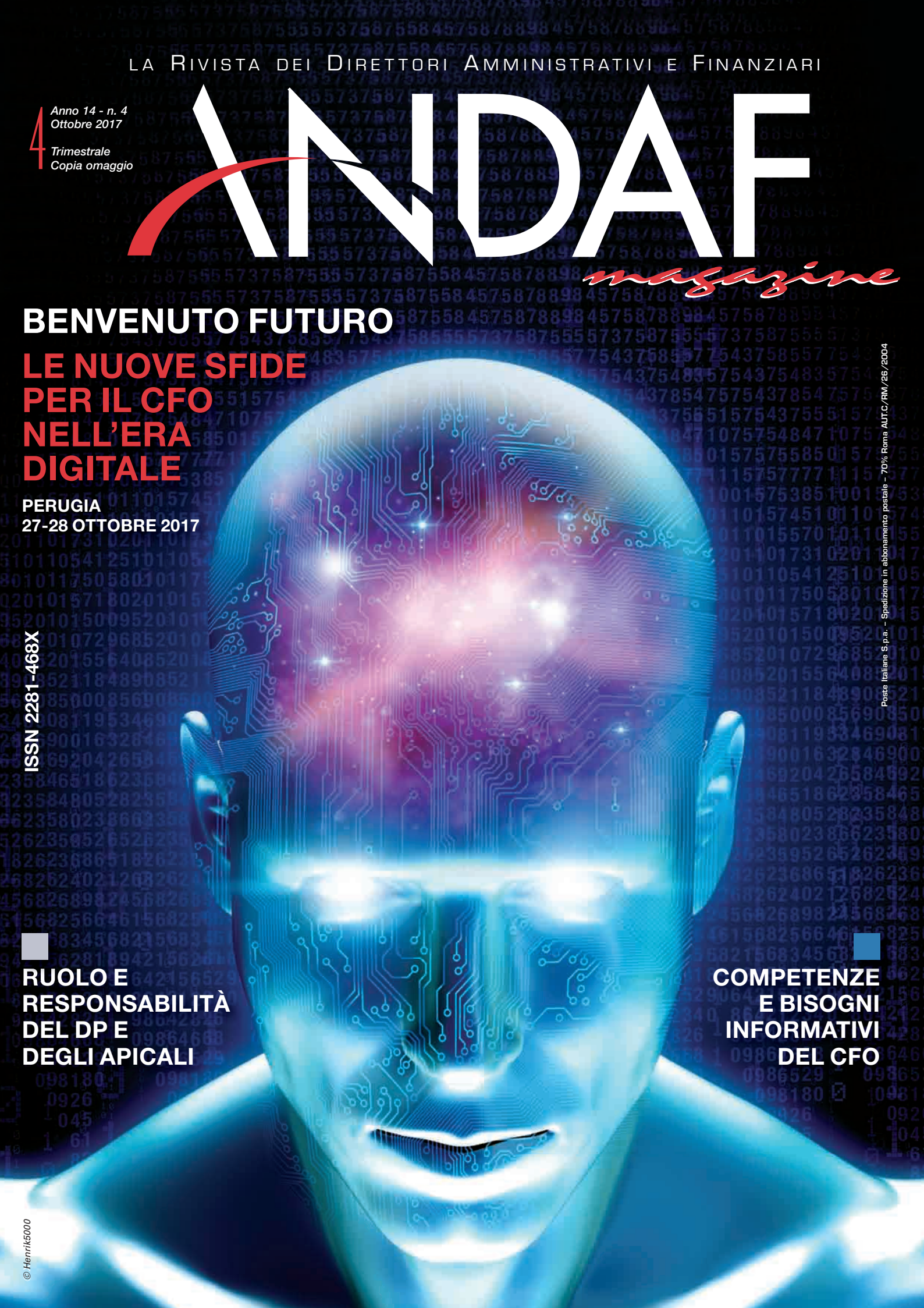
BENVENUTO FUTURO

LE NUOVE SFIDE PER IL CFO NELL'ERA DIGITALE

PERUGIA
27-28 OTTOBRE 2017

ISSN 2281-468X

Poste Italiane S.p.a. – Spedizione in abbonamento postale – 70% Roma AUT.C./RM/26/2004



RUOLO E RESPONSABILITÀ DEL DP E DEGLI APICALI

COMPETENZE E BISOGNI INFORMATIVI DEL CFO

GENERAL DATA PROTECTION REGULATION

TRA OBBLIGHI DI COMPLIANCE E NECESSITÀ DI RAFFORZAMENTO DELLA CYBERSECURITY

A MENO DI UN ANNO DALLA SCADENZA PER METTERSI IN REGOLA CON LE DISPOSIZIONI DEL GDPR, LE AZIENDE DEVONO VALUTARE GLI IMPATTI CHE LA NUOVA NORMATIVA IN AMBITO PRIVACY HA SULLE PROPRIE ATTIVITÀ E DEFINIRE UN PIANO D'AZIONE DI DETTAGLIO PER NON RISCHIARE DI FARSI TROVARE IMPREPARATE. IL GDPR RICHIEDE INOLTRE ALLE AZIENDE UNA APPROFONDITA VERIFICA DELLA PROPRIA SICUREZZA INFORMATICA, CREANDO UN'OPPORTUNITÀ NON PIÙ RINVIABILE

di ROBERTO CECILIA SANTAMARIA
Country Managing Partner Agic Technology

e MARCELLO MANCINI
Associate Partner aiComply

Una rapida *overview* sul GDPR

Il Regolamento UE n. 679/2016 (anche *"General Data Protection Regulation"* o GDPR), che diventerà direttamente applicabile dal 25 maggio 2018, nasce con l'obiettivo di armonizzare le Leggi sulla *privacy* di 28 Paesi Membri e introduce al contempo importanti novità in materia di protezione dei dati.

In Italia, il GDPR succederà al D.Lgs. 196/2003 (noto anche come "Codice della *Privacy*"), figlio della Direttiva 95/46/CE emanata in un periodo storico (l'anno era il 1995) in cui le aziende trattavano i dati personali principalmente in modalità cartacea, telefonicamente e via fax.

Con il continuo avanzamento del progresso tecnologico – si pensi ad esempio all'*e-commerce*, all'*Internet of Things* (IoT) e al mondo dei *social network* – gli scenari in cui si trovano a operare oggigiorno le aziende sono mutati completamente.

Una totale riforma della normativa sulla *privacy* si è resa pertanto indispensabile per regolamentare il trattamento dei


DATA
PROTECTION
GDPR

dati personali attraverso le nuove tecnologie e lo scambio degli stessi tra i vari Paesi.
Con l'entrata in vigore del Regolamento UE, ciò che principalmente cambia rispetto alla previgente normativa è l'approccio alle problematiche legate alla riservatezza e alla sicurezza dei dati personali.
Ai sensi del GDPR, ciascuna azienda dovrà infatti considerare il tema della *privacy* preliminarmente all'avvio di ogni attività o servizio *(Privacy by Design)*, nonché definire e implementare idonee misure di sicurezza del dato.

Più nel dettaglio, tra le principali novità introdotte dal GDPR si evidenziano quelle relative alle seguenti tematiche:

- *Accountability:* principio teso a responsabilizzare i titolari del trattamento, affinché questi adottino approcci e politiche che tengano conto del rischio che un determinato trattamento di dati personali possa rappresentare per i diritti e le libertà degli interessati.

- *Privacy Impact Analysis* (PIA): ciascun titolare del trattamento deve effettuare, nei casi previsti dalla normativa, una valutazione di impatto sulla protezione dei dati. Ciò comporta la necessità di valutare in via preliminare l'impatto, dal punto di vista della *privacy*, di ogni operazione di trattamento dei dati che sarà svolta (rif. art. 25 del GDPR: *"Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita"*).

- *Data Protection Officer* (DPO): nuova figura introdotta dal GDPR. Si tratta di un professionista con i compiti di informare e fornire consulenza al titolare del trattamento, sorvegliare sull'osservanza della normativa di riferimento, nonché delle politiche del titolare del trattamento, fornire – se richiesto – un parere in merito alla valutazione d'impatto sulla protezione dei dati, cooperare con l'autorità di controllo e fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento.

- Diritti degli interessati: diversi sono i diritti riconosciuti all'interessato dal GDPR. In particolare: a) il **diritto di accesso** che comporta il diritto di ricevere una copia dei dati oggetto di trattamento; b) il **diritto all'oblio**, cioè il diritto di cancellazione dei dati, che prevede che l'interessato possa richiedere la cancellazione dei propri dati anche dopo la revoca del consenso; c) il **diritto di limitazione del trattamento** che si applica anche solo se l'interessato chiede la rettifica dei dati o si oppone al loro trattamento; d) il **diritto alla portabilità dei dati** che si applica in presenza del consenso dell'interessato o per l'adempimento di obblighi contrattuali e limitatamente ai dati forniti dall'interessato stesso.

- Notifica delle violazioni: obbligo di notificare all'autorità di controllo violazioni di dati personali di cui si è a conoscenza entro 72 ore, se si ritiene che da tale violazione derivino dei rischi. È altresì previsto l'obbligo di notificare la violazione al diretto interessato quando il *breach* (la violazione) sia tale da poter determinare un rischio elevato per i diritti e le libertà fondamentali dell'interessato.

- Trasparenza: l'articolo 5, paragrafo 1, lettera a) del GDPR, prescrive che i dati personali siano trattati in modo trasparente nei confronti dell'interessato. La trasparenza è pertanto un elemento costitutivo fondamentale della responsabilizzazione del titolare del trattamento.

- Registro delle attività di trattamento: nei casi previsti dal GDPR, le aziende devono tenere un registro delle attività di trattamento svolte. Evidente è il legame tra il registro dei trattamenti e il Documento Programmatico sulla Sicurezza (DPS) inizialmente previsto dal D.Lgs. 196/2003, poi abolito dal D.L. 9 febbraio 2012, n. 5, convertito, con modificazioni, dalla Legge 4 aprile 2012, n. 35.

Il principio della *Privacy By Design*

La *Privacy By Design* è un principio chiave e del tutto innovativo introdotto dal Regolamento UE, che stabilisce l'obbligo di garantire la protezione dei dati dell'interessato, fin dalla fase di ideazione di un trattamento o di progettazione di un sistema informativo, e volto all'adozione di tutti i presidi necessari per prevenire trattamenti illeciti.
In altre parole, tale principio implica che le aziende trattino solo i dati indispensabili per lo svolgimento di una specifica attività o per l'erogazione di un determinato servizio e che venga limitato l'accesso alle informazioni solo a coloro che dovranno effettivamente "lavorare" il dato.

Il titolare del trattamento deve quindi rispettare il principio della *Privacy By Design*, tanto nello svolgimento delle attività di processo, quanto in ogni fase di progettazione, sviluppo, implementazione e utilizzo di un *software*.
A ben vedere, si tratta di un'importante novità quella introdotta dal GDPR, in quanto obbliga le aziende a rivedere i loro processi valutativi e decisionali in modo da assicurare il rispetto del principio della *Privacy By Design*.
Ciascuna azienda dovrà infatti, già in fase di ideazione/progettazione di un'attività, di un servizio o di un sistema informativo, effettuare un'accurata analisi dei rischi *privacy* e un'attenta valutazione dell'impatto sulla protezione dei dati personali, al fine di tenere in considerazione – nelle successive fasi di sviluppo, di implementazione ed esecutive – tutti gli aspetti relativi alla protezione dei dati personali e adottare idonee misure organizzative e tecniche per mitigare i rischi della *privacy*.

La *Privacy By Design* non deve ovviamente essere intesa come una valutazione finalizzata a se stessa, ma deve piuttosto rappresentare lo strumento che consente alle aziende di definire quel *set* di misure di sicurezza ritenute più idonee per un determinato tipo di trattamento. A titolo meramente esemplificativo, per una corretta applicazione del

principio della *Privacy By Design*, le aziende devono prevedere l'adozione di misure di sicurezza per la protezione dei dati personali quali la pseudonimizzazione, la cifratura, la *business continuity*, ecc.
La *ratio* sottostante all'introduzione del principio della *Privacy By Design* è strettamente collegata al fatto che, nei prossimi anni, la totalità dei trattamenti dei dati avverrà tramite sistemi informativi e reti *internet* e che la percentuale della popolazione mondiale connessa continuerà ad aumentare.

In tale prospettiva, si registrerà una crescita dello scambio di dati attraverso *social network, e-mail* e reti *internet,* e del numero dei device degli utenti connessi tra di loro.
Il punto di attenzione del Legislatore comunitario non poteva pertanto fare altro che spostarsi verso le nuove tecnologie (IoT, per esempio), con l'intento di definire un *set* di regole volte a garantire la sicurezza in un contesto i cui confini sono difficili da tracciare e quindi da monitorare.
In tale scenario, il GDPR vuole tutelare l'interessato e i suoi dati personali attraverso il principio della *Privacy By Design*, riducendo in modo significativo il rischio di violazione della riservatezza, piuttosto che della perdita dei dati o dell'accesso non autorizzato alle informazioni.

Privacy e *Cybersecurity*, due temi con diversi punti in comune

In maniera sempre più repentina, purtroppo anche a causa dell'aumento di attacchi informatici subiti da imprese di tutto il mondo, le aziende si sono ormai addentrate nell'era in cui la sicurezza informatica (la cosiddetta *cybersecurity*) acquisisce un ruolo chiave e, pertanto, la gestione e la sicurezza dei dati sono divenuti un elemento centrale da considerare in tutti i settori di *business* delle aziende.
Anche il Legislatore comunitario, pienamente consapevole dell'importanza di tale tema, pone un forte accento alla sicurezza all'interno del GDPR, definendola come un insieme di misure tecniche e organizzative a tutela dei dati.
Pertanto, l'innovazione delle tecnologie, l'intensificarsi degli attacchi cibernetici e l'adeguamento della normativa *privacy* impongono alle aziende una attenta ed efficace gestione della sicurezza dei dati.

Diventa quindi strategico adottare un approccio integrato della sicurezza, che consideri contestualmente sia aspetti organizzativi, che tecnologici e informatici.
Inoltre, nello scenario in via di definizione, le aziende non devono intendere la sicurezza come un'esclusiva competenza del Responsabile dei Sistemi Informativi; piuttosto, si tratta di un tema che deve coinvolgere la Direzione fin dalle iniziali fasi decisionali e che necessita di competenze di vario genere: dalle conoscenze organizzative, di processo e legali a quelle tecniche e informatiche.

È anche opportuno sottolineare che le misure di sicurezza che ciascuna azienda necessita implementare devono essere valutate sia da un punto di vista tecnico che economico (definizione di *budget*, piani di investimento, ecc.). Tali valutazioni dovrebbero essere integrate nei processi decisionali di ogni impresa, come sostiene anche l'OCSE nella nuova "Raccomandazione sulla sicurezza digitale e la gestione del rischio".
Per quanto concerne la sicurezza informatica, a differenza del D.Lgs. 196/2003 prossimo all'abrogazione, il GDPR non definisce un livello minimo ma lascia libertà alle aziende, richiedendo a queste un approccio *risk based*.
Le misure di sicurezza da implementare dovranno pertanto essere quelle che ciascuna azienda valuta come adeguate in relazione ai rischi insiti al trattamento e agli eventuali impatti che da tali rischi possano derivare rispetto alla protezione dei dati. Ciascuna impresa deve pertanto effettuare un *risk assessment* e implementare un processo di gestione del rischio nel tempo.
In questo panorama, il GDPR offre l'opportunità alle aziende di ripensare e potenziare le loro misure di sicurezza, in modo anche da prevenire i *cybercrime* causati da *virus, war*, *trojan, rootkit,* ecc.

Tra l'altro, a seguito del verificarsi sempre più frequente di fenomeni connessi al *cybercrime*, che hanno avuto diverse aziende e soggetti privati come vittime, si ravvisa un diffuso bisogno di adeguare la sicurezza delle aziende.
Giusto per fornire alcuni dati utili a dimensionare l'importanza del *cybercrime* su scala mondiale, nel corso del 2016 sono state vittime di *cyber attack* organizzazioni e aziende *leader* mondiali (quelle che spendono somme consistenti di denaro nella sicurezza informatica, per intenderci). Si pensi, ad esempio, alla University of Central Florida che ha riferito di un attacco informatico durante il quale sono stati trafugati dati personali di circa 63.000 tra studenti e personale dipendente, oppure al caso Yahoo! che ha dichiarato la violazione di circa 500.000.000 di *account e-mail,* o altri casi ancora che hanno interessato Cisco, LinkedIn, Deutsche Telekom, Twitter e altri.

E il *trend* degli attacchi informatici nel 2017 non sembra diminuito, si pensi ad esempio ai recenti casi che hanno interessato l'azienda multinazionale del settore *pharma* Merck o lo studio legale DLA Piper, o da ultimo all'attacco alla Unicredit che ha coinvolto circa 400.000 clienti italiani dell'istituto bancario.
Stando alle statistiche, non esistono segmenti di mercato immuni ai rischi di una violazione, anche solo accidentale.
L'Italia come si posiziona in questo scenario?
Secondo alcune statistiche, l'Italia è al secondo posto nella lista dei Paesi con la quota più elevata di utenti attaccati dagli *encryptor* (programmi dannosi) e al terzo in quella delle nazioni in cui gli utenti sono risultati maggiormente esposti al rischio di infezioni online.

Tutto ciò premesso, se si considera che a seguito di ogni attacco corrisponde – oltre alla perdita di dati – anche un fermo delle attività di *business*, necessario per ripristinare tutti i sistemi, il suggerimento non può essere che quello di

prevenire tali eventi sfruttando possibilmente anche le disposizioni contenute nel GDPR.
Per una competa analisi sul tema, va anche detto che una diretta conseguenza del *cybercrime* è quello che nel GDPR viene definito *data breach*.
Il GDPR, all'art. 4, definisce infatti la violazione dei dati personali come la violazione di sicurezza che comporta – accidentalmente o in modo illecito – la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
Inoltre, nel caso si verifichi un *data breach*, sul titolare del trattamento ricadranno determinati obblighi (i.e. notificazione).
Proviamo allora a immaginare le conseguenze, per un'azienda, del verificarsi di un *data breach*: perdita della fiducia da parte dell'interessato (e se l'interessato è un cliente, possibile perdita della clientela), danno reputazionale e di immagine a seguito della diffusione della notizia, interruzione del *business* con conseguenti perdite economiche, ispezioni da parte delle autorità preposte al controllo (Banca d'Italia, Consob, ecc.). A tutto ciò va anche aggiunto il regime sanzionatorio e il risarcimento del danno!
Ecco quindi che il GDPR pone in evidenza la sensibilità del Legislatore comunitario nei confronti delle nuove tecnologie, in quanto mezzi principali per il trattamento dei dati, e delle misure di sicurezza finalizzate a mitigare il rischio del *cybercrime*.
La gestione della sicurezza per rispondere agli obblighi previsti dal GDPR passa per un approccio *cybersecurity oriented*.

Le aziende devono pertanto rivedere il loro approccio alla sicurezza ponendo in essere azioni quali, ad esempio:

- adottare pratiche di *secure coding* fin dalla scrittura del codice di un programma;

- effettuare *test* per individuare difetti, debolezze o errori all'interno di un *software*, al fine di intervenire tempestivamente sulle vulnerabilità;

- pianificare ed effettuare verifiche sulla sicurezza informatica e, ove necessario, investimenti nella *cybersecurity*.

Tali azioni devono essere tutte indirizzate al raggiungimento di un livello di sicurezza in grado di contrastare i rischi di distruzione, perdita, modifica e divulgazione non autorizzata dei dati personali, e al loro accesso accidentale o illegale.

Le sanzioni del GDPR
Le violazioni del GDPR possono comportare l'applicazione di sanzioni con importi da capogiro.
In termini generali, la violazione delle disposizioni contenute nel GDPR può prevedere sanzioni amministrative pecuniarie fino a 20 milioni di euro, oppure fino al 4% del fatturato mondiale totale annuo del trasgressore.
Risulta quindi evidente che il Legislatore comunitario, nel definire il sistema sanzionatorio, si è basato sul principio della prevenzione, con l'intento di dissuadere le imprese dall'accettazione del rischio di non essere *compliant* con la nuova normativa.
La non conformità alle disposizioni del GDPR potrebbe inoltre comportare conseguenze ben più gravi di quelle derivanti dall'applicazione della sanzione amministrativa: si pensi, ad esempio, al caso di illiceità del trattamento dei dati effettuato da un'azienda, e quindi alla necessaria interruzione di un servizio o di un'attività già in atto con ovvie ripercussioni sui clienti, i quali potrebbero anche adire alle vie legali per ottenere il risarcimento dei danni subiti.

Adottare un corretto e completo approccio al GDPR
A meno di un anno dalla scadenza per adeguarsi alle disposizioni in ambito *privacy* introdotte dal Regolamento UE, le aziende devono avviare un "percorso" strutturato finalizzato a favorire il passaggio al GDPR e al mantenimento dei requisiti richiesti dalla normativa nel tempo.
Una strada percorribile dalle imprese potrebbe essere quella di effettuare un ***assessment* iniziale** volto a valutare il livello di rispondenza al disposto normativo.
Successivamente, in base ai risultati dell'*assessment* iniziale, è opportuno **definire un piano degli interventi** necessari per adeguarsi al GDPR stabilendo responsabilità e tempistiche, in modo da rispettare la data del 25 maggio 2018.
Lo *step* successivo è quello di **implementare le azioni di adeguamento** per la piena conformità ai requisiti stabiliti dal GDPR.
Infine, è necessario assicurare nel tempo il **mantenimento della conformità al GDPR** attraverso, ad esempio, la ripetizione di *assessment*, l'esecuzione di verifiche e di sessioni formative.
È utile precisare che le analisi vanno svolte anche in riferimento all'infrastruttura tecnologica e ai vari *asset*, in maniera da individuare gli interventi necessari per garantire la *cybersecurity*; si considerino, ad esempio, soluzioni atte a garantire la disponibilità del dato (es. *back up, policy* di *disaster recovery*, ecc.), la confidenzialità del dato (es. controlli preventivi quali la sicurezza logica) e l'integrità del dato (es. controlli detentivi quali *penetration test*).
I risultati delle analisi svolte dovranno confluire poi in un modello organizzativo che consideri gli aspetti *privacy* come tematiche fondamentali per tutte le attività di *business* e trasversali a tutti i processi aziendali.
Viste le specificità della normativa, resta inteso che la *compliance* al GDPR non possa prescindere dall'utilizzo di *tool* informatici di ultima generazione dotati delle misure di sicurezza logica conformi a soluzioni già ampiamente diffuse come quelle di Microsoft (*Azure, Dynamics 365, Office 365, SQL Server*, ecc.) o di altri produttori internazionali.

AGIC Technology

Protezione dei **dati personali**

General Data Protection Regulation

Un importante passo avanti verso la protezione dei dati personali e il rafforzamento della cybersecurity della vostra azienda. Agic Technology può aiutarvi in modo efficace a realizzare la conformità al Regolamento UE attraverso le tecnologie Microsoft.

GDPR

25 maggio 2018
data ultima per mettersi in regola!

#DIGITAL CUSTOMER EXPERIENCE

INFO & CONTATTI
www.agictech.com
info@agictech.com

DOVE SIAMO
Milano Roma Bologna
Napoli Brindisi Tirana

Gold
Microsoft Partner

Microsoft