Giancarlo Butti
Europrivacy

Il rispetto delle normative in tema di sicurezza e le opportunità per il business

Compliance with regulations on security and business opportunities

Sommario: *Le normative di carattere settoriale (relative al mondo finanziario, telco, infrastrutture critiche…) o applicabili a qualunque organizzazione (GDPR) che hanno fra i loro obiettivi diretti o indiretti la regolamentazione della sicurezza di un'organizzazione sono sempre più numerose.*

Gli adempimenti previsti per essere conformi a tali normative sono spesso considerati dalle organizzazioni solo come un costoso adempimento per essere compliance con la normativa, ma in realtà le misure di sicurezza richieste offrono alle aziende rilevanti vantaggi competitivi.

Abstract: *The sectorial set of rules (relating to the financial world, telco, critical infrastructures ...) or applicable to any organization (GDPR) that have among their direct or indirect objectives the regulation of the security of an organization are more and more increasing.*

The formalities required to comply with these regulations are often considered by the organizations only as an expensive formality to comply with the legislation, while the required security measures also offer to the companies significant competitive advantages.

1. Il perimetro di tutela

Sono solito iniziare i miei corsi in ambito privacy o sicurezza con la seguente espressione: "non esiste alcuna normativa che obbliga un'azienda a tutelare i propri asset, ma esistono normative che obbligando le aziende a tutelare altri asset, quali i dati personali, i propri collaboratori, gli stakeholder, tutelano indirettamente anche l'azienda".

Il concetto è chiaro ed immediato, tanto che diversi colleghi lo hanno fatto proprio.

Basta una semplice rassegna delle principali normative alle quali devono sottostare tutte le organizzazioni per verificarne la veridicità.

La normativa sulla **safety** (D.Lgs.81/08 e successive integrazioni) obbliga le organizzazioni a dotarsi, fra le altre, di misure antincendio, che ovviamente tutelano non solo i lavoratori, ma anche tutti gli **asset materiali** (e quelli immateriali in essi eventualmente contenuti) dell'azienda.

Le normative **privacy**, fra le quali il recente GDPR, obbligano le aziende a dotarsi di adeguate misure di sicurezza tecniche ed organizzative per tutelare i diritti e le libertà fondamentali delle persone

fisiche, con particolare riferimento al diritto alla protezione dei dati personali.

Per fare questo le aziende devono tutelare in particolare gli asset informativi nei quali sono presenti o transitano i dati personali dei soggetti interessati e sebbene questi siano un sottoinsieme (molto cospicuo) delle informazioni gestite da un'organizzazione, ne risultano tutelate di norma anche tutte le altre informazioni gestite dall'azienda e gli asset materiali che le contengono.

Già da soli questi due esempi costituiscono una valida dimostrazione dell'immediato ritorno economico per le organizzazioni derivante dall'applicazione della normativa.

È facile obiettare che il ritorno è esclusivamente di tutela; sono cioè protetti gli asset e le informazioni rispetto ad eventuali incidenti che nella realtà potrebbero non accadere mai e che le organizzazioni potrebbero mettere in atto altrimenti altre soluzioni, magari meno costose, quali un trasferimento di rischio ad una assicurazione.

2. Valutare i costi di un incidente di sicurezza

Le considerazioni espresse al precedente paragrafo potrebbero essere considerate valide se ci si limitasse ad una mera valutazione del rapporto fra i costi sostenuti per le misure di sicurezza implementate ed i costi derivanti dalla perdita di asset materiali/immateriali o peggio ancora in conseguenza di un infortunio di un collaboratore.

Tale valutazione dovrebbe inoltre tenere in debito conto il fatto che i costi delle implementazioni sono certi, mentre i costi di perdita/infortunio sarebbero da considerare solo nel caso in cui un evento avverso abbia luogo.

Tale valutazione è tuttavia non corretta.

In primo luogo, anche se non sarebbe del tutto corretto inserirlo nel nostro conteggio di costi e benefici, la corretta implementazione delle misure di sicurezza mette al riparo dalle sanzioni previste dalle specifiche normative di riferimento.

Tali sanzioni non sono da intendersi solo di natura economica o penale, ma ad esempio, nel caso della normativa privacy, potrebbero altresì comportare il blocco dei trattamenti dei dati personali e, nel caso più estremo, il blocco delle attività di un'organizzazione se questa dipende da tali trattamenti (si consideri ad esempio una società di mkt che si vede bloccare i database dei propri prospect).

Un incidente derivante dalla mancanza delle misure di sicurezza potrebbe portare alla perdita di informazioni importanti o vitali per l'azienda, al blocco dei server che erogano un servizio, al blocco di una linea di produzione.

Oltre al danno di natura prettamente materiale, si deve aggiungere il probabile danno di immagine per l'organizzazione, la cui quantificazione sebbene difficile è comunque possibile mediante tecniche reperibili in letteratura.

Se il danno subito ha come conseguenza il blocco temporaneo o definitivo della fornitura di un prodotto/servizio questo potrebbe

comportare conseguenze nella relazione con i clienti e all'attivazione di cause per inadempimento contrattuale.

Vanno inoltre aggiunti i costi di ripristino/riparazione derivanti dall'incidente che sono a loro volta condizionati dalle eventuali misure di sicurezza presenti (si pensi alla rottura di un disco fisso e alla conseguente perdita di dati il cui effettivo ripristino è condizionato dalla disponibilità di un backup o, in mancanza di questo, da una reimputazione manuale dei dati se questi sono disponibili su carta ovvero dal loro eventuale recupero presso terzi, se disponibili).

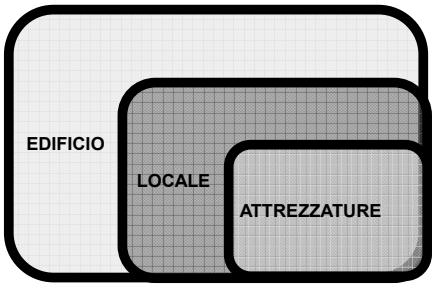

Figura 1 – Correlazione fra asset ai fini della valutazione dei rischi e delle relative contromisure (Fonte: Sicurezza totale, G. Butti ITER)

Descrizione bene	**Disco fisso**
Evento	Rottura
Impatti diretti	Perdita di dati Interruzione del servizio Costi di ripristino
Impatti indiretti	Perdite economiche (indirette e consequenziali) Perdita della clientela Impatti reputazionali (danni di immagine) Impatti legali

Descrizione bene	**Sito**
Evento	Distruzione
Impatti diretti	Inaccessibilità dei beni materiali ed immateriali presenti nell'edificio Distruzione parziale o totale dei beni presenti nell'edificio Costi di ripristino o attivazione di misure alternative
Impatti indiretti	Perdite economiche (indirette e consequenziali) Perdita della clientela Impatti reputazionali (danni di immagine) Impatti legali

Tabella 1 – Esempi delle conseguenze dirette, indirette di eventi avversi (Fonte: Sicurezza totale, G. Butti ITER)

Descrizione bene	**Materie prime**
Evento	Furto
Impatti diretti	Perdita economica Interruzione della produzione
Impatti indiretti	Perdite economiche (indirette e consequenziali) Perdita della clientela Impatti reputazionali (danni di immagine) Impatti legali

Eliminare il rischio	
Ridurre il rischio	Ridurre l'impatto Ridurre la probabilità
Trasferire il rischio	Assicurativo Non assicurativo
Accettare il rischio	

Tabella 2. IL trattamento del rischio residuo (Fonte: Sicurezza totale, G.Butti ITER)

3. La tutela delle informazioni riservate

La tutela delle informazioni riservate dovrebbe essere una delle principali preoccupazioni di un'azienda. Con tale termine si intendono le informazioni che consento all'azienda di mantenere un vantaggio competitivo sul mercato e sono costituite sia da informazioni di natura tecnica (ad esempio lo svolgimento di un processo industriale) sia di natura commerciale (ad esempio l'elenco dei propri clienti arricchito con informazioni che li caratterizzano dal punto di vista dell'azienda).

L'importanza di queste informazioni per le aziende è tale che il legislatore ha introdotto una loro autonoma tutela legale.

Al riguardo ci sono diversi motivi per cui il rispetto di normative come il GDPR consentano alle aziende di tutelare le proprie informazioni riservate e quindi il proprio know how.

In primo luogo è necessario mappare dettagliatamente le proprie informazioni, sia che queste siano presenti in database strutturati o in file destrutturati quali la posta elettronica o prodotti di produttività individuale.

Tale mappatura è infatti propedeutica alla individuazione dei dati personali trattati dalle aziende al fine della loro successiva protezione.

Inoltre questa attività, se effettuata con riferimento ai processi aziendali, consente di individuare anche le informazioni necessarie all'azienda per lo svolgimento della propria attività, ma che non sono formalizzate, ovvero quella componente del know how aziendale che è patrimonio implicito dei collaboratori[1].

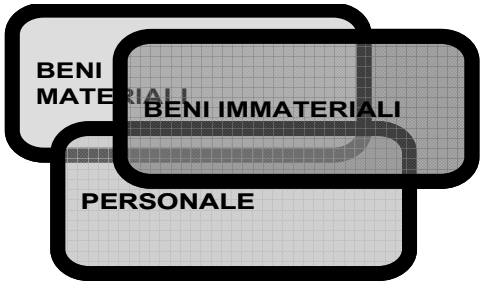

Figura 2. Relazione fra asset immateriali e gli asset materiali che li contengono (Fonte: Sicurezza totale, G.Butti ITER)

Gli strumenti di tutela dei dati personali, come già espresso in precedenza, portano a tutelare anche le informazioni che costituiscono il

[1] G. BUTTI, *La tutela del capitale intellettuale,* Il Mondo dell'intelligence – Sistema di Informazione per la sicurezza della Repubblica, Roma 2016,

know how aziendale; difficilmente infatti le misure tecniche ed organizzative messe in atto dall'azienda saranno limitate in modo puntale alla protezione dei dati personali (si pensi a firewall, antivirus, IDS, backup, credenziali di accesso differenziate…).

Ma c'è un secondo aspetto meno evidente che deriva da questa protezione "ereditata" dalle informazioni nel loro complesso.

L'articolo 98 del Codice di Proprietà Industriale (Legge n. 30/2005) che tutela i *segreti commerciali* (in precedenza *informazioni aziendali riservate*) così recita:

1) *Costituiscono oggetto di tutela le informazioni aziendali e le esperienze tecnico-industriali, comprese quelle commerciali, soggette al legittimo controllo del detentore, ove tali informazioni:*
   a) *siano segrete, nel senso che non siano nel loro insieme o nella precisa configurazione e combinazione dei loro elementi generalmente note o facilmente accessibili agli esperti ed agli operatori del settore;*
   b) *abbiano valore economico in quanto segrete;*
   c) ***siano sottoposte, da parte delle persone al cui legittimo controllo sono soggette, a misure da ritenersi ragionevolmente adeguate a mantenerle segrete.***

In altre parole tali informazioni per essere tutelate dalla legge devono essere protette da misure di sicurezza tali per cui possano rimanere segrete.

Appare quindi evidente che un database o una cartella di rete ai quali siano stati applicati dei criteri di sicurezza, in quanto contenenti dati personali, garantiscono che anche le altre informazioni, considerate segrete dall'azienda, siano automaticamente tutelate dalla legge.

Al riguardo è importante ricordare che altrimenti, un'informazione considerata segreta dall'azienda, ma non protetta mediante misure tecniche e/o organizzative, non è tutelata dal Codice di Proprietà Industriale.

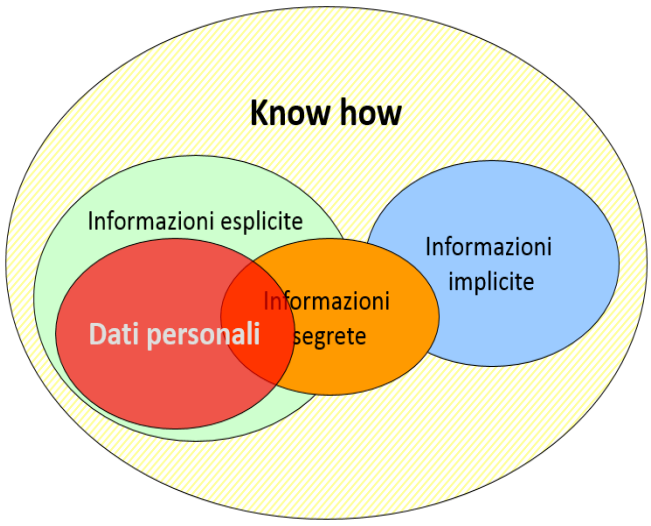

Figura 3. Relazione fra know how, informazioni segrete e dati personali

Anche la normativa safety tutela indirettamente le informazioni riservate, in quanto tutela i lavoratori (oltre agli asset aziendali rispetto al rischio indicendio…). Come più sopra specificato le informazioni implicite sono patrimonio dei singoli collaboratori ed un loro infortunio o decesso può portare ad una temporanea o definitiva indisponibilità di tali informazioni con conseguenze che difficilemente le aziende sono in grado di valutare preventivamente.

4. La continuità del business

In questo paragrafo verrà presentata una rassegna delle normative che obbligano le aziende a garantire la continuità nella erogazione dei loro servizi (l'argomento è particolarmente significativo, per cui per una trattazione più dettagliata si rimanda all'articolo **Aziende resilienti** su questo stesso numero della rivista **La Comunicazione - Note, Recensioni & Notizie**).

Tali normative possono riguardare settori specifici, quali le banche o le PA, oppure indistintamente tutti i soggetti che trattano dati personali, quali il GDPR.

Recente è inoltre l'attivazione della **DIRETTIVA (UE) 2016/1148 (NIS)** il cui recepimento in Italia è operativo dal 26 giugno del 2018 tramite il **DECRETO LEGISLATIVO 18 maggio 2018, n. 65**.

Nelle tabelle seguenti sono riportati gli articoli delle principali normative che hanno attinenza alla resilienza ed alla continuità operativa.

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)
Articolo 32 Sicurezza del trattamento 1.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 del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: … b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

Tabella 3. Regolamento (UE) 2016/679 - GDPR

Titolo IV – Governo societario, controlli interni e gestione dei rischi **Capitolo 4 – Il sistema informativo** **Sezione IV – La gestione della sicurezza informatica**
7. La disponibilità delle informazioni e delle risorse ICT *…* *— in relazione alle esigenze di disponibilità delle singole applicazioni, sono definite procedure di backup (di dati, software e configurazione) e di ripristino su sistemi alternativi, in precedenza individuati;* *— le architetture sono disegnate in considerazione dei profili di sicurezza informatica delle applicazioni ospitate, tenendo conto di tutte le risorse ICT e di supporto interessate (alimentazione elettrica, impianti di condizionamento, ecc.); a tale riguardo, l'intermediario valuta la necessità di predisporre piattaforme particolarmente robuste e ridondate (ad es., applicando il principio del no single point of failure) volte a garantire l'alta disponibilità delle applicazioni maggiormente critiche, in sinergia con le procedure e il sistema di disaster recovery;* *— in funzione dei profili di rischio delle comunicazioni, delle applicazioni e dei servizi acceduti, i collegamenti telematici interni alla banca o al gruppo sono opportunamente ridondati; in relazione al rischio di incidenti di sicurezza informatica che possono determinare l'interruzione dei servizi (ad es., mediante attacchi di tipo denial of service o distributed denial of service), oltre a soluzioni specifiche per l'individuazione e il blocco del traffico malevolo, la banca valuta l'opportunità di sfruttare procedure e strumenti per l'allocazione dinamica di capacità trasmissiva ed elaborativa;*
Titolo IV – Governo societario, controlli interni e gestione dei rischi **Capitolo 5 – La continuità operativa** **Allegato A – Requisiti per la continuità operativa** **Sezione II – Requisiti per tutti gli operatori**
1. Ambito del piano di continuità operativa **2. Analisi di impatto** **3. Definizione del piano di continuità operativa e gestione delle crisi** *3.1 Ruolo degli organi aziendali* *3.2 I processi critici* *3.3 La responsabilità del piano di continuità operativa* *3.4 Il contenuto del piano di continuità operativa* *3.5 Le verifiche* *3.6 Le risorse umane* *3.7 Esternalizzazione, infrastrutture e controparti rilevanti* *3.8 Controlli* *3.9 Comunicazioni alla Banca d'Italia e alla Banca centrale europea*

Tabella 4. Circolare 285 Banca d'Italia

Articolo abrogato dal D.LGS. 26 Agosto 2016, n. 179
Art. 50-bis. Continuità operativa. *1. In relazione ai nuovi scenari di rischio, alla crescente complessità dell'attività istituzionale caratterizzata da un intenso utilizzo della tecnologia dell'informazione, le pubbliche amministrazioni predispongono i piani di emergenza in grado di assicurare la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività.* *2. Il Ministro per la pubblica amministrazione e l'innovazione assicura l'omogeneità delle soluzioni di continuità operativa definite dalle diverse Amministrazioni e ne informa con cadenza almeno annuale il Parlamento.* *3. A tali fini, le pubbliche amministrazioni definiscono:* *a) il piano di continuità operativa, che fissa gli obiettivi e i principi da perseguire, descrive le procedure per la gestione della continuità operativa, anche affidate a soggetti esterni. Il piano tiene conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche e contiene idonee misure preventive. Le amministrazioni pubbliche verificano la funzionalità del piano di continuità operativa con cadenza biennale;* *b) il piano di disaster recovery, che costituisce parte integrante di quello di continuità*

operativa di cui alla lettera a) e stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione. DigitPA, sentito il Garante per la protezione dei dati personali, definisce le linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche, verifica annualmente il costante aggiornamento dei piani di disaster recovery delle amministrazioni interessate e ne informa annualmente il Ministro per la pubblica amministrazione e l'innovazione. *4. I piani di cui al comma 3 sono adottati da ciascuna amministrazione sulla base di appositi e dettagliati studi di fattibilità tecnica; su tali studi è obbligatoriamente acquisito il parere di DigitPA.*

Tabella 5. CAD – Codice dell'amministrazione digitale

DECRETO LEGISLATIVO 18 maggio 2018, n. 65. **Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.**
Art. 12. **Obblighi in materia di sicurezza e notifica degli incidenti** *…* *2. Gli operatori di servizi essenziali adottano misure adeguate per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura dei servizi essenziali, al fine di assicurare la continuità di tali servizi.* *Art. 14.* **Obblighi in materia di sicurezza e notifica degli incidenti** **…** *3. I fornitori di servizi digitali adottano misure per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi del fornitore di servizi digitali sui servizi di cui all'allegato III offerti all'interno dell'Unione europea, al fine di assicurare la continuità di tali servizi.*

Tabella 6. Direttiva (UE) 2016/1148 - NIS

DECRETO LEGISLATIVO 18 maggio 2018, n. 65. **Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.**
Art. 12. **Obblighi in materia di sicurezza e notifica degli incidenti** *…* *2. Gli operatori di servizi essenziali adottano misure adeguate per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura dei servizi essenziali, al fine di assicurare la continuità di tali servizi.* *Art. 14.* **Obblighi in materia di sicurezza e notifica degli incidenti** **…** *3. I fornitori di servizi digitali adottano misure per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi del fornitore di servizi digitali sui servizi di cui all'allegato III offerti all'interno dell'Unione europea, al fine di assicurare la continuità di tali servizi.*

Tabella 7. Decreto Legislativo 18 maggio 2018, n° 65

5. il presidio dei processi

Sebbene non sia strettamente connesso al tema della sicurezza, il GDPR introduce una serie di obblighi che costringono le aziende a migliorare la loro capacità nella gestione dei processi.

Innanzi tutto la compilazione del **Registro delle attività di trattamento**, che è di fatto un obbligo per qualunque organizzazione (le eccezioni previste dal comma 5 dell'art. 30 del GDPR sono di fatto inapplicabili in quanto tutti i titolari effettuano quantomeno trattamenti non occasionali) costringe le organizzazioni a mappare i propri processi, valutando se gli stessi comportano un trattamento di dati personali. Tale registro deve inoltre essere mantenuto costantemente aggiornato al fine di dimostrare la conformità alla norma.

Il registro non contiene solo informazioni sui dati personali, ma anche sulle misure di sicurezza; la corretta documentazione di queste ultime comporta di fatto anche la necessità di procedere ad una adeguata mappatura del proprio sistema informativo e delle misure di sicurezza in essere.

Si ottiene così un presidio sui propri processi e sul proprio livello di sicurezza, rafforzato dalla necessità di garantire il rispetto di altri due principi base del GDPR:

- la privacy by design
- l'accountaility

Il rispetto della privacy by design impone alle aziende un costante presidio su una serie di eventi che possono modificare il proprio modello privacy *(Articolo 25* ***Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita****):*

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)
Articolo 25 ***Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita***
1.Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

Tabella 8. Regolamento (UE) 2016/679 - GDPR

L'obbligo di svolgere tali attività preventivamente ed il fatto che in realtà, al di là di quanto individuato dalla normativa (variazioni in ambito

applicativo, servizi, prodotti), qualunque evento accada in azienda (nuovi prodotti/servizi offerti o acquisiti, variazioni al sistema informativo o al modello organizzativo, variazioni nel personale…) costringono l'azienda ad effettuare una valutazione degli impatti privacy fa sì che venga mantenuto un costante presidio sui processi aziendali.

Il titolare inoltre, non solo ha l'obbligo di rispettare la normativa, ma anche di essere in grado di dimostrarlo in ogni momento, documentando le azioni messe in atto per farlo.

Sebbene può sembrare paradossale, il fatto che le aziende non abbiano una piena consapevolezza né dei processi in atto, né delle informazioni di cui dispongono, è dimostrato dall'impegno necessario per l'adeguamento al GDPR.

6. La qualità dei dati

Anche il tema della qualità dei dati, sebbene solo indirettamente connesso al tema della sicurezza, viene ampiamente trattato sia dal GDPR, sia dalla Circolare 285 di Banca d'Italia.

Limitandoci al solo GDPR, in quanto valido per qualunque organizzazione, il tema della qualità dei dati trova riscontro nell'art. 5, il cui mancato rispetto comporta le sanzioni di fascia maggiore (20 milioni di euro o 4% del fatturato annuo mondiale).

Avere dati di qualità, in particolare dati esatti ed aggiornati, consente alle aziende di ridurre gli errori nell'ambito della produzione, nella gestione degli ordini, degli incassi e dei pagamenti, nella erogazione dei servizi e quindi in ultima analisi di ridurre i reclami ed i contenziosi con le varie controparti.

Il tutto si traduce quindi in un risparmio (si evitano rilavorazioni, nuove spedizioni, rimborsi, spese legali…) e in un incremento del livello di fiducia dei vari stakeholder nei confronti dell'azienda.

Nell'attuale contesto iper competitivo dove ai clienti basta un click su un sito on line per cambiare fornitore, garantire un servizio di qualità è fondamentale e questo molto spesso dipende dalla qualità dei dati che l'azienda e la sua intera filiera è in grado di garantire.

Anche quest'ultimo aspetto, per nulla scontato, è specificatamente previsto dal GDPR, che impone ad esempio al titolare che in caso di richiesta di aggiornamento dei propri dati da parte di un interessato, tale richiesta sia portata a conoscenza anche degli altri soggetti, esterni al titolare, che partecipano al trattamento.

Si pensi nella pratica ad un'azienda che fornisce un prodotti/servzio la cui manutenzione è affidata ad aziende terze sul territorio. Una variazione ad esempio del recapito telefonico del cliente/interessato da questi correttamente inoltrato all'azienda fonitrice del prodotto/servizio, ma da questa non comunicata ai suoi fornitori sul territorio può comportare la mancata assistenza anche per periodi prolungati (caso realmente accaduto), con grave disagio e disappunto dei clienti…

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)
Articolo 5 ***Principi applicabili al trattamento di dati personali*** *1. I dati personali sono:* *a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);* *b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);* *c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);* *d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);* *e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);* *f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).* *2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).*

Tabella 9. Regolamento (UE) 2016/679 - GDPR

7. L'analisi dei rischi

Sebbene solo nella Circolare 285 di Banca d'Italia vi sia uno specifico paragrafo dedicato a questo argomento, nelle altre normative quali il GDPR o il NIS tale adempimento risulta citato o implicitamente necessario come propedeutico alla implementazione di adeguate misure di sicurezza.

Titolo IV – Governo societario, controlli interni e gestione dei rischi **Capitolo 4 – Il sistema informativo** **Sezione III – L' analisi del rischio informatico**
L'analisi del rischio informatico costituisce uno strumento a garanzia dell'efficacia ed efficienza delle misure di protezione delle risorse ICT, permettendo di graduare le misure di mitigazione nei vari ambienti in funzione del profilo di rischio dell'intermediario. *Il processo di analisi è svolto con il concorso dell'utente responsabile (1), del personale della funzione ICT, delle funzioni di controllo dei rischi, di sicurezza informatica e, ove opportuno, dell'audit, secondo metodologie e responsabilità formalmente definite dall'organo con funzione di gestione. Esso si compone delle seguenti fasi:* *la valutazione del rischio potenziale cui sono esposte le risorse informatiche esaminate; tale attività interessa tutte le iniziative di sviluppo di nuovi progetti e di modifica rilevante del sistema informativo (2).* *Tale fase prende l'avvio con la classificazione delle risorse ICT (3) in termini di rischio informatico (4);* *il trattamento del rischio, volto a individuare, se necessario, misure di attenuazione – di tipo tecnico o organizzativo – idonee a contenere il rischio potenziale.* *L'analisi determina il rischio residuo da sottoporre ad accettazione formale dell'utente responsabile (5). Qualora il rischio residuo ecceda la propensione al rischio informatico, approvato dall'organo con funzione di supervisione strategica (cfr. Sezione II, par. 2), l'analisi propone l'adozione di misure alternative o ulteriori di trattamento del rischio (6), definite con il coinvolgimento della funzione di controllo dei rischi e sottoposte all'approvazione dell'organo con funzione di gestione.* *Per le procedure in esercizio, per le quali non è stata svolta un'analisi del rischio in fase di sviluppo, è comunque prevista una valutazione integrativa, al fine di individuare eventuali presidi in aggiunta a quelli già in essere, da attuare secondo uno specifico piano di implementazione. I tempi di attuazione del piano e i presidi compensativi di tipo organizzativo o procedurale nelle more dell'attuazione, sono documentati e sottoposti all'accettazione formale dell'utente responsabile.* *I risultati del processo (livelli di classificazione, rischi potenziali e residui, lista delle minacce considerate, elenco dei presidi individuati), ogni loro aggiornamento successivo, le assunzioni operate e le decisioni assunte, sono documentati e portati a conoscenza dell'organo con funzione di gestione.* *Il processo di analisi del rischio è ripetuto con periodicità adeguata alla tipologia delle risorse ICT e dei rischi e, comunque, in presenza di situazioni che possono influenzare il complessivo livello di rischio informatico.*

Tabella 10. Circolare 285 Banca d'Italia

Le varie normative tutelano ambiti diversi e quindi l'oggetto dell'analisi dei rischi varia.

Rispetto ai tradizionali asset aziendali ad esempio, l'oggetto di tutela del GDPR sono i diritti e le libertà delle persone fisiche e quindi l'analisi dei rischi deve essere effettuata rispetto a questo particolare asset

(anche se i dati personali degli interesati sono presenti negli asset aziendali e quindi le misure di tutela da implementare in conseguenza del risultato dell'analisi dei rischi avrà impatti positivi per la sicurezza dell'azienda).

Conclusioni

Sarebbe possibile continuare questo articolo con molti altri esempi, quali la riduzione dei costi di storage derivanti dall'obbligo (sanzionato) di limitare la conservazione dei dati al tempo strettamente necessario, o al rispetto della minimizzazione…

Quanto qui riportato evidenzia comunque che il rispetto "intelligente" delle normative citate permette alle aziende di essere:

- più consapevoli circa i propri processi, sistemi, informazioni, dati trattati
- più consapevoli rispetto ai rischi che incombono sui propri asset
- costantemente aggiornate e documentate in merito a quanto sopra esposto
- più consapevoli rispetto alla tutela del proprio know how e delle informazioni segrete
- più resilienti rispetto a eventi avversi quali eventi naturali, "attacchi" da parte di soggetti interni/esterni all'azienda, errori ed incidenti
- più competitive, grazie alla qualità delle informazioni gestite ed alla relativa riduzione dei costi derivanti da errori e contenziosi
- più appetibili per i vari stakeholder, in quanto l'immagine dell'azienda risulta consolidata.

Una valutazione costi/benefici che in ultima analisi pende decisamente a favore di questi ultimi e che dovrebbe portare le aziende a modificare radicalmente il loro approccio all'adeguamento normativo, cogliendone le opportunità.