



Area Metropolitana Bari



Dalla *Privacy* al GDPR

Relatore: Michele PERLA

Chi siamo



Area Metropolitana Bari



Michele Perla

digital evangelist

Socio Fondatore di ANORC

Responsabile Territoriale ANORC Bari

Responsabile ICT della Direzione Provinciale CNA Bari

Consulenza Informatica a Commercialisti e Aziende

De-materializzazione e Conservazione Digitale a Norma

Fatturazione Elettronica PA e B2B

Privacy e Sicurezza Informatica

Di che parleremo

- Qualche definizione del *Dott. Google*
- I nostri ultimi quarant'anni ...
- I Rischi
- Il G.D.P.R.
- Conclusioni

Qualche definizione del Dott. Google

Nel termine italiano ***Sicurezza*** collassano due distinti concetti che in altre lingue sono espressi da parole differenti:

- ***security*** corrisponde alla sicurezza intesa come protezione da atti intenzionali che potrebbero ledere cose o persone;
- ***safety*** riguarda la sicurezza delle persone, intesa come loro incolumità.

Qualche definizione del Dott. Google

Un ***foglio*** assume la caratteristica di ***Documento (Analogico)*** solo se

- è creato in modo che *forma* e *contenuto* non siano alterabili durante le fasi di tenuta e accesso,
- ne sia garantita la staticità nella fase di conservazione,
- sia identificato in modo univoco (firmato e datato),
- Sia tenuto in maniera sicura, la cui conservazione può anche essere delegata a terzi.

Qualche definizione del Dott. Google

Un ***file*** assume la caratteristica di ***Documento (Digitale)*** solo se

- è creato in modo che *forma* e *contenuto* non siano alterabili durante le fasi di tenuta e accesso,
- ne sia garantita la staticità nella fase di conservazione,
- sia identificato in modo univoco (firmato e datato),
- sia memorizzato in un sistema di gestione informatica dei documenti o di conservazione, la cui tenuta può anche essere delegata a terzi.

Esempi di Documenti Digitali

Un **Documento Digitale (DD)** può non essere solo un testo ma potrà essere un filmato, un audio, una radiografia, un ECG e tante altre cose ancora.

Non ce ne rendiamo conto, ma siamo già circondati da **DD**, come per esempio

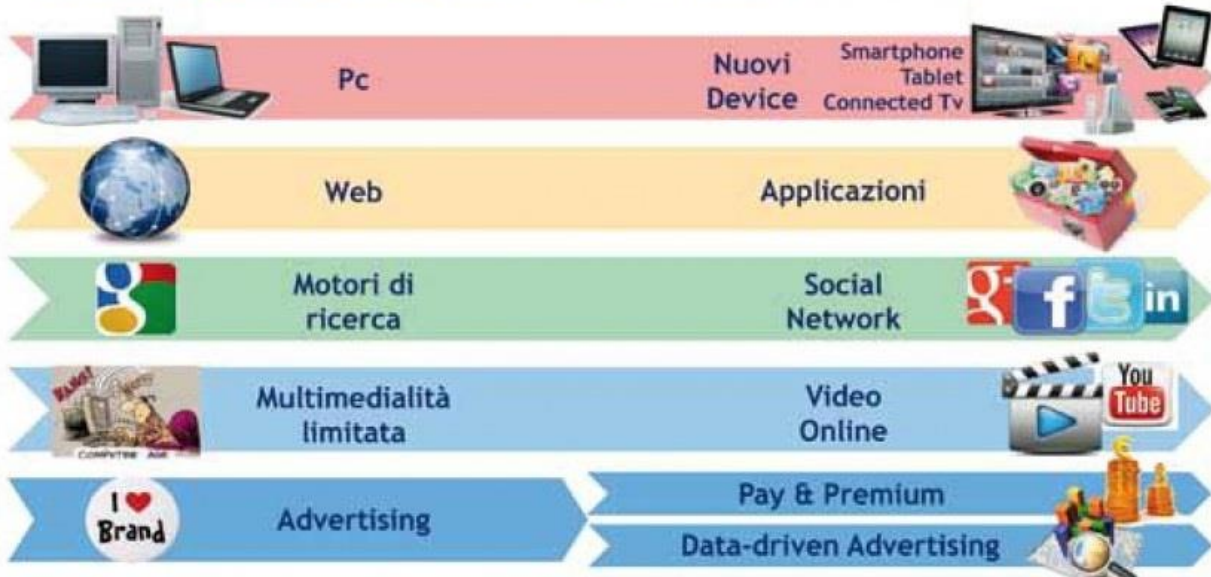
- la **PEC**, la posta elettronica certificata
- la **Fatturazione Elettronica**, ad oggi solo verso la P.A. ma dal 1° gennaio 2019 interesserà sia il ciclo attivo sia il ciclo passivo della nostra azienda



Area Metropolitana Bari



I nostri ultimi quarant'anni ...



dall'era di Internet

all'era Digitale

**Tutto questo fa parte
ormai della nostra vita,
ma quanto conosciamo
questo fenomeno?**

La Rivoluzione Digitale



Area Metropolitana Bari



... che sta succedendo?

ATTENZIONE!!!

Il prossimo 25 maggio entrerà in vigore la nuova normativa
(*GDPR Regolamento UE 2016/679*) sulla protezione dei dati
(*ex L.196/2003*)

Siete in regola?

Il G.D.P.R.

Il nuovo *Regolamento UE 2016/679* stabilisce le nuove regole per trattare i Dati Personali all'interno della Comunità Europea e per disciplinare l'esportazione dei Dati Personali al di fuori dei confini UE.

Il ***Regolamento*** o ***G.D.P.R. (General Data Protection Regulation)*** si applica non solo ai cittadini dell'Unione Europea ma anche agli Enti che risiedono al di fuori dei Paesi membri.

Nel nuovo *Regolamento* si definisce *Dato Personale*

“qualunque informazione relativa a un individuo, collegata alla sua vita sia privata, sia professionale che pubblica [...] come nomi, foto, indirizzi email, dettagli bancari, interventi su siti web di social network, informazioni mediche o indirizzi IP di computer”.

Si introducono nuovi concetti come la ***Privacy by Design*** e la ***Privacy by Default***, il ***Diritto all'Oblio*** del Dato Personale sui motori di ricerca su Internet, la ***DPIA – Data Protection Impact Assessment***, che prevede il monitoraggio sistematico del Trattamento dei Dati Personali sensibili e ad alto rischio.

"Il Titolare" (l'Art. 24 del Regolamento) *"non appena viene a conoscenza di un'avvenuta violazione dei dati personali, dovrebbe notificare la violazione all'autorità di controllo entro 72 ore dal momento in cui ne è venuto a conoscenza [...]"*

L'altra novità importante è la presenza di un esperto, il ***D.P.O.*** (***Data Protector Officer***), un esperto ("di comprovata esperienza" come recita la normativa: attenzione ai venditori di fumo!) in grado di monitorare la conformità dell'azienda alla stessa normativa. Il *DPO* comunica (tempestivamente ed in forma scritta) al *Titolare* le "non conformità". Spetta poi allo stesso *Titolare* prendere atto delle segnalazioni e provvedere all'uopo.

Ci soffermiamo su due articoli del Regolamento particolarmente importanti:

Articolo 30

Registri delle attività di trattamento

- c1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni: [...]*

Articolo 37

Designazione del responsabile della protezione dei dati

[...]

- c7. Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo.*

Ai quali si deve provvedere entro il 25/05/2018

La violazione delle norme previste dal regolamento prevede **sanzioni** severe e corpose sia dal punto di vista **amministrativo, con multe che partono da poche migliaia di euro fino a 100 milioni di euro o fino al 4% del fatturato mondiale annuo** del titolare del trattamento, non trascurando le implicazioni di natura penale.

Chi deve adeguarsi?

L'attuale normativa prevede che tutti i soggetti che fanno uso e trattamento di dati, applichino le normali procedure per mettere in sicurezza la propria struttura.

Quindi tutte le ditte, aziende e soggetti che nella loro attività hanno a che fare con lo scambio e l'archiviazione dei dati, necessitano di essere messi a norma, sia per quanto riguarda la protezione della propria rete informatica sia per la sicurezza dei propri ambienti di archiviazione.

Chi deve adeguarsi?

Le domande da porsi sono:

- *ho dei dipendenti, ho dato loro precise istruzioni sul trattamento dei dati propri e/o di terzi?*
- *esiste un disciplinare tecnico che questi devono seguire?*
- *ho predisposto misure di sicurezza minime e idonee a protezione delle banche dati?*
- *ho precise informative e consensi specifici per i miei clienti quando tratto i loro dati?*

Chi deve adeguarsi?

- *ho un impianto di videosorveglianza a norma, sia per quanto riguarda il controllo del lavoro sia per quanto riguarda i soggetti interessati da tale attività?*
- *ho fatto eseguire verifica preliminare in caso di particolari tipi di trattamenti o notifica quando necessario?*

Se ad almeno una di queste domande avete fornito risposta negativa, sappiate che siete fuori dai parametri imposti dalla legge e siete a rischio sanzioni.

Ma ci sono dei vantaggi?



La privacy: un valore aggiunto "reale" per l'azienda

Nella realtà aziendale, specie nelle PMI, è consuetudine vedere la privacy e in generale tutto quello che è legata al trattamento dati come un mero adempimento burocratico al quale i titolari del trattamento pensano solo nel momento in cui si deve andare ad intervenire per evitare sanzioni o rispondere a qualche reclamo. La realtà dei fatti dimostra invece che la privacy va ad impattare in modo significativo nei processi aziendali migliorandoli anche in maniera sostanziale.

Ma ci sono dei vantaggi?

La perdita di dati propri e degli interessati, il danneggiamento dei database, le procedure per il *disaster recovery*, i *backup*, le misure di sicurezza, ignorate fino al verificarsi di un evento non desiderato come un *data breach* di qualsiasi tipo, diventano un valore aggiunto nei processi aziendali.

La violazione dei sistemi comporta diversi problemi alle attività di un'azienda, creando un danno economico e di immagine che, oltre ai costi per la soluzione del problema, comprende la perdita di business, il tempo di inattività e altri danni.

Cosa richiede

- ☉ **Disponibilità al cambiamento**
- ☉ **Conoscenza delle regole (normativa)**
- ☉ **Strumenti adeguati**
- ☉ **Nuove figure (D.P.O.)**
- ☉ **Collaborazione tra tutti i soggetti coinvolti**

Conclusioni



Area Metropolitana Bari



- L'approccio come sempre deve essere un approccio sistematico e programmato
- Necessita di un adeguato percorso formativo
- Necessita supporto o va esteso in parte con qualche forma di outsourcing
- Necessita una particolare attenzione ai temi della privacy e della sicurezza informatica

Cosa possiamo offrirvi

- ✦ Consulenza
- ✦ Formazione
- ✦ Supporto
- ✦ Verifiche

In merito a:

- ✦ Fatturazione elettronica e conservazione sostitutiva
- ✦ Privacy
- ✦ Sicurezza Informatica



Area Metropolitana Bari



Grazie per l'attenzione

Michele Perla
digital evangelist



Area Metropolitana Bari



Area Metropolitana Bari

CNA

Area Metropolitana Bari

Via Nicola Tridente 2bis - 70125 Bari

Tel. 080.5486908

mail: info@cnabari.it