Regolamento Privacy G.D.P.R. 679/2016

Cosa cambia?

Daniele Maggiolo
senior management consultant

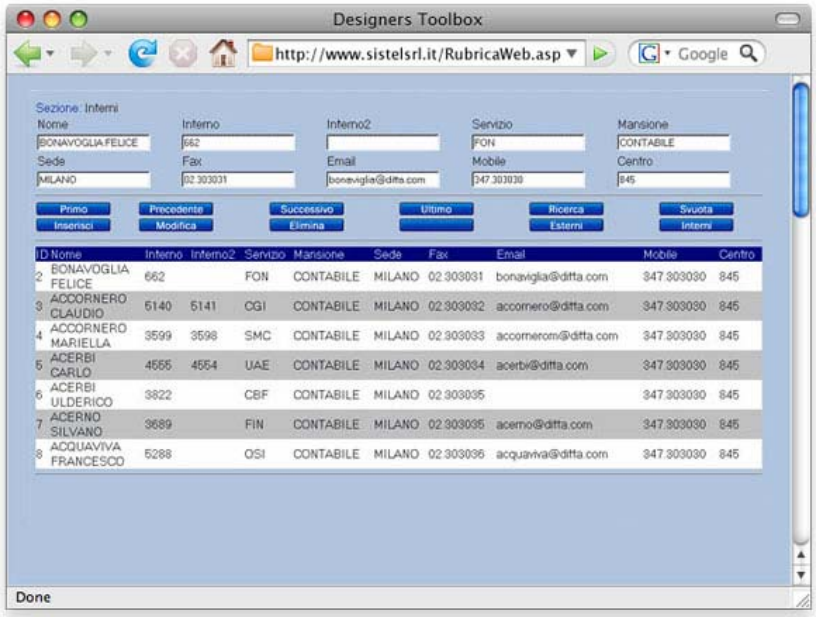
studio maggiolo pedini associati
marketing strategy | management consultancy | learning in house

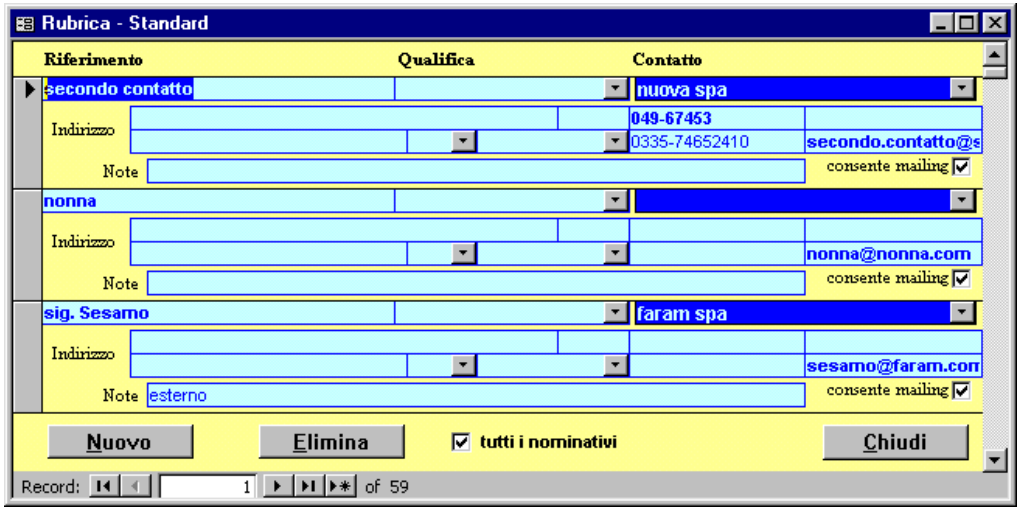
Privacy | quando, come e perché

- La protezione dei dati personali non è solo una responsabilità delle aziende
- Proteggere i dati (sensibili e non sensibili) è un dovere
- Essere protetti (aziende, persone) è un diritto
- Essere tutelati nel trattamento dei propri dati è una sicurezza
- Essere informati sui propri diritti di sicurezza nel trattamento è intelligente

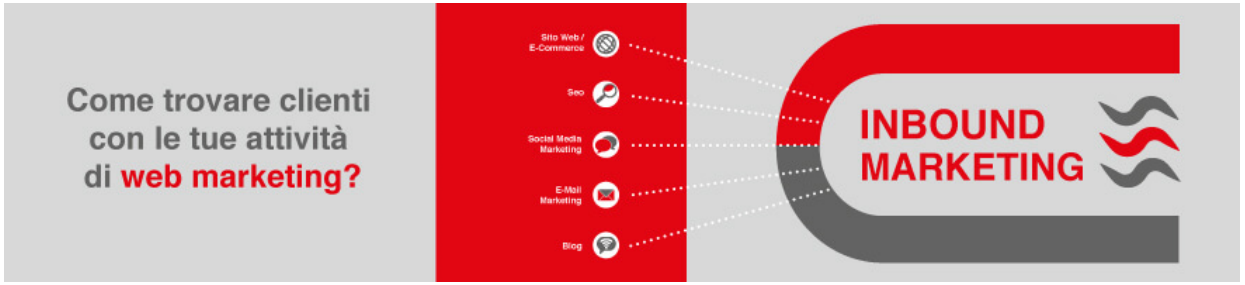
DATI E INFORMAZIONI

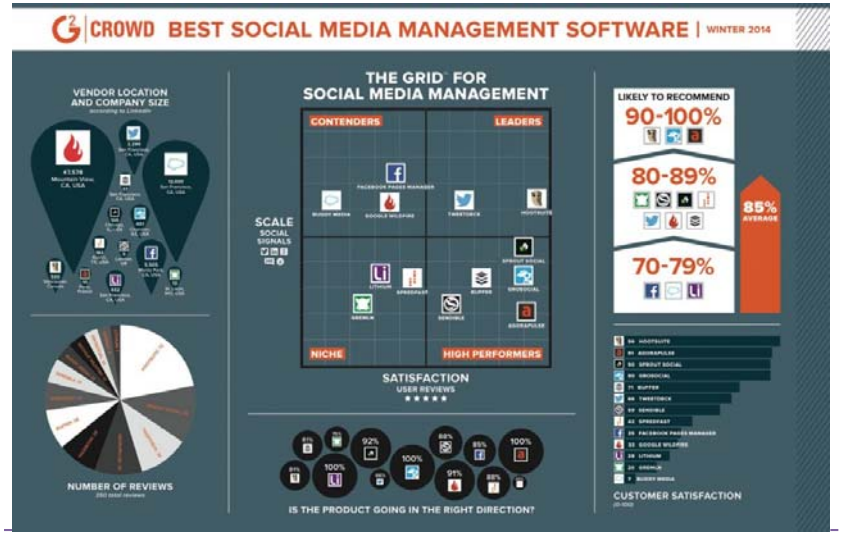
Gestione dei dati | ieri, oggi, domani



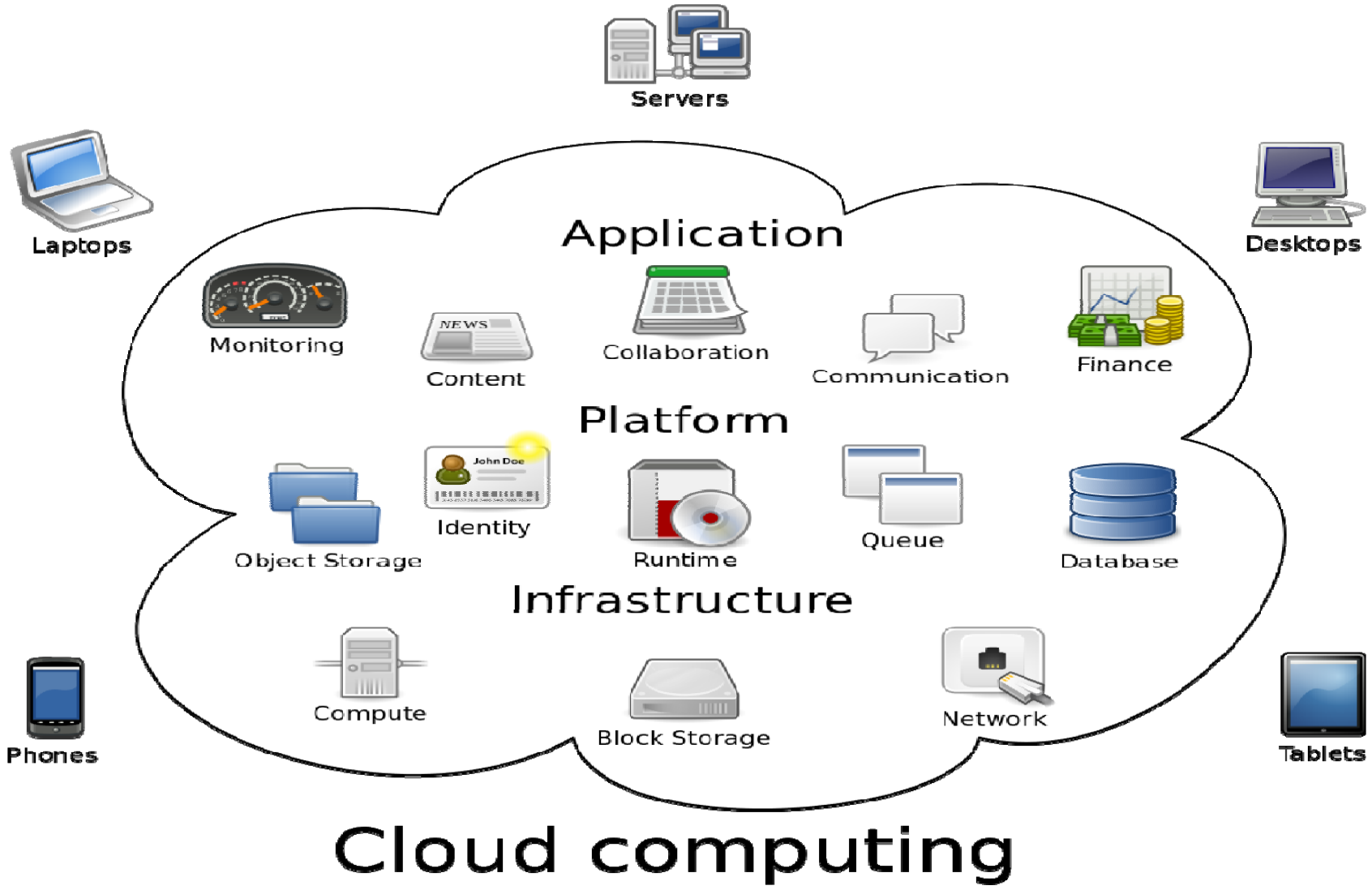


Gestione dei dati | ieri, oggi, domani





Gestione dei dati | ieri, oggi, domani



Gestione dei dati | schedatura totale …

Gestione dei dati | schedatura 360° …

Sistemi di classificazione delle informazioni sui CRM di profilatura

- Dati Demografici
  - Nome
  - Gender
  - Data di Nascita
  - *Età*
  - Nazionalità
- Canali
  - Numero di telefono
  - Indirizzo Postale
    - Città
    - Provincia
    - Codice postale
    - Nome strada e civico
  - Indirizzo Email
- ID Nazionali
  - Carta Identità
  - Codice Fiscale
  - *Passaporto*
  - Targa Automobilistica
  - *Patente*
- Organizzazione
  - Nome
  - Forma legale
- Conti finanziari
  - IBAN
  - *BIC*
- Numeri delle carte
  - Bancomat
  - American Express
  - VISA
  - MasterCard
  - Dinners Club
  - Discover
  - JCB
  - …
- Identificativi Digitali
  - IP Address (V4, V6)
  - MAC Address
  - X/Y Coordinate Geografiche
- Social Media
  - URL FaceBook
  - URL Linkedin
  - URL Pinterest
  - URL Instagram
- Dati Sensibili
  - *Salute*
  - *Politico*
  - *Religioso*
  - *Filosofico*
  - *Genetico*
  - *Biometrico*
  - *Razza*
  - *Etnia*

PRINCIPI GENERALI

Riferimenti | vecchio e nuovo

- REGOLAMENTO (UE) 2016/679 relativo alla **protezione delle persone fisiche** con riguardo al **trattamento dei dati personali**, nonché alla libera circolazione di tali dati
- È un **REGOLAMENTO** e non una legge ed è già in vigore
- Le aziende hanno tempo sino al **25 maggio 2018** per adeguarsi ALLE NUOVE DISPOSIZIONI
- Cambia l'attuale normativa 196/2003 concepita in un contesto e periodo di basso sviluppo tecnologico, con sistemi hardware e software poco adatti a garantire sicurezza

Riferimenti | definizioni

- a) "trattamento", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
- b) "dato personale", qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- c) "dati identificativi", i dati personali che permettono l'identificazione diretta dell'interessato;

Riferimenti | definizioni

- d) "dati sensibili", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
- e) "dati giudiziari", i dati personali idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato;

G.D.P.R. 679/2016

G.D.R.P. 679/2016 | Regolamento e contesto

- Il regolamento introduce una legislazione uniforme e valida in tutta europa, portando temi innovativi come il diritto all'oblio e la portabilità dei dati;
- Stabilisce criteri che responsabilizzano maggiormente le imprese e gli enti rispetto alla protezione dei dati;
- Gli stati membri possono mantenere e integrare gli attuali dispositivi di legge nazionali, adattandoli al mutevole contesto sociale, politico e tecnologico;
- Il regolamento non definisce requisiti precisi (196/2003), ma sposta la responsabilità sul titolare o responsabile del trattamento, di definire le misure maggiormente idonee a proteggere i dati dopo una analisi dei rischi.

G.D.R.P. 679/2016 | cosa resta rispetto alla 196/2003

- Viene regolamentato solo il trattamento dei dati personali di persone fisiche (non giuridiche) per scopi diversi dall'uso personale;
- Resta la distinzione tra trattamento dei dati personali comuni e trattamento dei dati sensibili;
- Resta l'obbligo di informare l'interessato sull'uso che verrà fatto dei suoi dati personali in modo chiaro e comprensibile;
- Resta l'obbligo di ottenere il consenso per i trattamenti non necessari o per il trattamento di dati sensibili, tipo quelli relativi allo stato di salute, le origini razziali, le idee religiose, le allergie, intolleranze alimentari (es. istituti scolastici).

G.D.R.P. 679/2016 | cosa cambia rispetto 196/2003

- I dati personali trattati devono essere protetti con misure organizzative e tecnologiche, adeguate a garantirne l'integrità e la riservatezza e continuamente aggiornate allo stato dell'arte;
- PRIVACY BY DEFAULT: devono essere trattati per default solo i dati necessari a perseguire le finalità del trattamento;
- PRIVACY BY DESIGN: ogni nuovo modello di trattamento dovrà essere progettato in modo da garantire la sicurezza in base ai rischi cui è sottoposto prima di essere implementato. In particolare i database, i C.R.M.
- Il responsabile del trattamento deve notificare all'autorità competente e anche all'interessato ogni violazione dei dati.
- Viene introdotta la certificazione del sistema di gestione e in alcuni casi la designazione dl D.P.O. (DATA PROTECTION OFFICER)

G.D.R.P. 679/2016 | cosa cambia rispetto 196/2003

- Il consenso al trattamento dovrà essere preventivo, inequivocabile ed esplicito, anche se espresso attraverso mezzi elettronici. I fornitori di servizi internet e i social media dovranno chiedere il consenso dei genitori per trattare i dati personali dei minori di 16 anni;
- Le decisioni che producono effetti giuridici (come la concessione di un prestito) non potranno essere basate solo su l trattamento automatizzato dei dati;
- Se il trattamento è finalizzato ad attività di marketing diretto, l'interessato ha sempre il diritto di opporsi alla profilazione;
- Viene introdotto il «diritto all'oblio», cioè a possibilità di ottenere la cancellazione dei propri dati personali qualora ricorrano alcune condizioni previste dal regolamento;
- Viene introdotto il diritto alla «portabilità»; es. cambiando provider di posta trasferisco contatti e messaggi salvati.

CONCLUSIONI

G.D.R.P. 679/2016 | conclusioni

- Il regolamento obbliga le aziende di qualsiasi dimensione ad adottare un nuovo insieme di processi politiche volte a dare alle persone un maggiore controllo sui propri dati;
- Ciò comporterà la scrittura di nuovi processi e manuali, riqualificazione del personale e l'aggiornamento di sistemi tecnologici;
- Non serve più solo la carta (informative, consensi, incarichi…) e misure minime di sicurezza (antivirus – magari free – password, etc…) per garantire il rispetto della legge, ma adattare continuamente la tecnologia allo stato dell'arte;
- Il responsabile al trattamento deve vigilare soprattutto quando il trattamento viene delegato a fornitori (consulenti del lavoro, consulenti fiscali, consulenti legali,…) che dovranno essere tenuti sotto periodico controllo;
- Ora la privacy sarà meno materia per avvocati (più specializzazione in contrattualistica) e più materia di esperti della sicurezza delle informazioni.