Il nuovo regolamento europeo sulla PRIVACY (GDPR) - Regolamento UE 679/2016

11 ottobre 2017

ALCUNE CRITICITA' ED IMPATTI PER IL BUSINESS

Avv. Diego Perini

(Esperto certificato e docente corsi DPO presso ADFOR – Esperto D.lgs 231/01)

Via Teatro Filarmonico 12, Verona

NUOVO APPROCCIO CULTURALE

Diritti e Libertà interessato

Interesse legittimo azienda

Considerando 47: "*quando esista una relazione pertinente e appropriata tra l'interessato e il titolare del trattamento, ad esempio quando l'interessato è un cliente o è alle dipendenze del titolare del trattamento*".

PRIMA: il bilanciamento tra i diritti delle parti era demandato all'Autorità per la protezione dei dati personali, sulla base dell'articolo 24, lettera g), del Codice della privacy

≠

ORA: compete alle aziende effettuare tale bilanciamento, consentendone un'applicazione generalizzata fermo restando la possibilità di verifica successiva da parte del Garante.

scelta di valorizzare l'aspetto speculare a quello dei diritti, ossia il profilo dei doveri che gravano sui titolari del trattamento (RESPONSABILIZZAZIONE)

Tutti i diritti riservati. E' vietata la riproduzione anche parziale di questo manuale senza autorizzazione di ADFOR S.p.A.

La normativa è molto precisa nel definire "cosa" bisogna garantire, ma non indica alcuna procedura sul "come" farlo.

GDPR e BEST PRACTIES

Alcuni nuovi adempimenti richiesti dal GDPR potrebbero essere risolti con un utilizzo completo o parziale di BEST PRACTICES (Framework/Standard o Norme ISO) già disponibili sul mercato oppure già **adottate in azienda** in altri ambiti.

Framework/ Standard o norme Iso

- ISO 27001
- Iso 31000- ISO 27005
- PMI - PRINCE2
- ISO 20000 (ITIL)
- ISO 29151
- Cobit5

Possibili utilizzi

- Controllli di sicurezza ICT
- Risk management
- Project management
- Gestione incidenti Change Management
- Controlli su principi Privacy
- Processi ICT con impatto su ottemperanza a GDPR

Adempimenti GDPR

- PIA/ Risk assessment, Privacy by design
- PIA/ Risk assessment
- Privacy by design
- Data Breach notification, Privacy by design
- Privacy by design

Le adozioni di norme ISO certificate è un elemento che può dare **robustezza e consistenza** alle soluzioni del sistema GDPR aziendale

Tutti i diritti riservati. E' vietata la riproduzione anche parziale di questo manuale senza autorizzazione di ADFOR S.p.A.

Principio della *Accountability*

Il Titolare deve **essere in grado di dimostrare**, che il trattamento dei dati personali effettuato sia conforme, *fin dalla prima fase della definizione delle procedure e egli strumenti*, a tutte le disposizioni del Regolamento relativamente a:

- Conservazione della documentazione sotto propria responsabilità
- Attuazione dei requisiti di sicurezza dei dati
- Esecuzione della valutazione d'impatto sulla protezione dei dati
- Rispetto dei requisiti di autorizzazione preventiva
  - o di consultazione preventiva dell'autorità di controllo
- Designazione del "Privacy Officer"
- Implementazione dei meccanismi per assicurare la verifica dell'efficacia delle misure sopracitate

RUOLO PROATTIVO e non reattivo

Privacy by Design e by Default

mette l'utente ed i suoi diritti al centro dell'analisi

PRIVACY BY DESIGN

(PROATTIVITA' PER SOLUZIONI TECNOLOGICHE)

principio di minimisation

2 PILASTRI

PROJECT MANAGEMENT

NUOVI PROGETTI

Metodologie e strumenti per intercettare i nuovi trattamenti

CHANGES

Anche per trattamenti già in esercizio il PROCESSO DI CHANGE MANAGEMENT (ossia quando le modalità vengono modificate) deve considerare gli aspetti di privacy

Tecnologie (**PET**)

per ridurre il rischio di

violazione dei principi privacy

Tutti i diritti riservati. E' vietata la riproduzione anche parziale di questo manuale senza autorizzazione di ADFOR S.p.A.

PET (Privacy Enhanced Technologies)

RICHIAMATE IMPLICITAMENTE DAL «CONSIDERANDO…» N. 78 GDPR

… i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati.

TUTELA MINORI: l'iscrizione a un servizio come quello di Facebook non è una semplice iscrizione a un social, bensì un vero e proprio contratto

Alcuni Frameworks/Standards di riferimento:

ENISA: privacy and Data Protection by Design

OASIS: Privacy Management Reference Model and Methodology (PMRM)

L´uso delle Pet può contribuire alla concezione di sistemi e servizi informatici e di comunicazione che consentono di RIDURRE AL MINIMO LA RACCOLTA E L´USO di dati personali e favoriscono il RISPETTO DELLE NORME relative alla protezione dei dati

GDPR e fornitori

Responsabilità solidale dei fornitori di sistemi: saranno disposti ad assumersi la responsabilità a costo zero?

Tutti i diritti riservati. E' vietata la riproduzione anche parziale di questo manuale senza autorizzazione di ADFOR S.p.A.

PRIVACY IMPACT ASSESSMENT

APPROCCIO RISK-BASED

OBBLIGO DI PIA QUANDO

- Venga effettuato con nuove tecnologie
- Presenta un rischio per i diritti e le libertà fondamentali dell'interessato
- Riguardi la profilazione
- Riguardi categorie particolari di dati (es biometrici)
- Riguardi la sorveglianza di zone accessibili al pubblico
- Altre ipotesi decise e pubblicate dall'Autorità

La norma ISO/IEC 29134 per il processo di PIA

Processo PIA

- DESCRIVERE I **FLUSSI DELLE INFORMAZIONI** E INDIVIDUARE **RUOLI** E FIGURE COINVOLTE
- PRIVACY RISK ASSESSMENT
- PRIVACY RISK TREATMENT
- **DOCUMENTARE** I RISULTATI DELLA PIA E INSERIRLI NELLA DOCUMENTAZIONE DI PROGETTO

PIA è un PROCESSO CICLICO, valutato prima di un nuovo trattamento, rivalutato durante il ciclo di trattamento

Data Protection Impact Assessment
DPIA Workshop
GDPR

Tutti i diritti riservati. E' vietata la riproduzione anche parziale di questo manuale senza autorizzazione di ADFOR S.p.A.

Identificare e Valutare i rischi privacy

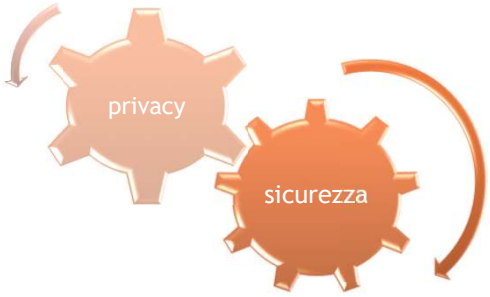
Relazione tra privacy e sicurezza dei dati

OTTEMPERANZA AI PRINCIPI PRIVACY

(art. 5, 9)

PROTEZIONE DEI DATI PERSONALI

(art. 32 oltre agli art. 4, 5, 30, 35, 40, 83)



STANDARD DI RIFERIMENTO

ISO 29100 - 29101
(Privacy Frameworks)

ISO 29151

(Code of Practice for Personally Identified Information Protection)

ISO 27001/2
(Information Security Management System)

DATA BREACH NOTIFICATION

VIOLAZIONE DATI PERSONALI: la violazione di sicurezza che comporta accidentalmente o in modo illecito (DOLO/COLPA) la **distruzione**, la **perdita**, la **modifica**, la **divulgazione** non autorizzata o l'**accesso** ai dati personali trasmessi, conservati o comunque trattati (Art. 4 – paragrafo 12)

- Adozione di prassi formali e procedure di **INCIDENT MANAGEMENT** (anomalie utenti, …)
- Utilizzo di **TOOLS** o **SOLUZIONI INFORMATICHE** (spesso già in uso nelle aziende) per segnalazione di anomalie tecniche, fino alla gestione di gravi incidenti/disastri di **BUSINESS CONTINUITY**

NOTIFICA ALL'AUTORITA' DI CONTROLLO E ALL'INTERESSATO entro **72 ORE**

ATTENZIONE

NON SOLO ATTACCHI DI HACKERS, MA TUTTE LE VIOLAZIONI

Tutti i diritti riservati. E' vietata la riproduzione anche parziale di questo manuale senza autorizzazione di ADFOR S.p.A.

DIRITTI DELL'INTERESSATO

DIRITO ALLA PORTABILITA'

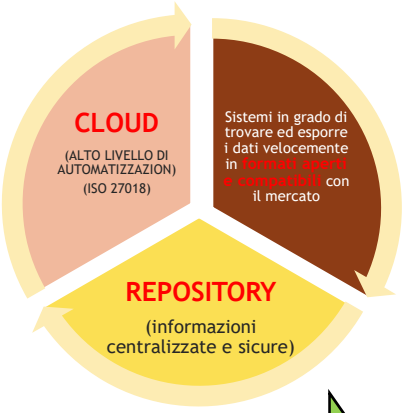
DIRITTO DI OPPOSIZIONE

DIRITTO DI RETTIFICA

DIRITTO DI LIMITAZIONE

DIRITTO ALL'OBLIO

DIRITTO ALLA PORTABILITA', MINACCIA O OPPORTUNITA?



QUALI DATI TRASFERIRE?

- DATI FORNITI DA INTERESSATO
- NO RIELABORAZIONI (DATA MANAGEMENT + SPIDER)

CON QUALI MODALITA'?

- DISCREZIONALITA' SU TECNOLOGIA
- TRASFERIMENTO SICURO

COMPLESSITA'

VANTAGGIO COMPETITIVO

Tutti i diritti riservati. E' vietata la riproduzione anche parziale di questo manuale senza autorizzazione di ADFOR S.p.A.

MODELLO GDPR

APPROCCIO STRUTTURATO

- MAPPATURA DATI AZIENDA (dove, da dove, chi, cosa ne fai)
- DATI INDISPENSABILI (trattamento più responsabile)
- MISURE SICUREZZA (contenere le violazioni)
- REVISIONE DOCUMENTAZIONE
- PROCEDURE (da opto-in a double opto-in)

Tutti i diritti riservati. E' vietata la riproduzione anche parziale di questo manuale senza autorizzazione di ADFOR S.p.A.

Come affrontare le novità del GDPR

- Valorizzare le SOLUZIONI GIÀ ADOTTATE IN AZIENDA, coerentemente con i vincoli di compliance del GDPR
- Scegliere L'APPROCCIO PIÙ EFFICACE ED EFFICIENTE in risposta alle novità metodologiche del GDPR (capo IV) considerando la tipologia di dati personali trattati, i rischi dei trattamenti e la tipologia di azienda
- Adottare APPROCCI METODOLOGICI che:
  - Garantiscano una copertura completa dei requisiti del Regolamento
  - Permettano al Titolare di dimostrare quanto effettuato per la conformità al Regolamento
  - Siano aderenti a Codici di Condotta certificati

REALIZZARE UN ACTION PLAN GDPR

Assessment del sistema Privacy attuale

- Assetto societario, mercati, prodotti, servizi, dati dimensionali dell'azienda
- Tipologia di trattamenti e Modello organizzativo Privacy
- Provvedimenti del Garante di interesse specifico dell'azienda
- Portafoglio applicazioni e Progetti nei quali è previsto il trattamento di dati personali
- Rischi e Procedure Privacy in azienda
- Accountability e Privacy Governance

Quale la rilevanza dei trattamenti di dati personali per l'azienda?

Quali processi aziendali sono potenzialmente critici per la Privacy?

Quale la risposta aziendale all'attuale normativa Privacy?

Quale l'esposizione dell'azienda ai rischi Privacy in generale?

L'Assessment è svolto tramite interviste e analisi documentali utilizzando una checklist 196/2003 (12 sezioni, 68 controlli)

Tutti i diritti riservati. E' vietata la riproduzione anche parziale di questo manuale senza autorizzazione di ADFOR S.p.A.

Gap analysis

- Nuovi aspetti normativi GDPR
- Nuovi aspetti di Privacy Governance e relazione con meccanismi aziendali di Corporate Governance già in atto (es. D.lgs 231/2001, etc)
- Nuove Policies e Procedure aziendali richieste da GDPR
- Nuove informazioni da formalizzare nei registri
- Mappatura dei Processi aziendali di trattamento di dati personali

Nuovi obblighi (oblio, portabilità, accesso ai dati, etc)

Assegnazione (eventuale) del ruolo di DPO

PIA e Risk assessment integrato (sicurezza ICT e Principi Privacy)

Quale la risposta aziendale per gli adempimenti privacy dei responsabili (esterni) dei trattamenti (contratti e controlli)

Privacy Policy, gestione e notifica incidenti, Privacy by Design (project & change manegement, soluzioni), Risk management, etc

Quale la risposta aziendale per la redazione dei registri?

Livello di formalizzazione dei Processi di trattamento

LA GAP ANALISYS È SVOLTA TRAMITE INTERVISTE E ANALISI DOCUMENTALI UTILIZZANDO UNA «CHECKLIST GDPR» (14 SEZIONI, 127 CONTROLLI)

Ridefinire i processi interni – logica multidisciplinare

Tutti i diritti riservati. E' vietata la riproduzione anche parziale di questo manuale senza autorizzazione di ADFOR S.p.A.

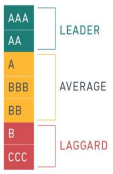
CYBER RISK

APPROCCIO TECNOLOGICO

+

APPROCCIO ORGANIZZATIVO (interazione tra strutture e componenti aziendali)

→ ADEGUAMENTO GDPR



«Su una scala da 1 a 10, in termini di rischio per i consumatori, **questo incidente è da considerare 10**, per la quantità e la riservatezza dei dati trafugati» (Gartner)

Rapporto Clusit

EQUIFAX DATA BREACH

ATTACCANTI PER TIPOLOGIA	2011	2012	2013	2014	2015	2016	Variazioni 2016 su 2015	Trend 2016
Cybercrime	170	633	609	526	684	751	9,80%	↑
Hacktivism	114	368	451	236	209	161	-22,97%	↓
Espionage / Sabotage	23	29	67	69	96	88	-8,33%	↘
Cyber warfare	14	43	25	42	23	50	117,39%	↑
TOTALE	469	1.183	1.152	873	1.012	1.050	+3,75%	↗

come per tutti gli altri rischi il **cyber risk** deve smettere di essere un rischio tecnologico e deve diventare un **rischio d'impresa e aziendale** gestito come tutti gli altri rischi

Ransomware e GDPR

L'impresa può essere considerata come colpevole, in parte, della perdita d'informazioni se non adotta **efficienti misure per prevenire** il virus del riscatto

ATTACCO RANSOMWARE

Notifica autorità → **Sanzioni gdpr**

Notifica all'interessato → **recupero dei dati dei clienti**; **danno d'immagine**

Tutti i diritti riservati. E' vietata la riproduzione anche parziale di questo manuale senza autorizzazione di ADFOR S.p.A.

Action plan

Fase 1	• Valutazione della compliance
Fase 2	• Creazione del registro dei trattamenti
Fase 3	• Stesura modifica della documentazione
Fase 4	• Individuazione ruoli e responsabilità
Fase 5	• Definizione delle politiche di sicurezza e valutazione rischi
Fase 6	• Processo di Data Breach
Fase 7	• Valutazione di impatto
Fase 8	• Implementazione processi per l'esercizio dei diritti dell'interessato
Fase 9	• Individuazione e nomina DPO

ESSERE CONFORMI AL GDPR E' OBBLIGATORIO PER TUTTE LE IMPRESE

E' NECESSARIO IL COINVOLGIMENTO DI PIU' RUOLI AZIENDALI

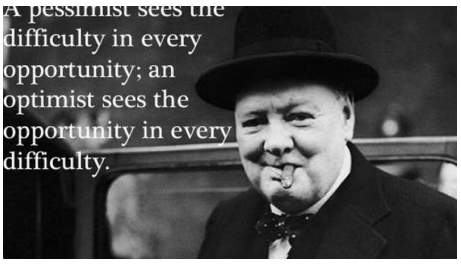
E' NECESSARIO POTER DIMOSTRARE, CON IMMEDIATEZZA, IL PROPRIO IMPEGNO E L'ATTIVITA' DI CONFORMITA' SVOLTA

E' UN PROCESSO COSTANTEMENTE ATTIVO

Tutti i diritti riservati. E' vietata la riproduzione anche parziale di questo manuale senza autorizzazione di ADFOR S.p.A.

CRITICITA' vs OPPORTUNITA'

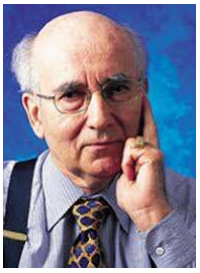
PREOCCUPAZIONI LEGITTIME	BENEFICI COLLATERALI
➢ Gravi sanzioni ➢ Costretti a investire per la conformità, anziché per necessità strategiche, commerciali o tecnologiche ➢ Grave rischio per l'immagine in caso di compromissione ➢ Impatto negativo su: vendite, marketing, relazioni clienti, trattamento dati, outsourcing, cloud ➢ Impatto negativo sulle relazioni aziendali e sul controllo dei dipendenti	✓ Maggiore sicurezza dei dati ✓ Evita perdite finanziarie ed economiche ✓ Previene problemi di reputazione, migliora l'immagine aziendale ✓ Stimola investitori e partner ✓ Contrasta il traffico illegale di dati ✓ Beneficia anche per la protezione del resto dell'informazione (Proprietà Intellettuale) ✓ Rompe i silo tra divisioni aziendali ✓ Snellisce processi e dati ✓ I consumatori pretendono più sicurezza e privacy per i propri dati personali.



Le aziende prestano troppa attenzione a quanto costa fare certe cose.

Dovrebbero preoccuparsi di più di quanto costa non farle.

(Philip Kotler)



Tutti i diritti riservati. E' vietata la riproduzione anche parziale di questo manuale senza autorizzazione di ADFOR S.p.A.