FEDERMANAGER ASDAI - LIGURIA

Il tarlo e le gambe del tavolo

PRIVACY 4.0 PER LA MIGRAZIONE EVOLUTIVA DEL MANAGEMENT DI IMPRESA 4.0

18 Ottobre 2018 – Salvo Reina

FEDERMANAGER

Data Protection & Managers

PRIVACY 4.0 PER LA MIGRAZIONE EVOLUTIVA DEL MANAGEMENT DI IMPRESA 4.0

Prima parte (*prima del 19 Sett 2018*)
- *Indagine attuariale sulla postura dei Manager 4.0*
- *Evoluzione e storiografia delle norme*
- *Maggiori novità e criticità della Riforma europea*
- *Non «**cosa**» fare, piuttosto «**come**» fare*

Seconda parte (*dopo del 19 Sett 2018*)
- *Criticità dell' ultimo Dlgs.101/2018*
- *Piano di Adeguamento e ispezioni GAT*
- *L'esperto risponde – tiro al piattello*
- *Un Manuale di Sistema PPD dal vivo!*

FEDERMANAGER Data Protection & Managers – ***PRIVACY 4.0***

La consapevolezza dei Leader nelle multinazionali

Fatti e numeri cognitivi

95% business leaders consapevoli del GDPR
85% business leaders lo ha studiato
79% è convinto che i dati siano già protetti
64% non sa che la data di nascita è dato personale
42% non considera e-mail come dato sensibile
32% non considera sensibili indirizzi di domicilio
66% non ritiene una priorità la cifra di una sanzione pecuniaria
33% ammette che l'azienda potrebbe sacrificare il 4% del fatturato
46% si dichiara «*concerned*» di danni reputazionali sui clienti
14% pensa che responsabilità di perdite dati ricada su TdT e IT Providers
51% pensa che responsabilità di perdite dati ricada solo su TdT
24% pensa che responsabilità di perdite dati ricada solo su IT Providers

Gartner EY accenture KPMG

C.Level Executives – Fonte Trend Micro Gen-Mar 2018

FEDERMANAGER Data Protection & Managers – ***PRIVACY 4.0***

La consapevolezza dei Leader nelle multinazionali

Fatti e numeri operativi

31% assegna responsabilità GDPR al CEO
27% assegna responsabilità GDPR al CISO (IT security)
21% ha effettivamente un senior CISO coinvolto nel GDPR
65% ha coinvolto solo lo staff IT (anche come RdT)
22% ha coinvolto un manager come RdT /DPO
34% ha implementato soluzione IDS/IPS (*Data Breach*)
33% ha investito in CyberSecurity
31% ha adottato crittografia

C.Level Executives – Fonte Trend Micro Gen-Mar 2018

FEDERMANAGER

Evoluzione di Privacy e Data Protection

675/96	318/99	196/03
Detenzione	Trattamento	Comunicazione

11/2008 A.D.S.
2/2012 No DPS
Dlg5/2012 Viol. Telco
Dlg69/2012 Market/ISP
Reg.UE2014/EIDAS Identità Digitale
Reg.UE/680/16 Contrasto Repress Crimini 679
170 PROVVEDIMENTI !

General Data Protection Regulation

Data subject
Data controller
Data processor
Personal data

Dir. 1148/2016 Data Breach
Dlg. 101/2018 sett) e.Privacy e dir-NIS

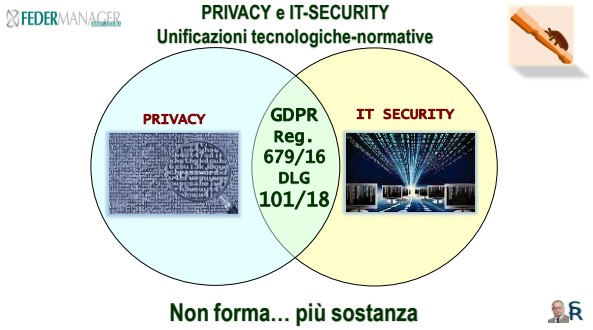
FEDERMANAGER

Dlg.vo 101/2018 Privacy 4.0

Managers 4.0 consci e preoccupati...

Esposti amministrativamente e economicamente sia professionisti e soggetti giuridici


FEDERMANAGER
Dlg.vo 101/2018
Privacy 4.0
Managers 4.0
Accountable
anche colpe
non loro!
Titolari e/o Responsabili del Trattamento
rispondono per ICT/ADS e incaricati/designati


FEDERMANAGER
PRIVACY e IT-SECURITY
Unificazioni tecnologiche-normative
PRIVACY
GDPR
Reg.
679/16
DLG
101/18
IT SECURITY
Non forma... più sostanza


FEDERMANAGER
Trilogo UE : Parlamento, Commissione e Consiglio
Modello di GDPR
Identificare
Costruire Formalizzare
Erogare
Rilevare Rispondere
Monitor
Commissione
Parlamento
Consiglio
EDPS
Comitato: gruppo ex Art. 29 WP29


FEDERMANAGER
Cambia
davvero la
musica ?


ART. 5, 12 -
C.do 58,100
NOVITA'
INFORMATIVA
Trasparenza
L'interessato deve sapere tutto
sull'uso dei propri dati... prima !


Accountability
Chi, come, cosa
e quando
rende conto
ART. 4,24,27,28,29 - C.do 74,75,76,77,79,80,81


Niente Protocollo Informatico o Amministrazione Digitale 2.0 senza DP
NOVITA'
PA e Privato
non più duellanti
AGID – opportunità con molte contraddizioni per Outsource privato / Housing service


Documento
Valutazione
dei Rischi e
degli Impatti
P.I.A.
D.V.R.
Processo
Permanente
Delle Politiche
Del trattamento
Art. 24
ART. 35, 36 C.do 89,96 – Per trattamenti a rischio elevato


NOVITA'
Diritto all'oblio
Secure Erasure
De-Indexing
Portability
ART. 17, C.do 65,66 | Art 13,20 C.do 68,73


Profilazione
on-line
Automatizzata
NOVITA'
ART. 21,22,23 – C.do 70,73 – Prevenzione frodi/antiriciclaggio – Progr. Fidelizzazione – DPR430/01 «concorso premi»


Legitimate
Interest
Data subject does not necessarely
override Controllers
NOVITA'
Introduzione del principio di BILANCIAMENTO
A seconda dei dati, rischi connessi il TdT contiene i costi
e proporziona impiego di risorse (IT, DPO)
ARTT. 4 – 11 Co 47


Autorità
controllo
capofila
NOVITA'
unico interlocutore del
titolare del trattamento in
merito al trattamento
transfrontaliero
ART. 60, 67 : Capofila Holding controlla blacklist!
One-Stop-shop Sportello
Unico sedi/filiali UE

Codici di sigilli e marchi

ART. 40,41,42 43
C.do 77,81,100

Considerando 100

"Al fine di migliorare la trasparenza e il rispetto del presente regolamento dovrebbe essere incoraggiata l'istituzione di meccanismi di certificazione e sigilli nonché marchi di protezione dei dati che consentano agli interessati di valutare rapidamente il livello di protezione dei dati dei relativi prodotti e servizi"

Se adottati TQM e Certificazioni possono semplificare

Basi giuridiche di frontiera

Whistleblowing

NOVITA'

Consenso, Contratto, legittimo interesse, Conservazione limitata nel tempo, discriminazione, Informativa dipendenti e collaboratori, procedura dati sensibili, garanzia misure di trattamento

Art. 2 L.179 Nov 2017 – Denuncia illeciti lavoro Privato e Pubblico -

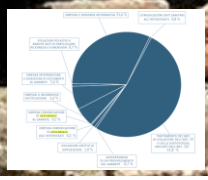
Data.Breach Art. 34 e 24

Si intende In due Direzioni LEAKS

Dir2009/136/EU 28 - Dlg. 69/2012 - Art. 4, comma 3, lett. g-bis Dlg.196/03 - Art. 34 Reg.679/16

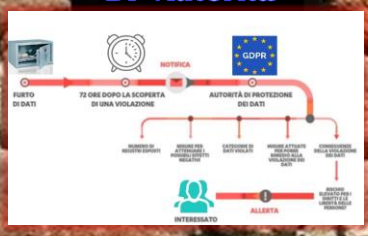
Data.Breach Art. 33

Torniamo al DP sul campo



Data.Breach

Procedura DP Autorità

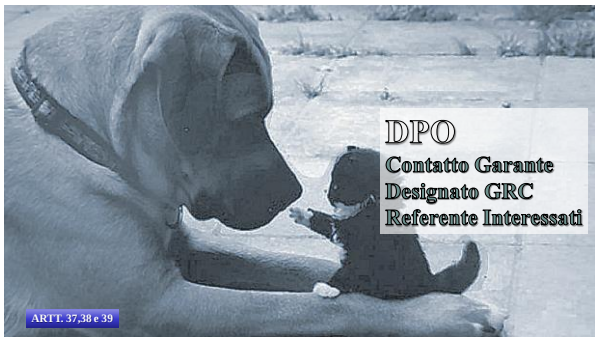


ART. 8, C.do 38, 58

NOVITA'

Social & Minori
Dir. under thirteenth


Chiese e associazioni religiose
NOVITA'
Corte di giustizia dell'Unione europea
COMUNICATO STAMPA n. 103/18
Lussemburgo, 10 luglio 2018
Una comunità religiosa, come quella dei testimoni di Geova, è responsabile, congiuntamente ai suoi membri predicatori, del trattamento dei dati personali raccolti nell'ambito di un'attività di predicazione porta a porta
ART. 91, C.do 165 – Applicazione conforme diritto costituzionale nazionale e rispetto Art. 17 TFUE


DPO
Contatto Garante
Designato GRC
Referente Interessati
ARTT. 37,38 e 39


Un ingaggio scorretto
Può costare
al business
più delle
sanzioni
ART 83
G.A.T.


1) Lo spartito non è uno…
2) sicuramente la musica è dal vivo !


FEDERMANAGER
Data Protection & Managers
PRIVACY 4.0 PER LA MIGRAZIONE EVOLUTIVA
DEL MANGEMENT DI IMPRESA 4.0
Prima parte (prima del 19 Sett 2018)
Indagine attuariale sulla postura dei Manager 4.0
Evoluzione e storiografia delle norme
Maggiori novità e criticità della Riforma europea
Non «cosa» fare, piuttosto «come» fare
Seconda parte (dopo del 19 Sett 2018)
Criticità dell' ultimo Dlgs.101/2018
Piano di Adeguamento e ispezioni GAT
L'esperto risponde – tiro al piattello
Un Manuale «digitale» di Sistema PPD Intralan

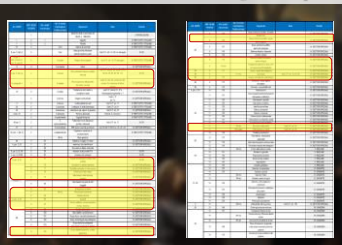

FEDERMANAGER
Dlg.vo 101/2018 - 19 Settembre 2018
Buona Novella o cataclisma legale?
Privacy 4.0 – tutti sanno cosa fare…
Nessuno spiega come?

Dlg.vo 101/2018: cosa contiene la Novella?

- Abrogazione parziale Dlg.196/03 (*GDPR displ.primaria*)
- Integrazioni Dlg.196/03 – Reg.679/16 (*crasi legale*)
- Modifiche e/o rettifiche (*Es. sistema sanzioni*)
- Coordinamento normativo (*Es. Statuto lavoratori*)
- Norme transitorie Dlg.101/18 (*Es. Regole di condotta*)
- Ruolo Autorità di controllo (*Provv. e prescrizioni*)

Privacy 4.0 – Adeguamento, coordinamento, integrazione

Dlg.vo 101/2018: la Novella per i manager di Impresa 4.0



45% su 27 Articoli

Declina adempimenti, obblighi organizzativi, scelte tecnologiche, prassi di Sicurezza e implementazione di Sistemi di Qualità sotto la responsabilità dei Titolari e dei loro Managers

Privacy 4.0 – Codice Privacy + Regolamento UE + 101/18

Dlg.vo 101/2018 e la Privacy 4.0

Cosa ci si aspettava…

- Proroghe dei termini
- Depenalizzazioni
- Semplificazioni
- Condoni e moratorie

Dlg.vo 101/2018 e la Privacy 4.0

E' accaduto altro !

Dlg.vo 101/2018 e la Privacy 4.0

Nessuna estensione dei termini di decorrenza

Cogenza adempimenti non procrastinata!

Dlg.vo 101/2018 e la Privacy 4.0

Nessuna sospensione per obblighi e adempimenti

Varato piano ispettivo a fronte «Richiesta di grazie» parlamento…

Crescono reclami, segnalazioni, ispezioni, notificazioni per Data Breach e registro DPO

Dlg.vo 101/2018 e la Privacy 4.0

Nessuno sconto o depenalizzazione…

Introduce «Reati Privacy»
Estrema severità del Legislatore italiano (9 reati, di cui 4 nuovi)

Dlg.vo 101/2018 e la Privacy 4.0

Disciplina non semplificata semmai estesa!

Codice privacy (parziale) +
Regolamento + Provvedimenti +
Norme transitorie +
Regole deontologiche (quando?)

Dlg.vo 101/2018 e la Privacy 4.0

Ma… allora?

- Nessuna sospensione ispezioni/sanzioni
- Semplificazioni solo *µ-m e* PMI… FORSE!
- Inasprimento sanzioni Amministrative
- Ulteriore stringenza sugli adempimenti
- Dir. Civ. e penale: detenzione 3-6 anni

Dlg.vo 101/2018 e la Privacy 4.0

PROBLEMA: Non più forma ma sostanza!

- ***Progettare By Design & By Default***
- ***Accountability: rendere conto proattivo***
- ***Ingaggio Ispezioni: sanzioni gravi ed effettive***
- ***Non solo carta: adempimenti dimostrabili***
- ***Costo o investimento tecnologico ICT***

Dlg.vo 101/2018 e la Privacy 4.0

SDP senza «se» e senza «ma»
e senza Errori

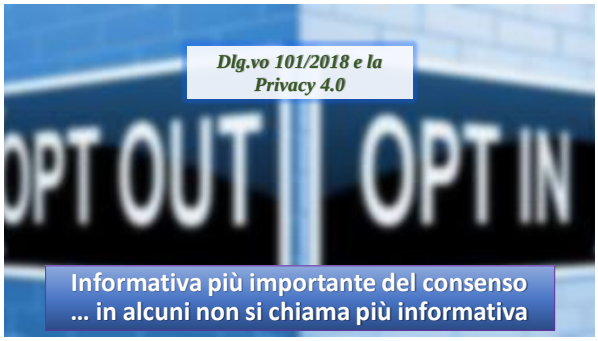
- **No *Cut & Paste* dei Documenti Sistemi DP**
- **Tutelare il dato è tutelare la *persona (paziente)***
- **Non confondere *conformità* e *compliance***
- **Non pensare di scaricare oneri a *legali o DPO interni***
- **Formazione e consulenza: *NON FAI DA TE***

Dlg.vo 101/2018

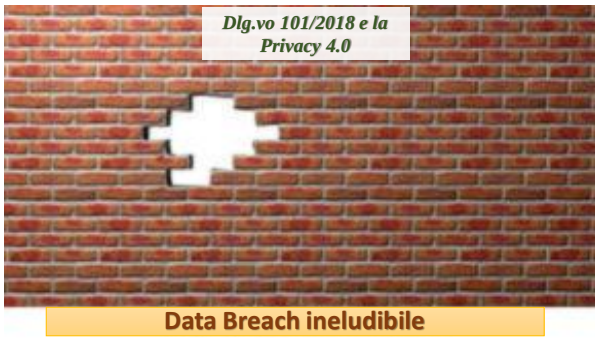
Conoscere le maggiori criticità
PRIVACY 4.0 per non inciampare


Dlg.vo 101/2018 e la Privacy 4.0
PLA/SLA ISP
Vetrina con sigillo/marchio
Informativa completa!
Doc/Referti On-Line
Cert.OWASP Back-access
GAT e-Discovery ispezioni
Attenzione al web !


Dlg.vo 101/2018 e la Privacy 4.0
Revisione globale contrattualistica affiancando tecnologo ai legali e dir. ICT
SLA, PLA, BCR, NVI - Smart Contract DAO

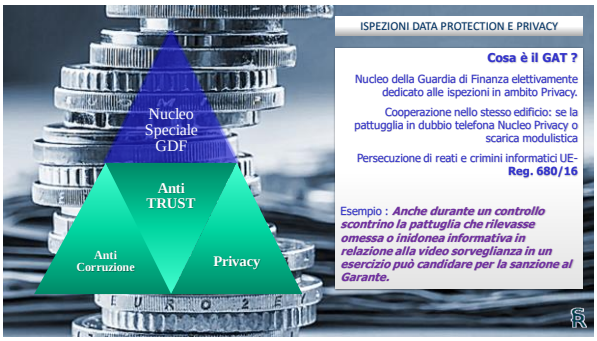

Dlg.vo 101/2018 e la Privacy 4.0
OPT OUT
OPT IN
Informativa più importante del consenso
… in alcuni non si chiama più informativa


Anche la Sanità, l'assistenza Socio Sanitaria, Il terzo Settore, Lab. Analisi e ICRS, medici famiglia e dati san. lavoratori


Dlg.vo 101/2018 e la Privacy 4.0
Data Breach ineludibile


Dlg.vo 101/2018 e la Privacy 4.0
Caducanza norma: Blocco dei dati!
Reato: Trattamento illecito reclusione fino a 18 mesi


ISPEZIONI DATA PROTECTION E PRIVACY
Cosa è il GAT ?
Nucleo della Guardia di Finanza elettivamente dedicato alle ispezioni in ambito Privacy.
Dal Gen Rapetto >> Cmd.
Col. Menegazzo >> Col. Reccia


Nucleo Speciale GDF
Anti TRUST
Anti Corruzione
Privacy
ISPEZIONI DATA PROTECTION E PRIVACY
Cosa è il GAT ?
Nucleo della Guardia di Finanza elettivamente dedicato alle ispezioni in ambito Privacy.
Cooperazione nello stesso edificio: se la pattuglia in dubbio telefona Nucleo Privacy o scarica modulistica
Persecuzione di reati e crimini informatici UE- Reg. 680/16
Esempio : Anche durante un controllo scontrino la pattuglia che rilevasse omessa o inidonea informativa in relazione alla video sorveglianza in un esercizio può candidare per la sanzione al Garante.


Dlg.vo 101/2018 e la Privacy 4.0
Formazione continua, pianificata,specifica e verbalizzata


Dlg.vo 101/2018 e la Privacy 4.0
Privacy: Indagine conoscitiva internazionale sul rispetto delle norme. L'Autorità italiana si concentrerà su Regioni, Province autonome e società controllate
Sudditanza degli Enti Locali e di coloro che con la PA lavorano!!!


Dlg.vo 101/2018 e la Privacy 4.0
PERICOLO DI INCIAMPO
Codici di Settore, di condotta, deontologici future Regole di Condotta della AC Garante


Dlg.vo 101/2018 e la Privacy 4.0
DPO vero e credibile!

Dlg.vo 101/2018 e la Privacy 4.0

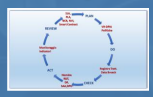
Sostenibilità Impresa 4.0 passa dalla Privacy 4.0

misure fisiche, logiche e organizzative

possibile sfruttare un approccio TQM

Dlg.vo 101/2018

Impresa 4.0 vs Privacy 4.0?



GRC - READINESS

Governo
Rischio
Controllo

Dlg.vo 101/2018 TQM per i Dati

Rischio

Ricognizione globale
Censimenti dispositivi
Risk assesment
Impact assessment
SLA/PLA fornitori

Dlg.vo 101/2018 TQM per i Dati

Governo

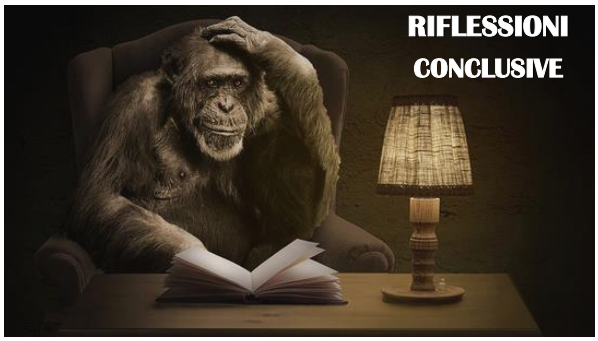
Politiche
Incarichi/deleghe
Piano Formazione
Qualifica fornitori
PLA/SLA Servizi

Dlg.vo 101/2018 TQM per i Dati

Controllo

Continual Logs Sys
Audit interni /esterni
IT IDS/IPS -ISO-CSF
Hypervisors CLOUD
Storage Integrity

Dlg.vo 101/2018 TQM per i Dati


RIFLESSIONI
CONCLUSIVE


4 SUGGERIMENTI 4
Non necessariamente dobbiamo essere geni che conoscono la relatività !
Il salto quantico occorre
• Commitment proprietà
• una delega forte
• un DPO
E atterrate in sicurezza...


Non puoi migliorare
quello che non vedi


Non confondere
Sforzi con risultati !


L'approccio
fai da te poco
plausibile ...


Ambire nuove possibilità, non minimo possibile


Digital Forensics
Privacy Officer
IL CODICE PRIVACY IN ITALIA
Come cambia dopo il D.Lgs. n. 101/2018
CODICE PRIVACY LAVORO
CODICE DELLA PRIVACY
Privacy Primi Passi
PRIVACY E REGOLAMENTO EUROPEO
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
NATIONAL PRIVACY COMMISSION


FEDERPRIVACY
ATTESTATO DI QUALITA'
Salvo Reina
Data Protection Officer
ISACA
CERTIFICATO
ISSA


Profilo professionale
Excursus accademico e competenze
➢ Ricercatore e docente universitario
➢ Biotecnologia e QA biomedicale
➢ Total Quality Manamentt - Auditor
➢ Data protection officer
➢ Privacy & Safety Blogger
➢ Company ICT Security advisory
Salvo Reina
tiro al piattello !
Certificazioni
Accreditamenti e affiliazioni
➢ EMAS – EMAS2
➢ ISO 14001:2005
➢ ISO 20000:2010
➢ ISO 27001:2009
➢ AM ISACA
➢ TÜV DPO (ISO 17024:2005)
➢ Ref. FEDERPRIVACY
Expertise & skills
➢ Scientific Ghost-writer
➢ Lead Auditor – ICT Governance
➢ Lead Analyst – IT Security, Risk Mngmt, OHSAS
➢ Integrator & Advisor on 231, Dlg191/07, Dlg81/08
➢ Data protection officer, CDA
➢ Privacy & Safety Advisor & Blogger
issa
AKADEMIE
ISACA
PrivacyOfficer
British Standards Institution
aipsi
FEDERPRIVACY