


**La riforma Privacy 4.0 del GDPR: come fare nella PMA?**

Mauro Costa e Salvo Reina



Milano  
27 Settembre 2019  
Hotel Michelangelo

**Co-chair, advise-Board & Group Leader**

**NOTIFY LIBRARY**  
The global vigilance and surveillance database for medical products of human origin (MPMO): Transplantation, Transfusion, Assisted Reproduction

Product Type	Category	Product	Status	Manufacturer	Responsible Party
Assisted Reproduction	Embryos	Embryos	Active	IVF Clinics	IVF Clinics
		Embryos	Active	IVF Clinics	IVF Clinics

**NOTIFY LIBRARY**

The Global Vigilance and Surveillance Database for Medical Products of Human Origin  
Transplantation, Transfusion and Assisted Reproduction

**VISTART**  
VIGILANCE AND INSPECTION FOR THE SAFETY OF TRANSFUSION ASSISTED REPRODUCTION AND TRANSPLANTATION



**Adverse incidents in fertility clinics: lessons to learn**

Figure 2: Number of incidents by category January-December 2014

Category	Number of Incidents
Reorganisation	2
Communication	2
Security	3
Clinical equipment	16
General	16
Consent	16
Laboratory equipment	24
Laboratory practice	21
Laboratory control	108
Administration	12

Category	Example
Reorganisation	Theatre list cancelled or rearranged, impacting on patients.
Communication	Incorrect information given to patient regarding medication, resulting in an abandoned cycle.
Security	Break ins and/or theft of equipment from clinics.
Clinical equipment	Clinical equipment malfunctioning.
General	Adverse weather conditions causing flooding in a laboratory or clinical area.
Consent	Embryos removed from storage without the patient's consent.
Laboratory equipment	Most commonly equipment faults and failures eg. dewar failure.
Laboratory practice	Disturbances containing eggs or embryos knocked or dropped and failure to inspect or inseminate eggs.
Laboratory control	Embryos not fully thawed.
Administration	Breach of patient confidentiality.








**Dalla Legge 675 al Codice Privacy dal 1996 al 2016 fino Reg679/16UE ad oggi Corso DP per Resp. di Centro**

**Manuali di Sicurezza e Qualità !**

## Gestione del Rischio sui Dati – Audit, Bio-RedTech, ICT, TQM/GRC, Legal DF e Readiness







**Esposizione applicativa non accademica - Materiale originale dell'autore**

# PARTE 1

# PARTE 2

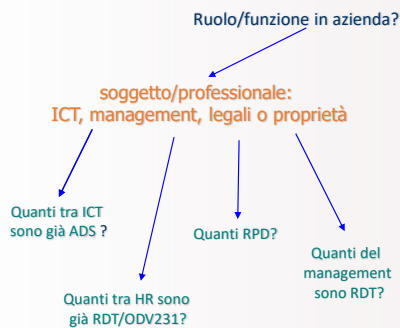
## Question Time



**Privacy 4.0  
nella PMA**

## Privacy 4.0: PRIMA DI INIZIARE CONOSCIAMOCI MEGLIO!

*indagine esplorativa, informale in ambito privato e P.P.A.A.*



audience : quanti sono «soggetti autorizzati» Sistema Privacy aziendale



# PARTE 1

Filogenesi delle normative: Migrazione  
dal Codice Privacy del Dlg.196/03  
al Regolamento 679/16 e Dlg.101/18

*Privacy 4.0  
nella PMA*



Privacy 4.0 – Protezione dei dati orientata al rischio

Capire da dove si viene per decidere dove andare

## Reg.679/16 sulla Data Protection

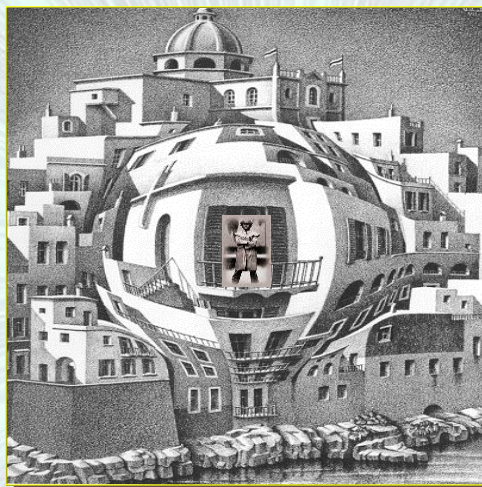
Antesignana la **Corte costituzionale** tedesca che, nel **1984**, dichiarò l'esistenza di "**diritto alla autodeterminazione informativa**", meglio definito come "diritto del singolo a decidere autonomamente quando e con quali limiti possono essere diffuse informazioni riguardanti la propria persona" o altrimenti come "diritto a decidere circa la rinuncia o il trattamento dei propri dati personali".

**Concetti di qualità e sicurezza legati alla economia della etica**



**Costi della non Privacy ! ISO 18000**

## GDPR-EU e Reg.679/2016



**Fuoco sulla persona... in che senso**

GDPR-EU e Reg.679/2016



NON fuoco alla persona !



SalvoReina

Persona elettronica permutatoria  
della nostra identità digitale

QUALE ???

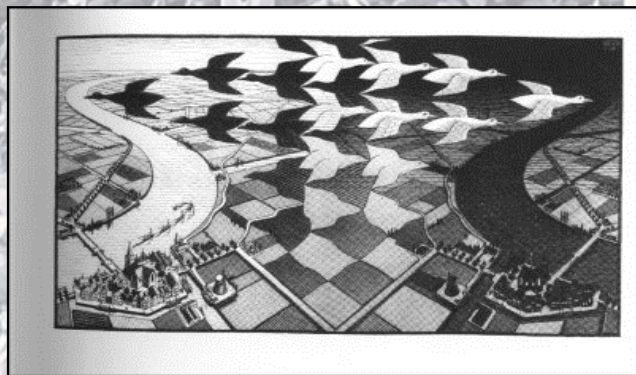


Privacy

GDPR-EU e Reg.679/2016

# ì MIEI DATI SONO MIEI (?)

GDPR-EU e Reg.679/2016



Due opposte libertà: libera circolazione dei dati tutela privacy

Una migrazione culturale evolutiva

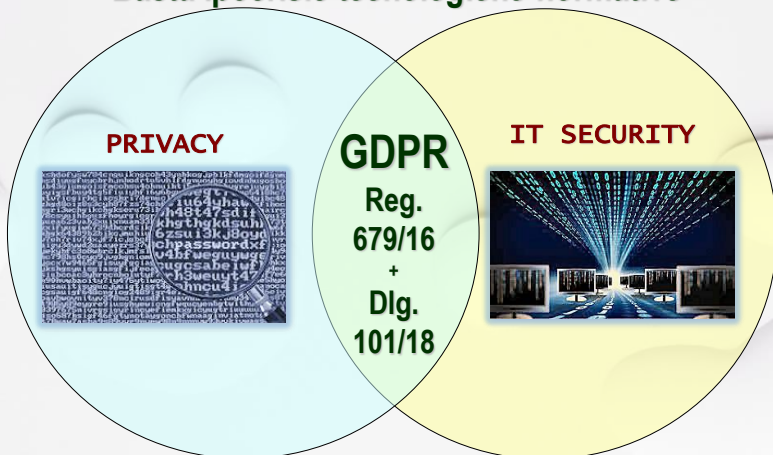
SalvoReina

R



**Data Protection: futuro UNIFICATO di PRIVACY e IT-SECURITY**

**Basta ipocrisie tecnologiche-normative**

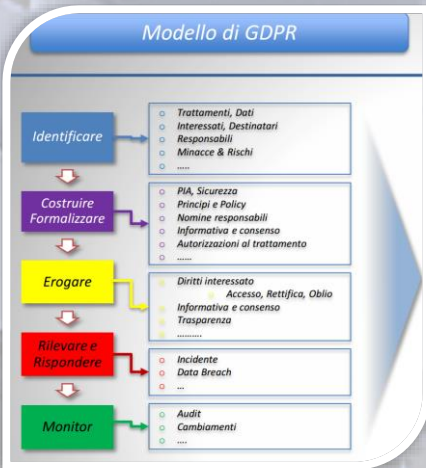


**Era della Privacy 4.0 – Non più forma... ma sostanza**





## Trilogia UE : Parlamento, Commissione e Consiglio



Commissione



Parlamento



Consiglio

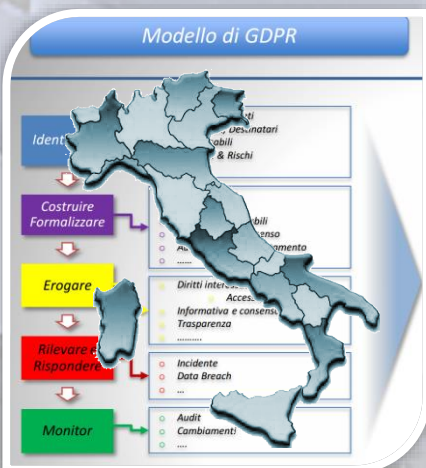


EDPB



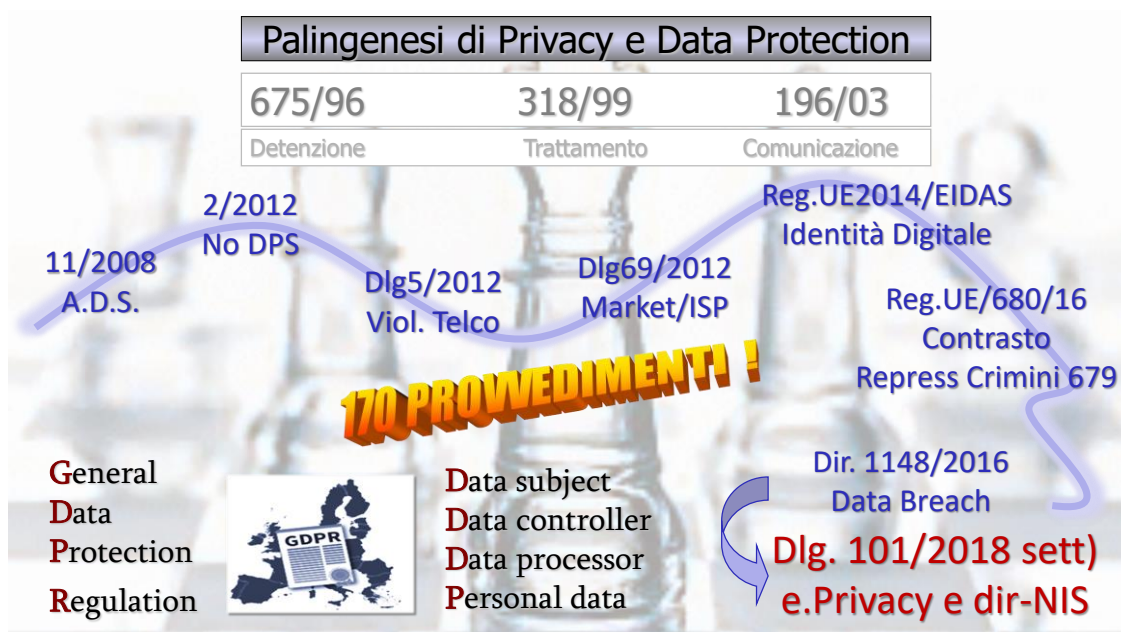
Comitato: gruppo ex Art. 29 WP29 – Board ex Garante Garanti

## In Italia : Garante Privacy poi Autorità di Controllo



Garante Europeo





## *Dlg.vo 101/2018: la Novella in PMA*

Privacy 4.0 – Adeguamento, coordinamento, integrazione

- **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 (Prov. e prescrizioni)**

# Dlg.vo 101/2018 - 19 Settembre 2018

## Buona Novella o cataclisma legale per la PMA?



**PMA esplicitamente  
riferita nel corpo  
della legge  
(Dlg.196/03 novellato)**

4-9-2018 GAZZETTA UFFICIALE DELLA REPUBBLICA ITALIANA Serie generale - n. 205

— Gli articoli 37 e 160 del citato decreto legislativo 30 giugno 2003, n. 196, così recitano:

«Art. 37 (Notificazione del trattamento) — 1. Il titolare notifica al Garante il trattamento di dati personali cui intende procedere, solo se il trattamento riguarda:

a) dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica;

b) dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini diversi da quelli relativi a banche di dati alla fornitura di beni, indagini epidemiologiche, trapianto di organi e tessuti e monitoraggio della spesa sanitaria;

c) dati idonei a rivelare l'attività sessuale o dati genetici correlati».

5. Nell'effettuare gli accertamenti di cui al presente articolo nei riguardi di uffici giudiziari, il Garante adotta idonee modalità nel rispetto delle reciproche attribuzioni e della particolare collocazione istituzionale dell'organo procedente. Gli accertamenti riferiti ad atti di indagine coperti dal segreto sono differiti, se vi è richiesta dell'organo procedente, al momento in cui cessa il segreto.

6. La validità, l'efficacia e l'utilizzabilità di atti, documenti e provvedimenti nel procedimento giudiziario basati sul trattamento di dati personali non conforme a disposizioni di legge o di regolamento restano disciplinate dalle pertinenti disposizioni processuali nella materia civile e penale».

— 1.art. 1 della legge 11 gennaio 2018, n. 5 (Nuove disposizioni in materia di iscrizione e funzionamento del registro delle opposizioni e istituzione di prefissi nazionali per le chiamate telefoniche a scopo statistico, professionale e di ricerche di mercato), pubblicata nella Gazzetta Ufficiale 3 febbraio 2018, n. 28, come modificata dal presente decreto, così recita:

### Dlg.vo 101/2018: quanto la Novella impatta la PMA

Art. 101/18	Art. 101/18	Art. 101/18	Art. 101/18	Art. 101/18	Art. 101/18
1	1	1	1	1	1
2	2	2	2	2	2
3	3	3	3	3	3
4	4	4	4	4	4
5	5	5	5	5	5
6	6	6	6	6	6
7	7	7	7	7	7
8	8	8	8	8	8
9	9	9	9	9	9
10	10	10	10	10	10
11	11	11	11	11	11
12	12	12	12	12	12
13	13	13	13	13	13
14	14	14	14	14	14
15	15	15	15	15	15
16	16	16	16	16	16
17	17	17	17	17	17
18	18	18	18	18	18
19	19	19	19	19	19
20	20	20	20	20	20
21	21	21	21	21	21
22	22	22	22	22	22
23	23	23	23	23	23
24	24	24	24	24	24
25	25	25	25	25	25
26	26	26	26	26	26
27	27	27	27	27	27

Art. 101/18	Art. 101/18	Art. 101/18	Art. 101/18	Art. 101/18	Art. 101/18
1	1	1	1	1	1
2	2	2	2	2	2
3	3	3	3	3	3
4	4	4	4	4	4
5	5	5	5	5	5
6	6	6	6	6	6
7	7	7	7	7	7
8	8	8	8	8	8
9	9	9	9	9	9
10	10	10	10	10	10
11	11	11	11	11	11
12	12	12	12	12	12
13	13	13	13	13	13
14	14	14	14	14	14
15	15	15	15	15	15
16	16	16	16	16	16
17	17	17	17	17	17
18	18	18	18	18	18
19	19	19	19	19	19
20	20	20	20	20	20
21	21	21	21	21	21
22	22	22	22	22	22
23	23	23	23	23	23
24	24	24	24	24	24
25	25	25	25	25	25
26	26	26	26	26	26
27	27	27	27	27	27

**9.9% su 27 Articoli**  
*Sanità, Ass Socio Sanitaria,  
 Nosocomi, strutt Ospitaliere, Medici  
 di Famiglia, Diagnostica omica, IRCS  
 Ricerca stat e epidemiol, Genetica,  
 PMA, Pediatria, Cartelle cliniche,  
 Dossier e fascicolo San. Ele., anagr  
 Centri nascita e reg. decessi,  
 precizioni mediche, comun. ISTAT,  
 dati ultra-sensibili, particolari e  
 specifici .*

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

## *Dlg.vo 101/2018: su cosa la Novella impatta la PMA*

### *Riferimenti Basi giuridiche PMA sui trattamenti dati*

- Prot. 1025.CNT.2018 l'import-export gameti/embrioni Centri PMA-banche esteri Eterologa
- Prot. 3693/CNT/2017-1 modalità comuncaz import export (Allegato 1)
- Legge 190/2014/ comma298 registro donatori
- DM 15 novembre 2016 recepimento importazione Mat.Biol. DE 2015/566/UE
- GMP allegato su laboratorio PMA e ISO 14644 sulle «clean rooms»
- Dlg. 16/2010 e L. 256 /99
- Dir. 2012/39/EU – Amendig 2006/17/EC – testing Hum.tissues & cells
- Dlgs 85 2012 modifica e agg. dlgs 16/2010
- Linee guida legge 40 III edizione 2015 e GL Sala criologica
- Coding - parere favorevole regioni Art. 2 c3 Dlg.281/97. Cod.4.10/2016/79
- Dlgs. 191/2007 e accordo Conf. Perman. Stato Regioni del 2012
- Accordo 25 marzo 2015 stato regioni su ispezioni e DM 31 luglio 2015 registro valutatori



**Art. 5  
Principi**

## *Dlg.vo 101/2018 - 19 Settembre 2018*

### *Buona Novella o cataclisma legale per la PMA?*

**Privacy 4.0 – tutti sanno cosa fare...  
Chi spiega come?**



**Dlg.vo 101/2018  
Privacy 4.0**

**Centri PMA  
Accountable  
anche colpe  
non loro!**

**Senza se  
Senza ma!**

**Titolari e/o Responsabili del Trattamento rispondono  
per ICT/ADS, receptionist e infermieri OTA (incaricati/designati)**



**Dlg.vo 101/2018  
Privacy 4.0**

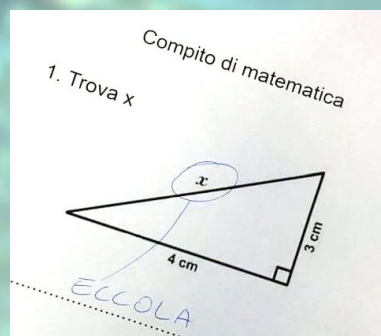
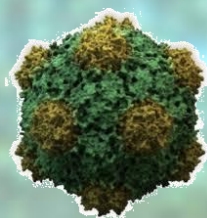
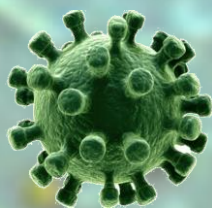
**Responsabili  
Centri PMA  
consci e  
preoccupati...**

**Esposti amministrativamente e  
economicamente sia  
professionisti e soggetti  
giuridici (pubblico e privato)**

**Garante per la protezione  
dei dati personali**  
PROVVEDIMENTO 5 giugno 2019.  
Prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'articolo 21, comma 1 del decreto legislativo 10 agosto 2018, n. 101, (Provvedimento n. 146), (19A04879) ... Pag. 20



## Dlg.vo 101/2018 - Privacy 4.0



Approccio alla PRIVACY 4.0 sostenibile  
Quello che non viene detto!

## Dlg.vo 101/2018 e la Privacy 4.0

Cosa ci si aspettava  
dal 2018...

- **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 grazia» 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 5 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 in PMA*

Ma... le italiane abitudini?

- Nessuna sospensione ispezioni/sanzioni
- Semplificazioni solo  $\mu$ -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 in PMA*

**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 in PMA

Sistema Privacy e Protezione Dati  
senza «**se**», senza «**ma**» e senza **ERRORI**

- No **Cut & Paste** dei Documenti Sistemi DP
- Tutelare il dato è tutelare la **persona (coppia, don.eterol)**
- Non confondere **conformità e compliance**
- Non pensare di scaricare oneri a **legali o peggio DPO**
- Formazione e consulenza: **non ricorrere al «fai da te»**

## Dlg.vo 101/2018



Nuove **maggiori criticità** obblighi **disattesi o inidonei**



**PERICOLO DI INCIAMPO**

*Dlg.vo 101/2018 e la Privacy 4.0*

**PLA/SLA ISP – SSL/TLS**  
**Vetrina con sigillo/marchio**  
**Informativa completa!**  
**Doc/Referti On-Line /2FA**  
**Cert.OWASP / proprio CLOUD**  
**GAT e-Discovery ispezioni**

**Attenzione al web !**



**PERICOLO DI INCIAMPO**

*Dlg.vo 101/2018 e la Privacy 4.0 in PMA*

**Revisione globale contrattualistica affiancando tecnologo ai legali e dir. ICT / Es.: Ag. Pulizie**  
**REGISTRO TRATTAMENTI E DPIA**

**SLA, PLA, BCR, NVI - Smart Contract DAO**



**Dlg.vo 101/2018 e la Privacy 4.0 in PMA**



**Informativa più importante del consenso  
in Sanità... non sempre si chiama informativa!**




**Ricerca statistica, clinica, epidemiologica o  
studi censori di popolazione/territorio  
Profilazione *de facto* e collaborazioni tra  
Centri Co-titolari (Art.23) e DPO congiunto (Art.37-39)**



Stoccaggio Sanitario Art.30  
 Dati transfrontalieri – Eterologa Art.45  
 Sito Freddo DLP/IDP/IDS - CC  
 Cripto-imaging Biometrica Art.22,9  
 Archive anon-Pseudonimizzazione  
 Provv. VDT Ctrl Remoto  
 CV – Art.111-bis

Diritto all'oblio Art. 12-17  
 Secure Erasure Certif.  
 De-Indexing anagrafico  
 e Portability alter Centro  
 Whistleblowing A.2 L.179  
 Anamnesi e Counselling Psi  
 Art.2-terdecies - decessi

PERICOLO DI INCIAMPO



Dlg.vo 101/2018 e Reg.679/16 – Art.32-33-34

Tutti lo sanno  
 R-PMA!

**Data Breach: quello che dovevate già sapere prima!**

PERICOLO DI INCIAMPO

## Reg.679/16 sulla Data Protection

**Non è solo un problema di sanzioni...**

Una normativa di seconda generazione

***Inibitoria e Caducante***

**Art. 2 Quaterdecies Dlg.101/18**



**20** anni di privacy con una miriade di provvedimenti emanati – Ultimo Rapporto Garante

Se la ispezione è motivata da una segnalazione, in presenza di una in'adempienza

**fermo delle attività del Centro PMA**

## *Dlg.vo 101/2018 e la Privacy 4.0 in PMA*



Reato: «Trattamento illecito» reclusione fino a 18 mesi (Art. 167)

**Caducanza norma: Blocco dei dati!**



**Dlg.vo 101/2018 e la Privacy 4.0**

Formazione continua, pianificata, specifica e verbalizzata  
**Nuovi:** Archivio, Rappresentante, Terzi, Destinatari, Capofila ecc



**Dlg.vo 101/2018 e la Privacy 4.0**

**GARANTE PER LA PROTEZIONE DEI DATI PERSONALI**

**Privacy: indagine conoscitiva internazionale sul rispetto delle norme. L'Autorità italiana si concentrerà su Regioni, Province autonome e società controllate**

Privacy: indagine conoscitiva internazionale sul rispetto delle norme  
 L'Autorità italiana si concentrerà su Regioni, Province autonome e società controllate

Da oggi parte il "Privacy Sweep 2018", un'indagine a carattere internazionale dedicata quest'anno al principio di responsabilizzazione (accountability), introdotto anche in Europa dal Regolamento Ue.

L'iniziativa è coordinata dalla [Global Privacy Enforcement Network \(GPEEN\)](#) - la rete internazionale nata per rafforzare la cooperazione tra le Autorità della privacy di diversi Paesi - e prenderà in esame le misure che titolari o responsabili del trattamento hanno adottato per garantire e dimostrare il rispetto delle norme e degli standard in materia di protezione dei dati.

Il Garante italiano concentrerà la sua azione sulle Regioni e sulle Province autonome e sulle rispettive società controllate che effettuano rilevanti trattamenti di dati personali per lo svolgimento di compiti di interesse pubblico.

**Sudditanza degli Enti Locali**  
 Es. «Fiduciario sanitario» tra Regione e Comune



## Dlg.vo 101/2018 e la Privacy 4.0

Codici di Settore,  
di condotta,  
deontologici  
future Regole di  
Condotta della  
AC Garante

**GARANTE PER LA PROTEZIONE DEI DATI PERSONALI**

**Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018 [9069637]**

VEDI ANCHE: [comunicato stampa del 24 dicembre 2018](#)  
[doc. web n. 9069637]

Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018  
[/Pubblicate sulla Gazzetta Ufficiale n. 11 del 14 gennaio 2019](#)

Registro dei provvedimenti n. 205 del 19 dicembre 2018

**IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI**

NELLA riunione odierna, in presenza dei dott. **Alessandro Soro**, presidente, **Augusta Iannini**, vicepresidente, della dott.ssa **Giovanna Bianchi Clerici** e della perita **Liliana Calvano**, componenti il dott. **Giuseppe Busia**, segretario generale;

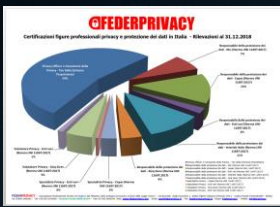
VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento "GDPR" o "Regolamento dei dati") (di seguito "GDPR" e "RGPD");

VISTO il d.lgs. 10 agosto 2018, n. 101, recante "Disposizioni di adeguamento della normativa nazionale alle disposizioni del 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";

VISTO il Codice in materia di protezione dei dati personali, d.lgs. 30 giugno 2003, n. 196, (di seguito "Codice"), così come modificato dal predetto d.lgs. n. 101 del 2018;

VISTO il Codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e scientifici allegato A.4 al Codice;

**Gennaio - Marzo 2019**



**Dlg.vo 101/2018 e la Privacy 4.0 e PMA**  
**DPO credibile non aberrante!**



Come è  
cambiata la  
musica ?

PRIVACY 4.0 : nuovo paradigma futuro per ogni settore e ambito

**RITOCCHI** tsunamici su molti ambiti ...

- a) Avvocatura – provv. Disciplinari
- b) Stampa, giornalismo ed editoria
- c) Registro Pubblico delle Opposizioni (abbonati)
- d) Accordi deontologici – Ordini profess.
- e) Dati ultra sensibili – dati sanit. in indagini giurisprudenz.
- f) Studi statistici – epidemiologia e censimenti
- g) Sweet Thirteenth: bambini più tutelati
- h) Investigazioni base giurid. Pari Rango non esimente ICT
- i) Trasmissione dati all'estero (INTRA-EXTRA UE)
- j) Gestione privacy negli istituti Religiosi

**NOVITA'**



**Casi studio:** Studi legali, Larga distribuzione, Assicurazioni, Banche, Sanità, Sociale





# Dato personale

ART. 44 Comma 1  
- C.do 26

«Dato o Informazione» della persona fisica...

**Def. Invariata dal Codice Privacy**  
**La differenza è piuttosto nelle**  
**Tipologie di dato!**

**Dati Particolari (art.9):** ex-dati sensibili, dati genetici, dati biometrici

**Dati Penali,** relativi a condanne penali, reati, legati a misure di sicurezza

**Dati con rischi elevati** per la dignità e la libertà della persona (es. profilazione, geolocalizzazione, videosorveglianza...)

**Dati comuni** (es. dati anagrafici, codici identificativi, etc...)

**Dati anonimi** : non associabili a una persona identificata o identificabile. **A tali dati non si applica il Regolamento**

**NOVITA'**

... e Pubblico non è Pubblicato!

Per Comunic. Elettroniche/Marketing si applica Dir. 2002/58/UE – persone fisiche e persone giuridiche (Abbonati)

Concetti e approcci rivoluzionari

Art. 25 - un nuovo paradigma  
non un vecchio paradosso ...

... per disegno progettuale

... per scelta predefinita

**Privacy by design**  
**Privacy by default**



Impatto di coordinamento sul mondo del Lavoro!

Art. 4 - 8 Statuto Lavoratori - Legge n. 300/1970  
Prov. Garante 2 Apr 2008 – Controllo Remoto  
D.lgs. n. 151/2015, L. delega n. 183/2014 - Jobs Act



Comunicazioni On-line, Cookies (Dig 69/2012 Art.122), violazione dato personale Provv. "Data Breach" (Art. 3, 32, 132, 162-ter Codice privacy), pregiudizio violazione a terzi (150K€ non più del 5% fatturato). Conservazione dati di traffico (Dig 109/2008 modalità) e Codice Privacy per misure conservazione



**Registro Proattivo dei Trattamenti**

**9 PRINCIPI di TRATTAMENTO** **Art. 5.1/5.2**

- Liceità
- Correttezza
- Trasparenza
- Limitazione della finalità
- Minimizzazione dei dati
- Esattezza
- Limitazione della conservazione
- Integrità
- Riservatezza

**NOVITA'**

**Reg.I.T.**

**ART. 30,35, 36 - C.do 89,96**

**Introduzione del principio di BILANCIAMENTO**

A seconda dei dati, rischi connessi il TdT contiene i costi e proporziona impiego di risorse (IT, DPO)

**Legitimate Interest**  
Data subject does not necessarily override Controllers

**NOVITA'**

**ARTT. 4 – 11 Co 47**



**LICEITA'**

**INTERESSE LEGITTIMO**

**NOVITA'**

il **CONSENSO**  
 l'adempimento ad **OBBLIGHI CONTRATTUALI**  
 gli **INTERESSI VITALI** della persona interessata o di terzi  
 gli **OBBLIGHI DI LEGGE** cui è soggetto il Titolare  
 l'**INTERESSE PUBBLICO** o l'**ESERCIZIO DI PUBBLICI POTERI**  
 l'**INTERESSE LEGITTIMO** prevalente del Titolare o di terzi  
 cui i dati vengono comunicati.

ART. 6 par. 1, 7 - C.do 89,96

**LICEITA'**

**AMBITI DI APPLICAZIONE INTERESSE LEGITTIMO**

**NOVITA'**

1. Libertà di stampa e di espressione
2. Marketing diretto
3. Comunicazione politica
4. Campagne di raccolta fondi delle organizzazioni non lucrative
5. Recupero crediti anche stragiudiziale
6. Prevenzione frodi, antiriciclaggio
7. Controllo indiretto dei lavoratori
8. Segnalazioni di illeciti (whistle-blowing)
9. sicurezza fisica
10. Sicurezza informatica e delle reti
11. Ricerca storica, scientifica e statistica
12. Ricerche di mercato (comprese ricerche di marketing)

ART. 6 par. 1, 7 - C.do 89,96 – dimenticheremo Ex Art. 24 comma 1 Lettera g come Interpello Ex Art.17

ART. 15, C.do 146  
 coord. Capo VIII –  
 Danno e risarcimento

PECULIARE CASO  
 IN **PMA** SONO  
 FINO A **4** !!!

Interessato  
 «**Chiunque**» al CapoVIII

Crescente numero di cause di paternità, affidamento, rivendicazioni legali sulla prole

Data Protection coordinamento giuridico con DirUE: Es. **TUCE**

### Comunicazione e **diffusione** del dato!

il Titolo X del Codice italiano, concernente le **Comunicazioni Elettroniche**, racchiude una trama normativa di particolare efficacia e completezza, che consente di dare piena attuazione alla direttiva 2002/58/EU.

i dati relativi al traffico; informazioni raccolte nei riguardi dell'abbonato o dell'utente; la identificazione della linea; i dati relativi alla ubicazione; le chiamate di emergenza; gli elenchi degli abbonati; le comunicazioni indesiderate; la conservazione dei dati di traffico per altre finalità



interazione fra due codici, l'uno delle comunicazioni e l'altro della protezione dei dati personali  
 Per valutare idoneità, liceità e adeguatezza delle misure di protezione dei dati personali

# Dalla Protezione alla vera Resilienza

PEN Test  
IDS/IPS  
V.A.  
UTMs  
NAS  
Firewall

Per non stare in corsia di emergenza tutti i giorni ...

ART. 5, 12 -  
C.do 58,100

**NOVITA'  
INFORMATIVA**

# Trasparenza

L'interessato deve sapere tutto sull'uso dei propri dati... prima !



**Accountability**

**NOVITA'**

Chi, come, di cosa  
e quando si rende  
conto...

ART. 4,24,27,28,29 - C.do 74,75,76,77,79,80,81



**Accountability**

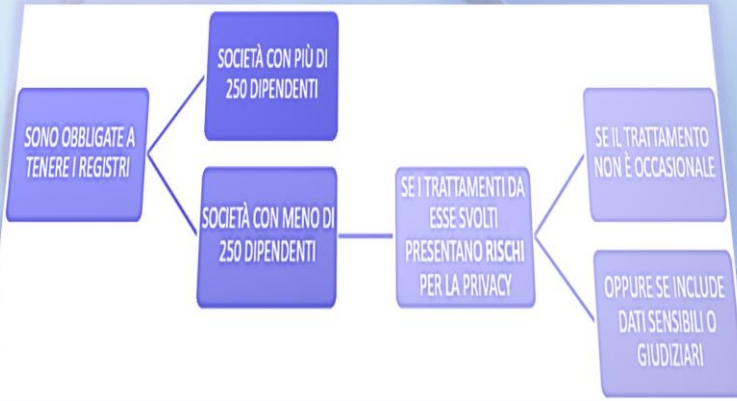
**NOVITA'**

«DIMOSTRARE»  
«COMPROVARE»  
«RENDICONTARE»

ART. 4,24,27,28,29 - C.do 74,75,76,77,79,80,81

## REGISTRO DEI TRATTAMENTI – Reg679/16 - Art. 30

Keyword: **COMPROVARE**



ANNO 20		MESE												PAGINA				
														NUMERO				
														1				
Piano di ruolo:																		
ESERCIZIO	TOTALE	CREDITI (VALORI MASSIMI DELLA RIFORMA FISCALE)												CREDITI CONSERVATI PERIODICI	PRELIEVI (CANCELLAZIONE)	RISERVE ESISTENTI	RISERVE NON ESISTENTI	
		1	2	3	4	5	6	7	8	9	10	11	12					
2011																		
2012																		
2013																		
2014																		
2015																		
2016																		
2017																		
2018																		
2019																		
2020																		

**NOVITA'**

NON CONFONDERE CON IL REMINISCENTE DPS!

## Misure di Sicurezza basate su Rischio – Art 33-32

RILEVANZA PENALE A CARICO DEL TITOLARE DEL TRATTAMENTO

MISURE TECNICHE/  
ORGANIZZATIVE  
ADEGUATE PER  
GARANTIRE UN LIVELLO  
DI SICUREZZA ADEGUATO  
AL RISCHIO, TENENDO  
CONTO:

**NOVITA'**

DEI COSTI  
DI ATTUAZIONE

DEL CONTESTO  
DEL TRATTAMENTO

DELLA NATURA  
DEL TRATTAMENTO

DELLE FINALITÀ  
DEL TRATTAMENTO

DELL'OGGETTO  
DEL TRATTAMENTO

DEL RISCHIO PER  
I DIRITTI E LE LIBERTÀ  
DELLE PERSONE FISICHE



**OPT/IN/OUT**  
 Libero, incondizionato, informato  
**Consenso**  
**INEQUIVOCABILE** (deducibile da  
 azioni attive o comportamenti  
 concludenti dopo Informativa)

**ESPLICITO** per Dati Salute,  
 Biometrici ecc.

Sempre **PROVATO**

Soluzione tecnica  
 Pratica perché  
**Non Obbligo Scritto**

**BY DESIGN**  
**BY DEFAULT**

ART. 7, 17, C.do 65,66

Niente Protocollo Informativo o Amministrazione Digitale 2.0 senza DP  
 AGID – opportunità con molte contraddizioni per Outsourcing privato / Housing service



**NOVITA'**

**PA e Privato**  
 non più duellanti





**NOVITA'**

**Diritto all'oblio  
Secure Erasure  
De-Indexing  
Portability**

ART. 17, C.do 65,66 | Art 13,20 C.do 68,73



ART. 8, C.do 38, 58

**NOVITA'**

**Social & Minori  
Dir. under thirteenth**

## Piano di Formazione

### NESSUN TRATTAMENTO CON SOGGETTI NON ISTRUITI

- *Obbligo nel settore sanitario (Art. 29 tutti soggetti autorizzati)*
- *Differenziale per attività e trattamento – Percorsi aula/eLearning*
- *Art. 32- Accesso ai dati solo dopo istruzione (frontali, scritte)*
- *Verbalizzazione Piano di Formazione (MSDP – crono/calendario)*
- *Supervisione DPO (Art. 39) AUDIT e prove finali (registrazioni)*
- *Obbligo da Sanzione amministrativa (Art. 83 GAT > 30% 2016)*
- *Comprovare accantonamento in Bilancio approvato*
- *Rubricata formazione nella BCR (Art. 47 – Gruppi di impresa)*

**NOVITA'**

*Nelle PPA.A. – CAD, FOIA, ANAC, whistleblowing, trasparenza, pazienti interessati*

Artt. 29, 32, 39, 47 C.do 74

**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

**NOVITA'**

Profilazione  
on-line  
Automatizzata

ART. 21,22,23 – C.do 70,73 – Prevenzione frodi/antiriciclaggio – Progr. Fidelizzazione – DPR430/01 «concorso premi»

**NOVITA'**

Basi giuridiche di  
frontiera  
Whistleblowing

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

10 MAG 2018  
11322.18  
REPUBBLICA ITALIANA  
IN NOME DEL POPOLO ITALIANO  
LA CORTE SUPREMA DI CASSAZIONE  
SEZIONE UNICA

COMPRESA NELLA LEGGE 20/01/2017 N. 12

SENTENZA  
N. 11322/18  
OGGETTO: RICORSO PER CASSAZIONE  
PROVVEDIMENTO: CASSAZIONE  
RAGIONE: UNICA  
PUNTO: UNICO  
RISULTATO: CASSAZIONE  
RAGIONE: UNICA  
PUNTO: UNICO

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

**GARANTE PER LA PROTEZIONE DEI DATI PERSONALI**

## NOTIFICAZIONE NO !!

### Notificazione e Registro dei trattamenti

(artt. 37 e 38 d. lg. 30 giugno 2003, n.194)

- Cosa è la notificazione
- Istruzioni
- Domande più frequenti (FAQ)
- Intermediari
- Link utili
- Esoneri, chiarimenti e precisazioni
- Compilazione della notificazione
  - Prima notificazione - Modifica - Cessazioni
  - Notificazione sospesa
- Consultazione del registro

**Facsimile del modello**

**ATTENZIONE:** Si prega di leggere con attenzione le istruzioni e le note al Garante per la protezione dei dati personali indicate nella sezione "Domande più frequenti (FAQ)".

**AVVENENZA**

Il Garante per la protezione dei dati personali (D.Lgs. n. 196 del 30 giugno 2003) informa che, ai sensi dell'art. 37 del D.Lgs. n. 196 del 30 giugno 2003, la notificazione telematica dei trattamenti di dati deve essere fornita alle autorità competenti (in Italia, il Garante per la protezione dei dati personali) e, se omessa, non impedisce di completare la notificazione, con conseguente responsabilità per omessa notificazione (art. 163 del Codice).

L'indicazione dei dati personali nei campi non contrassegnati da un asterisco può risultare utile per agevolare i rapporti con il Garante e con gli interessati, ma è comunque facoltativa e, se omessa, non impedisce di completare la notificazione.

I dati personali indicati nella notificazione possono essere conosciuti (alcuni, anche dall'Istituto bancario responsabile del trattamento tramite il quale sono versati i diritti di segreteria) da soggetti convenzionati con il Garante ai quali il notificante può rivolgersi per la trasmissione telematica della notificazione con apposizione di firma digitale. Si tratta di

**Non Novità!**

**R**

**Data.Breach**  
**Art. 34 e 24**

**Non Novità!**

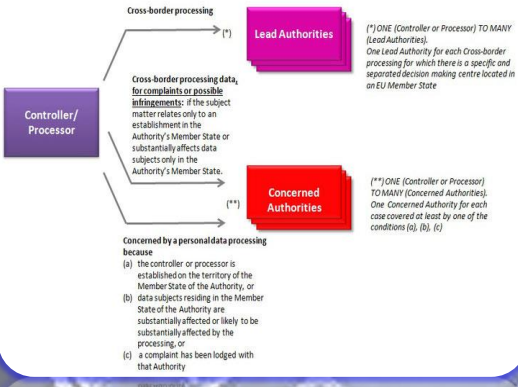
**Si intende**  
**In due**  
**Direzioni**  
**LEAKS**

Dit:2009/136/EU 28 - Dlg. 69/2012 - Art. 4, comma 3, lett. g-bis Dlg.196/03 – Art. 34 Reg.679/16

**R**

# SLA PLA BCR TDT CCS

## Companies with multi-establishments in the EU



**Dati Trans-Frontalieri (Extra UE)**  
Art. 44-50

**Legati all'Ambito Territoriale!**

**NOVITA' SUB-trasferimenti Stati terzi White List**

The screenshot shows the California Legislative Information website. The main heading is "AB-375 Privacy: personal information: businesses. (2017-2018)". It includes a search bar, navigation links, and a list of tabs: Text, Votes, History, Bill Analysis, Today's Law As Amended, Compare Versions, Status, Comments To Author. The main content area displays the text of the bill, starting with "TITLE 1.81.5 California Consumer Privacy Act of 2018" and "ASSEMBLY BILL NO. 375 CHAPTER 55 THE PEOPLE OF THE STATE OF CALIFORNIA DO ENACT AS FOLLOWS: An act to add Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, relating to privacy." It also mentions "Approved by Governor June 28, 2018. Filed with Secretary of State June 28, 2018." and a link to "LEGISLATIVE COUNSELS DIGEST".

**Dati Trans-Frontalieri (Extra UE) Art. 44-50**

**Consumer Privacy Act 2018-2020**

**Privacy Shield 2015**

**Safe Harbour 1998-2000**

The screenshot shows the FEDERPRIVACY website, which provides information on data protection laws. It features a navigation bar with "HOME", "PROCESS", "PELLETTI", and "SPECIALI". The main content area includes sections for "Dati Trans-Frontalieri (Extra UE) Art. 44-50", "Consumer Privacy Act 2018-2020", "Privacy Shield 2015", and "Safe Harbour 1998-2000". The website also includes a search bar, a sidebar with "HOME", "PROCESS", "PELLETTI", and "SPECIALI", and a footer with "FEDERPRIVACY" and "SPECIALI".

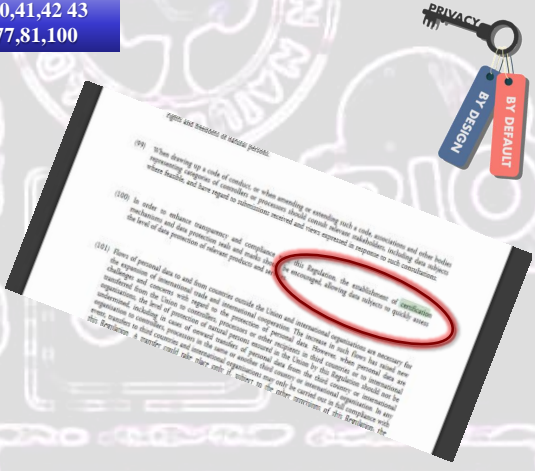


## Codici di condotta e Certificazioni

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

### L'art. 39. Certificazione

1. Gli Stati membri, il comitato europeo per la protezione dei dati e la Commissione incoraggiano, in particolare a livello unionale, l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento, delle operazioni di trattamento effettuate dai responsabili del trattamento e dagli incaricati del trattamento. Si tiene conto delle esigenze specifiche delle micro, piccole e medie imprese. [...]



Se adottati TQM e Certificazioni possono semplificare



## Un esempio pratico: schemi

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



Se adottati schemi riconosciuti TQM e Certificazioni

# NON CONFONDERSI: Privacy e ICT

P.I.A.  
D.V.R.

**Privacy Impact  
Assessment**

**ICT Risk  
Assessment**

Framework/Standard di riferimento:

ENISA: Privacy and Data Protection by Design

OASIS: Privacy Management Reference Model and Methodology (PMRM)

ART. 35, 36 C.do78, 89,96 – PIA: PRIMA (By Design/Default) PLA: in corso... e ciclico sul sistema

22 Luglio 2019 – seguire Misure  
Autorità Dati Particolari

**Ottemperanza ai  
principi privacy  
(art. 5, 9)**

**Protezione dei dati  
Personali  
(art. 32 oltre agli  
art. 4, 5, 30, 35, 40,  
83)**

GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

**Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101 [9124510]**

VEDI ANCHE [Newstetter del 22 luglio 2019](#)

Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101  
[\[Pubblicato sulla Gazzetta Ufficiale Serie Generale n. 178 del 29 luglio 2019\]](#)

Registro dei provvedimenti  
n. 146 del 5 giugno 2019

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione del dott. Antonello Sorio, presidente, della dott.ssa Augusta Iannini, vicepresidente, della dott.ssa Giovanna Bianchi Carini e della prof.ssa Lucia Caffarini, componenti, e del dott. Giuseppe Butta, segretario generale;

VISTO il 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 (di seguito "Regolamento");

VISTO il d.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali, di seguito il "Codice"), come rivelato dal d.lgs. 10 agosto 2018, n. 101 recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679";

VISTE le autorizzazioni generali adottate ai sensi degli artt. 26 e 40 del Codice;

CONSIDERATO che gli artt. 26 e 40 del Codice sono stati abrogati dall'art. 27, comma 1, lett. A), n. 2), del citato d.lgs. n. 101/2018;

CONSIDERATO che l'art. 21 del d.lgs. n. 101/2018, in attuazione delle disposizioni del Regolamento, ha demandato al Garante il compito di individuare, con proprio provvedimento di carattere generale, le prescrizioni contenute nelle autorizzazioni generali già adottate, relative alle situazioni di trattamento di cui agli artt. 5, par. 1, lett. c) ed n), 9, par. 2, lett. b) e 4, nonché al Capo IX, del Regolamento, che risultano compatibili con le disposizioni comunitarie e il decreto medesimo che ha rivelato il Codice, provvedendo, altresì, al loro aggiornamento ove necessario;

SENTENDO di dare attuazione al citato art. 21 del d.lgs. n. 101/2018 a mezzo del presente provvedimento, che produce effetti fino all'abrogazione, per le parti di pertinenza, delle regole deontologiche e delle misure di garanzia di cui agli artt. 2-quater e 2-septies del Codice;

RILEVATO che l'autorizzazione generale al trattamento dei dati giudiziari da parte di privati, di enti pubblici economici e di soggetti pubblici n. 7/2016, alla luce della disciplina applicabile ai medesimi stati contenuta nel Regolamento e nel Codice (art. 10 Regolamento; 2° comma del Codice e art. 37 del d.lgs. n. 101/2018), ha cessato di produrre effetti giuridici alla data del 19 settembre u.s., ai sensi del comma 3 della citata disposizione;

ART. 35, 36 C.do 89,96 – DOPO V.R. SI POSSONO DEFINIRE MISURE CREDIBILI!

## Reg.679/16 sulla Data Protection: **GAT**

### **GIA' AL PRIMO ANNO**

- **Oltre 600 provvedimenti**
- **Oltre 400 controlli**
- **Oltre 360 ricorsi esaminati**
- **Circa 4000 reclami, segnalazioni considerati**
- **43 violazioni di rilevanza giudiziaria**
- **3 milioni Euro riscosse al primo trimestre 2010**

**Controlli  
veri!  
Reg.680/16**

Intanto il bilancio 2017 dell'attività spedita dall'Autorità conferma il forte incremento dell'attività sanzionatoria registrata lo scorso anno. Nel corso del 2017 sono stati infatti definiti oltre 1.000 provvedimenti sanzionatori in più rispetto all'anno precedente, pari ad un aumento del 307%. L'importo delle sanzioni applicate con ordinanza-piùgiunzione sono cresciute ammontando ad oltre 13 milioni e 300 mila euro. Le sanzioni più riscosse dall'Ente sono state di circa 3 milioni e 800 mila euro (pari ad un complessivo 15% in più rispetto al 2016).

2009 15% incrementale nell'ultimo report 2018 sup. **8.600K€** comminati.

## Un ingaggio scorretto



Può costare al business più delle sanzioni  
...meglio una «**Captatio Benevolentiae**»

**ART 83  
G.A.T.**



## Chiese e associazioni religiose



Stampa e informazione

Tietosuojavaltuutettu/Jehovan todistajat – uskonnollinen yhdyyskunta

Corte di giustizia dell'Unione europea

**COMUNICATO STAMPA n. 103/18**

Lussemburgo, 10 luglio 2018

Sentenza nella causa C-25/17

**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**

*I trattamenti di dati personali effettuati nell'ambito di un'attività di questo tipo devono rispettare le norme del diritto dell'Unione in materia di protezione dei dati personali*

**NOVITA'**

ART. 91, C.do 165 – Applicazione conforme diritto costituzionale nazionale e rispetto Art. 17 TFUE



Reg.2016/679 e Dlg.101/18

## CRITICAL CONTROL NEWS



**Accountability:** «rendere conto» globale Titolare politiche sistemiche (Art. 24-26)

**Trasparenza:** flussi transfrontalieri (periodi di conservazione) (Art. 44-47)

**Sistema di gestione:** Documentazione, Struttura organigramma (Art.3), deleghe/audit indipendente

**Sanzioni:** fino ad un milione di € e/o 2-3% del fatturato di una *holding* (anche internazionale se sede IT) (Art.82/83)

**Data Breach:** Gestione notifica, Registro, modulistica, gruppo di risposta (Art.33)

**Ruoli DP:** Joint controllers, nomine di soggetti responsabili interni e/o esterni (Art.30)

**Data Protection Officer:** Art. 37,38 e 39, natura indipendente, supporto TDT e consorziale

**Audit periodici:** Interni e *outsourcing* coinvolti nei trattamenti, Gestione Reclami, Whistleblowing (Art.29)

**Diritto portabilità:** migrazioni tecnologiche ICT su Cloud Computing (ITIL, CoBIT e CSA); (Art. 20)

**Diritto all'Oblio:** Rafforza le facoltà di controllo degli utenti sui propri dati (Art. 17 e Art. 4 c1) Secure Erasure.

**Data Retention:** Misure di preservazione del dato adeguamento reale misure di accesso al dato (Art. 32)

**Formazione:** pianificata, verbalizzata e differenziata – **propedeutica ai trattamenti (Art. 29)**

Orientamento dato-centrico : perimetro network IT



*Dlg.vo 101/2018 e la Privacy 4.0*

Come il Centro PMA 4.0  
rende sostenibile la Privacy 4.0

**misure fisiche, logiche e organizzative**

**Sostenibile solo approccio TQM**

**G**overno  
**R**ischio  
**C**ontrollo

## Non tutto è mostruoso Sfruttare le novità favorevoli:

- Legittimo interesse (Art.4-11, C.do47)
- Co-titolarità fra Centri (anche estero)
- DPO congiunto e/o condiviso
- SPP anche in formato elettronico
- PLA e corresponsabilità esterne
- Integrazione Dlg.81/01, Dlg.231, SQS
- Art. 2-undecies – Limitaz. Diritti Interessato

***Dlg.vo 101/2018 TQM per la Data Protection***

***Dlg.vo 101/2018 in PMA***

Nuovo paradigma sfruttando il  
Dlg.191/07 - Artt. 14 e 20 c.3

**SCHEMI: GRC – TQM**  
**Metodologie: READINESS**

# Rischio



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

**INTEGRAZIONE: Dlg.vo 101/2018 TQM per i Dati**

# Governo



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

**INTEGRAZIONE: Dlg.vo 101/2018 TQM per i Dati**

# Controllo



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

*INTEGRAZIONE: Dlg.vo 101/2018 TQM per i Dati*

## PARTE 2

Adempimenti critici e loro  
implementazione nel SPPD per la PMA

*Privacy 4.0  
nella PMA*