

Ordine CdL Napoli
Convegno privacy
23 Maggio 2018

Relatori: Francesco Capaccio e Pietro Di Nono

REGOLAMENTO PRIVACY

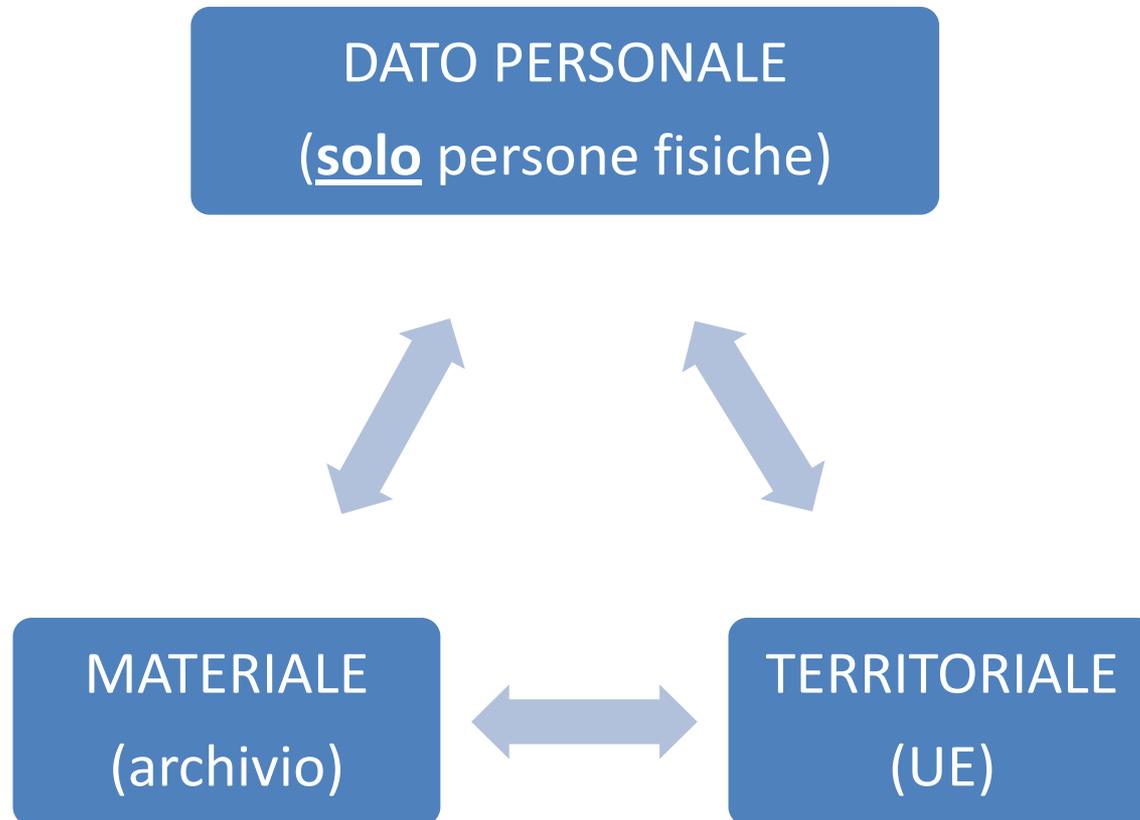
(GDPR – General Data Processing Regulation)

Reg. 679/2016

Entrata in vigore: **25 maggio 2018**

I DATI DA PROTEGGERE – Artt. 2-3

*«ogni individuo ha diritto alla protezione dei dati personali che lo riguardano»
(art. 8 Carta dei diritti fondamentali UE)*



I DATI DA PROTEGGERE – Art. 4

*«ogni individuo ha diritto alla protezione dei dati personali che lo riguardano»
(art. 8 Carta dei diritti fondamentali UE)*

TRATTAMENTO DI DATI DA PROTEGGERE

QUALSIASI OPERAZIONE O INSIEME DI OPERAZIONI, COMPIUTE CON O SENZA L'AUSILIO DI PROCESSI AUTOMATIZZATI E PPLICATE A DATI PERSONALI O INSIEME DI DATI PERSONALI, COME LA **RACCOLTA**, LA **REGISTRAZIONE**, L'**ORGANIZZAZIONE**, LA **STRUTTURAZIONE**, LA **CONSERVAZIONE**, L'**ADATTAMENTO** O LA **MODIFICA**, L'**ESTRAZIONE**, LA **CONSULTAZIONE**, L'**USO**, LA **COMUNICAZIONE** MEDIANTE **TRASMISSIONE**, LA **DIFFUSIONE** O QUALSIASI ALTRA FORMA DI **MESSA A DISPOSIZIONE**, IL **RAFFRONTO** O L'**INTERCONNESSIONE**, LA **LIMITAZIONE**, LA **CANCELLAZIONE** O LA **DISTRUZIONE**.

,

I DATI DA PROTEGGERE – Art. 4

DATI (persone «vive») DA PROTEGGERE «codificati»

DATO
PERSONALE

NEW

DATI
GENETICI

NEW

DATI
BIOMETRICI

NEW

DATI SULLA
SALUTE

DATI ART. 9
«SENSIBILI»

DATI ART. 10
«GIUDIZIARI»

I DATI DA PROTEGGERE – Art. 4

NON SONO DATI PERSONALI

- Indirizzo e-mail generico dell'azienda (es. info@.....)
- Numero di iscrizione alla CCIAA
- I dati anonimizzati in maniera irreversibile

LE FIGURE DELLA PRIVACY

LE FIGURE PRIVACY «CODIFICATE»

24-26

- TITOLARE/CONTITOLARE

27

- RAPPRESENTANTE

28

- RESPONSABILE

28 c. 3 b)

- INCARICATO

37

- DPO

LE FIGURE DELLA PRIVACY

TITOLARE

- Determina **le finalità** ed i **mezzi di trattamento** dei dati

RAPPRESENTANTE

- Va nominato per iscritto se i dati riguardano interessati UE ed il titolare o responsabile non è stabilito nell'UE

RESPONSABILE

- Incaricato del trattamento per conto del titolare (figura esterna)

INCARICATO

- Autorizzato dal titolare/responsabile al trattamento dei dati

DPO

- Controllore, consulente, formatore **indipendente, imparziale, autonomo**

LE FIGURE DELLA PRIVACY

LA FIGURE PRIVACY «NON CODIFICATA»

AMINISTRATORE DI SISTEMA

- ❑ PROVVEDIMENTO DEL GARANTE DEL 27/11/2008 MODIFICATO DAL PROVVEDIMENTO DEL 25 GIUGNO 2009
- ❑ **GESTIONE E MANUTENZIONE DI IMPIANTI DI ELABORAZIONE CON CUI VENGONO EFFETTUATI TRATTAMENTI DI DATI PERSONALI**
- ❑ **NON RIENTRA** CHI OCCASIONALMENTE INTERVIENE (RISOLVERE GUASTI O MALFUNZIONAMENTI) SUI SISTEMI DI ELABORAZIONE E SUI SISTEMI SOFTWARE

PRINCIPI GENERALI – art. 5



PRINCIPI GENERALI – art. 5

ACCOUNTABILITY

GIUSTIFICARE

DOCUMENTARE

DIMOSTRARE

OBBLIGHI DEL TITOLARE

TITOLARE **DEVE** SEMPRE:

- ❑ FORNIRE L'INFORMATIVA ALL'INTERESSATO (ART. 13)
- ❑ METTERE IN ATTO MISURE TECNICHE ED ORGANIZZATIVE ADEGUATE PER GARANTIRE ED ESSERE IN GRADO DI DIMOSTRARE (**PRIVACY BY DESIGN – PRIVACY BY DEFAULT**)
- ❑ NOTIFICARE AL GARANTE EVENTUALI «DATA BREACH» (ART. 33).

OBBLIGHI GENERALI DEL TITOLARE

TITOLARE **DEVE** SE SI REALIZZA LA PREVISIONE DEL GDPR:

- NOMINARE UN «RAPPRESENTANTE» (ART. 27) – CASI ART. 3 COMMA 2
- TENERE IL «REGISTRO DELLE ATTIVITA' DI TRATTAMENTO» (ART. 30) SALVO REALTA' FINO A 250 DIPENDENTI (**sempre opportuno**)
- NOTIFICIARE ALL'INTERESSATO I «DATA BREACH» CHE LO RIGUARDANO SE C'E' RISCHIO ELEVATO (ART. 34)
- EFFETTUARE LA VALUTAZIONE DI IMPATTO (ART. 35) – **attesa Garante** – linee guida WP 29 del 04.04.2017
- CONSULTARE «PREVENTIVAMENTE» IL GARANTE NEI CASI DI CUI ALL' ART. 36
- NOMINARE, NEI CASI PREVISTI, IL DPO (ART. 37) – da indicare nell'informativa ex art. 13 e da comunicare al GARANTE

OBBLIGHI GENERALI DEL TITOLARE

TITOLARE PUO':

- NOMINARE UN RESPONSABILE DEL TRATTAMENTO [ESTERNO] – ART. 28
- DESIGNARE DEGLI INCARICATI
- DESIGNARE L'AMMINISTRATORE DI SISTEMA
- NOMINARE, IN OGNI CASO, IL DPO (Garante FAQ del 26/03/2018) – [informativa + Garante]
- ADERIRE AI CODICI DI CONDOTTA (ART. 40) **quando e se elaborati**
- CERTIFICARE IL SISTEMA DI «PRIVACY» ADOTTATO (ART. 42) **de iure condendo**



CONSIGLIATI

L'INFORMATIVA – art. 13

CONTENUTI

- SOGGETTI
- FINALITA' DEL TRATTAMENTO (eventuale **profilazione**)
- FONDAMENTO GIURIDICO
- DESTINATARI (eventuale trasferimento a Paesi extra UE)
- DURATA DEL TRATTAMENTO
- DIRITTI DELL'INTERESSATO (modalità di esercizio degli stessi)
- CONSEGUENZE IN CASO DI REVOCA DEL CONSENSO
- CONSENSO (trattamento, trattamento artt. 9 e 10, trasmissione)

PROFILAZIONE – artt. 4 e 22

DEFINIZIONE (art. 4)

qualsiasi forma di **trattamento automatizzato** di dati personali consistente nell'utilizzo di tali dati personali **per valutare determinati aspetti personali relativi a una persona fisica**, in particolare per analizzare o prevedere aspetti riguardanti il **rendimento professionale**, la **situazione economica**, la **salute**, le **preferenze personali**, gli **interessi**, l'**affidabilità**, il **comportamento**, l'**ubicazione** o gli **spostamenti** di detta persona fisica

- ❑ L'INTERESSATO NON PUO' ESSERE SOTTOPOSTO AD UNA DECISIONE SULLA SOLA BASE DELLA PROFILAZIONE (eccezioni paragrafi 2, 3 e 4 art. 22)

DURATA DEL TRATTAMENTO

CATEGORIA	DURATA	FONTI NORMATIVE
lavoratori dipendenti	10 anni	2946 c.c., art. 43 DPR 600/73, Titolo I Capo III d.lgs. 81/2008
clienti e fornitori	10 anni	art. 2220 c.c. e comunque art. 22 DPR 600/73
candidati	finalità	provv. 2484965 del 04.04.2013

SITO WEB

- NOMINARE RESPONSABILE DEL TRATTAMENTO IL SERVIZIO DI «WEB HOSTING»
- VALUTARE UTILIZZO DEI COOKIES PER INFORMATIVA, E/O CONSENSO, E/O NOTIFICA AL GARANTE (?)
- VALUTARE UTILIZZO DI ALTRI FILE DI LOG AI FINI DELL'INFORMATIVA.

COOKIES

I cookie sono stringhe di testo di piccole dimensioni che i siti visitati dall'utente inviano al suo terminale (solitamente al browser), dove vengono memorizzati per essere poi ritrasmessi agli stessi siti alla successiva visita del medesimo utente

L'utente può ricevere sul suo terminale anche cookie che vengono inviati da siti o da web server diversi (c.d. "terze parti")

Si distinguono in due macro-categorie:

- TECNICI:** solo per migliorare la qualità della navigazione (analitici sono assimilati)
- PROFILAZIONE:** creano un profilo dell'utente per inviare allo stesso messaggi

ADEMPIMENTI NEGLI STUDI CDL

- INFORMATIVA AI PROPRI DIPENDENTI/COLLABORATORI
- RILASCIARE INFORMATIVA AI PROPRI CLIENTI (PERSONE FISICHE)
- (STUDIO PERSONA FISICA) RICEVERE L'INFORMATIVA DAL TITOLARE
- RICEVERE L'INCARICO DI «RESPONSABILE» DEL TRATTAMENTO PER CONTO DEI PROPRI CLIENTI (rischio di trattamento illecito)
- NOMINA DEI PROPRI DIPENDENTI/COLLABORATORI AD «INCARICATI DEL TRATTAMENTO PER CONTO DEI CLIENTI»
- VALUTARE LA NOMINA AMMINISTRATORE DI SISTEMA
- ISTITUIRE UNA *POLICY* DI STUDIO *PRIVACY* CON PARTICOLARE RIFERIMENTO ALLE STRUMENTAZIONI INFORMATICHE PER DIPENDENTI/COLLABORATORI (Garante – provv. 53/2018)
- REDIGERE IL REGISTRO DELLE ATTIVITA' DEI TRATTAMENTI
- SITO INTERNET – VALUTARE INFORMATIVA COOKIES E PER ALTRI FIEL DI LOG (EVITARE, SE POSSIBILE, LA PROFILAZIONE) E NOMINA RESPONSABILE WEB HOSTING
- ADEGUAMENTO A CODICI DI CONDOTTA E/O SISTEMI DI QUALIFICAZIONE (**quando adottati**)
- NOMINA DPO (per il singolo professionista da escludere, faq Garante)
- VALUTARE DPIA (WP29 del 04.04.17, salvo diversa indicazione del Garante)