

Nuova
data!

Pillola di GDPR:

Mercoledì 23 Maggio dalle 14.00 alle 15.30



 **C-DIRECT**
consulting



STUDIO LEGALE

Avv. Barbara De Cillis

Via delle Lame 58, Bologna

barbara.decillis@studiolegaledds.it

Tel./Fax 051.58844467 - Mob. 339.7028579

www.studiolegaledds.it

Il “frastagliato” panorama legislativo

Dir UE 95/46/CE del 24/10/1995 (direttiva madre)

D.Lgs. 196/03 – “Codice in materia di Trattamento dei Dati Personali”

Reg. EU 679/16 “Regolamento Europeo in materia di tutela dei dati personali”
entrato in vigore dal 25 maggio 2016
si applicherà a decorrere dal **25 maggio 2018**

L. 163 del 25 ottobre 2017 (L. di delegazione EU)

21 marzo 2018 (l bozza approvata dal Cons. Min)

(10 maggio) Schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Reg. UE 2016/679

21 maggio – scadenza delega conferita alle Camere - proroga della delega di tre mesi



LA RIVOLUZIONE COPERNICANA DEL G.D.P.R



ACCOUNTABILITY, PRIVACY BY DESIGN E BY DEFAULT

BASE GIURIDICA DEL TRATTAMENTO, MINIMIZZAZIONE E FINALITA'
Titolare e Responsabile del Trattamento devono mettere in atto
MISURE TECNICHE E ORGANIZZATIVE **ADEGUATE** PER GARANTIRE UN
LIVELLO DI SICUREZZA ADEGUATO AL RISCHIO

INDIVIDUARE

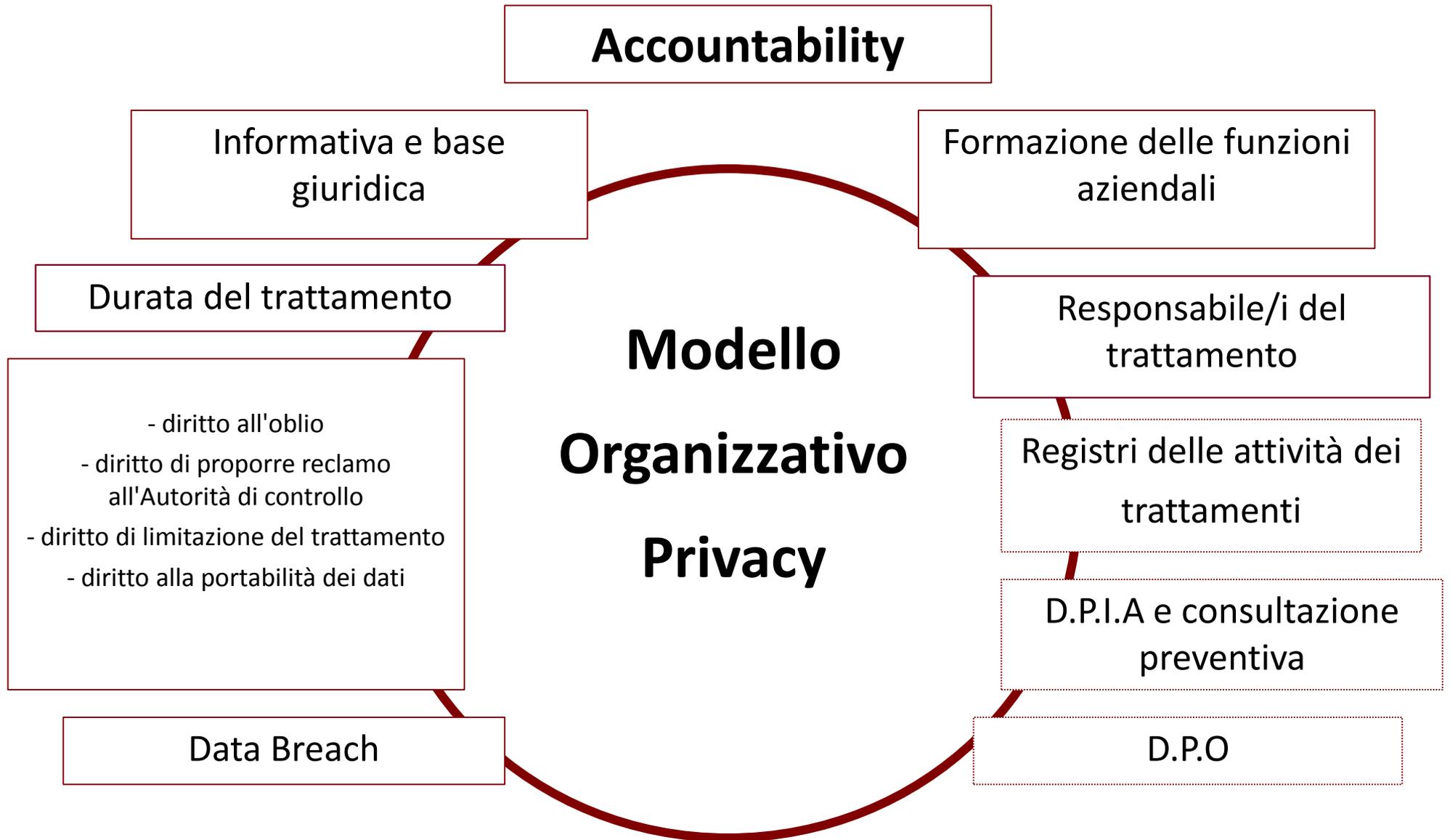
ADEMPIERE

DIMOSTRARE

OPPORTUNITA'

1. Sfruttare il GDPR per tutelare la riservatezza dei dati aziendali, asset strategico dell'azienda
2. Utilizzare i nuovi adempimenti come strumento di competitività, rinnovando l'impianto di data protection
3. Provvedere agli adempimenti con strumenti su misura, non esistono standard «buoni per tutti»

Principali novità G.D.P.R.



REGISTRO DELLE ATTIVITA' DEI TRATTAMENTI

- NON è obbligatorio** per le imprese che occupano **MENO di 250 dipendenti** salvo che:
- il trattamento possa presentare un rischio per i diritti e le libertà degli interessati
 - il trattamento non sia occasionale
 - il trattamento includa categorie particolari di dati

DATA PROTECTION IMPACT ASSESSMENT

- Deve essere eseguita** quando l'uso di nuove tecnologie può presentare un **rischio elevato per i diritti e le libertà delle persone fisiche**
- trattamento automatizzato che produce effetti giuridici sulle persone fisiche
 - trattamento su larga scala di particolari categorie di dati
 - sorveglianza sistematica su larga scala di zona accessibile al pubblico

DATA PROTECTION OFFICER

- Deve essere nominato** in caso di:
- trattamento eseguito da un'autorità pubblica o da un organismo pubblico
 - trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala
 - trattamento su larga scala di particolari categorie di dati

... Profilo sanzionatorio

M.O.P.

Informativa al trattamento dei dati – durata del trattamento	✓
Analisi e valutazione dei rischi	✓
Individuazione delle misure di sicurezza di tipo “fisico” e logico (sistemi informativi) adottate	✓
Gestione dei trattamenti per finalità di marketing	✓
Procedure di back up e disaster recovery	✓
Nomina Referente Privacy	✓
Nomina incaricati	✓
Nomina ADS	✓
Nomina D.P.O.	✓
Contrattualizzazione dei rapporti con i Responsabili del Trattamento	✓
Procedura di data breach (semplificata)	✓
Procedura di riscontro delle istanze degli interessati (semplificata)	✓
Valutazione di impatto	✓
Registri delle Attività dei Trattamenti del Titolare	✓
Registri delle Attività di trattamento del Responsabile	✓
Disciplina Sito web (Privacy Policy)	✓

Il "Ciclo Vitale" del dato



TO DO LIST



- Pianificare una revisione generale dell'architettura della data protection
- Verificare se sussiste l'obbligo (o valutare l'opportunità di) eseguire una D.P.I.A., nominare il D.P.O. e predisporre i registri delle attività dei trattamenti
- Eseguire il “Compatibility Test” sulle informative
- Censire i Responsabili dei Trattamenti e contrattualizzarne il rapporto
- Verificare la liceità dei trattamenti eseguiti
- Implementare la struttura di Governance Privacy
- Allocare i rischi rispetto all'innovato regime sanzionatorio
- Formare le funzioni aziendali preposte al trattamento dei dati