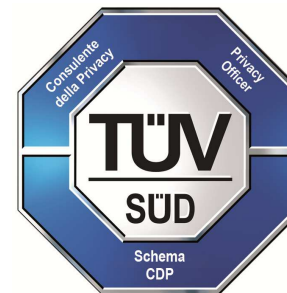


Verso il nuovo Regolamento Europeo Privacy



Chi sono?



UNI CEI EN ISO/IEC 17024:2012
iscrizione al Registro Numero
CDP_158

Armando Iovino – PQA Progetto Qualità Ambiente S.r.l.
Data protection officer

armando.iovino@pqa.it

<https://www.linkedin.com/pub/armando-iovino/5a/97/a83>



Progetto Qualità e Ambiente



Progetto Qualità e Ambiente

consulenza aziendale certificata



- ☐ Torino Corso Racconigi 180/6, 10141 Torino
- ☐ Milano Via Copernico 38 20125 Milano
- ☐ Mantova Via Parigi n. 38, 46047 Porto Mantovano

[visita la sezione](#)



Progetto Qualità e Ambiente

consulenza formazione

sicurezza sul lavoro
adempimenti privacy
ambiente
231/2001
qualità

in aula
e-learning
finanziata Fondimpresa
corsi aziendali



PROGETTO QUALITA' E AMBIENTE S.R.L.

pratiche A.U.A. | due diligence | gestione rifiuti e CO.NA.I. | impatti acustici | regolamento R.E.A.C.H.
valutazione dei rischi | incarichi RSPP | redazione D.V.R. | responsabilità sociale di impresa SA8000
sicurezza delle informazioni ISO 27001 | sistemi di gestione 9001-14001-18001 | normativa Dual Use
antiriciclaggio 231/2007 | piani di autocontrollo HACCP | audit di conformità

Via Parigi 38 – 46047 Porto Mantovano (Mn) | T 0376 387408 | info@pqa.it | www.pqa.it



AiFOS
Centro di Formazione



APINDUSTRIA
Associazione Piccole e Medie Industrie di Mantova



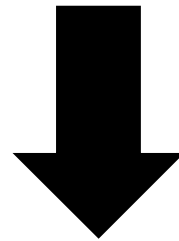
Progetto Qualità e Ambiente



APINDUSTRIA
Associazione Piccole e Medie Industrie di Mantova

La Normativa Privacy oggi: il quadro normativo

Direttiva Madre



**95/46/CE del 24 Ottobre 1995
(Recepita in maniera diversa dai 28 Paesi Membri)**



E in Italia?



**Recepita la Direttiva con la Legge 675/96
(Legge promulgata in maniera frettolosa per
onorare gli impegni derivanti dagli Accordi di
Schengen)**



**D.Lgs. 196/03 del 30 Giugno 2003 in vigore dal 1 Gennaio
2004 + Provvedimenti del Garante Privacy**



Semplificazioni D.L. 6/12/2011 Salva Italia: persone Giuridiche, Enti e Associazioni non rientrano nel campo di applicabilità

D.L. 9 Febbraio 2012, n.5 Decreto Sviluppo: viene abolito l'obbligo di presentazione del D.P.S. e di formazione del personale

E per i Cookie?

Se ne parla nella Direttiva 2002/58/CE, modificata dalla
Direttiva 2009/136/CE

Recepita in Italia dal D.Lgs. 69/2012 (non vengono fornite le
modalità per il rilascio dell'informativa semplificata)



Provvedimento del Garante Privacy 8 Maggio 2014



Chiarimenti in merito all'attuazione della Normativa in materia di Cookie
(5/06/2015)

Infografica. Il tuo sito/blog installa cookie? Cosa devi fare (10/06/2015)

Il Dato Privacy



Cosa si intende per dato?

**IL «DATO PERSONALE» È UNA
QUALUNQUE INFORMAZIONE RELATIVA
A PERSONA FISICA, ~~Persona giuridica, ente
ed associazione~~**

(Inclusi i suoni e le immagini)

Dato comune/identificativo

- Nome, cognome, indirizzo, ecc
- C.F.
- Indirizzo @mail, numero di telefono
- Indirizzo IP
- UserID e PW
- Stile di vita e abitudini di consumo
- Posizione geolocalizzata

Dato sensibile

- Stato di salute
- Origine razziale, etnica, convinzioni religiose e filosofiche
- Opinioni politiche, adesioni a partiti, sindacati, ecc
- Orientamento sessuale

**INFORMAZIONI CONCERNENTI GLI
ASPETTI PIU' INTIMI DELLA VITA
DELL'INDIVIDUO**

Dato giudiziario

- **Provvedimenti iscritti nel casellario giudiziale**
- **Sanzioni amministrative derivanti da reato**
- **Informazioni relative allo stato di imputato o indagato**

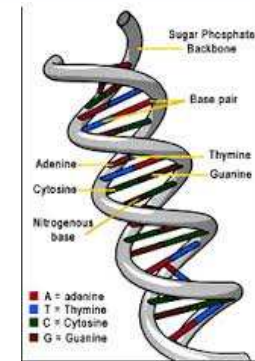
**SONO ESCLUSI I PROVVEDIMENTI
RELATIVI A CAUSE CIVILI**

Dato semi_sensibile



- **Dati biometrici**
- **Dati relativi alla capacità di solvibilità dei debiti**
- **Dati relativi alla situazione finanziaria**

Dati genetici



Informazioni relative al patrimonio genetico dell'individuo; fondamentalmente consistono nella ricostruzione della catena di Aminoacidi che ricostruiscono il DNA.

Trattamento dei dati

- Raccolta
- Conservazione
- Registrazione
- Organizzazione
- Raffronto
- Modificazione
- Diffusione
- Cancellazione
- Ecc.

Regolamento Privacy

Diventano dati sensibili anche i dati biometrici, i dati genetici e i dati giudiziari

Attenzione: diventa lecito trattarli se “il trattamento riguarda dati resi manifestamente pubblici dall’interessato”

Regolamento Privacy

Portabilità del dato

L'interessato ha il diritto, quando i dati sono trattati con mezzi elettronici, di ottenere dal responsabile del trattamento copia dei dati trattati in un formato elettronico che gli consenta di farne ulteriore uso.

Attenzione: la portabilità è diritto degli interessati, non di un titolare rispetto ai dati personali di terzi collocati su un sistema altrui (es. cloud)

Data Breach

- **Notifica della violazione all'Autorità competente entro 72/h**
- **Notifica della violazione all'interessato (se i dati mettono a serio rischio le libertà civili)**

I Soggetti Privacy

Il Titolare del trattamento

La persona fisica, giuridica, P.A., ente, associazione a cui competono le decisioni in ordine alle finalità e alle modalità di trattamento

Responsabile del trattamento

La persona fisica, giuridica, P.A., ente,
associazione preposti dal Titolare al
trattamento dei dati



Interno



Esterno

Incaricati al trattamento

**Le persone fisiche autorizzate dal
Titolare o dal Responsabile a compiere
operazioni di trattamento**

Interessato

**La persone fisica a cui si riferiscono i
dati personali.**

Amministratore di sistema

Figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti.

Provvedimento 27 Novembre 2008

Regolamento Privacy

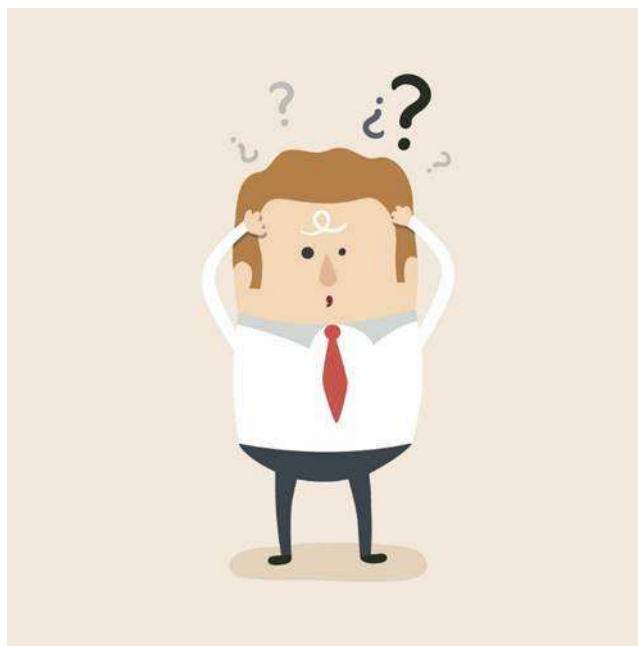
- **Data Controller (Titolare del trattamento)**
- **Data Processor (Responsabile del trattamento)**
- **Data Protection Officer: Responsabile della Protezione dei dati**

Regolamento Privacy

Il DPO obbligatorio per:

- **Pubblica Amministrazione**
- **Imprese oltre 250 dipendenti**
- **tutti i soggetti la cui attività principale consiste in trattamenti che per la loro natura, il loro oggetto o le loro finalità, richiedono un controllo periodico degli interessati.**

L'informativa Privacy



L'Informativa

È la comunicazione con la quale il Titolare (ai sensi dell'art 13 del Codice) informa l'interessato del trattamento svolto e può essere fornita oralmente o per iscritto.

Come si compone/1

- Finalità del trattamento
- Modalità del trattamento
- Natura obbligatoria o facoltativa del conferimento dei dati
- Conseguenze di un eventuale rifiuto di rispondere
- Soggetti ai quali i dati possono essere comunicati

Come si compone/2

- **Possibilità di diffusione dei dati**
- **Diritti di cui all'Art. 7**
- **Estremi identificativi del Titolare o del Responsabile**

(vedi informativa clienti PQA)

Informativa breve



Sanzioni

**Amministrativa dai 6.000 ai 36.000€
ridotta dei 2/5 quando le risorse
economiche sono limitate**

Regolamento Privacy

- **Tutti gli elementi della «vecchia» informativa**
- **Tempi di conservazione dei dati o criterio utilizzato per determinarlo**
- **Possibilità di revoca del consenso**
- **Possibilità di portabilità del dato**
- **Diritto di presentare reclamo alla A.C.**

Regolamento Privacy

- l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Regolamento Privacy

- **L'informativa dovrà essere solo scritta**
- **Il testo dovrà adottare sistemi di comunicazione di facile comprensione: pittogrammi, fumetti, tabelle, ecc.**

Misure Minime di Sicurezza (Allegato B)



Art. 31 Obblighi di Sicurezza

Obbligo di adottare procedure idonee a proteggere i dati personali archiviati sia su sistema informatico che cartaceo



Allegato B

Autenticazione

- **Obbligo di adottare un sistema di User ID e PW per l'accesso al sistema informatico (cambio PW 3/6 mesi)**
- **Garantire efficacia della PW**
- **File di Log Server**
- **Garantire la riservatezza della PW**
- **Disattivazione delle credenziali se non più utilizzate**
- **Nominare un custode delle PW**
- **Formazione del personale**

Autorizzazioni

- Individuare un profilo di autorizzazione per ogni incaricato
- Aggiornare i profili almeno annualmente
- Installare sistemi di screensaver automatizzati

Sicurezza informatica

- **Adottare un firewall efficace**
- **Adottare un SW Antivirus pay**
- **Aggiornare periodicamente i sistemi di protezione**
- **Non usare sistemi operativi «obsoleti»**
- **Creare una procedura per lo smaltimento delle apparecchiature dismesse**
- **Attenzione ai Device!**
- **Formazione degli incaricati (Criptolocker)**
- **Attenzione alle copie in Gdrive e DropBox!**

Back_Up

- **Predisporre un sistema idoneo a garantire la conservazione dei dati**
- **Garantire che almeno una copia sia conservata al di fuori dell'azienda**
- **Verificare i contratti con i fornitori di servizi in Cloud**
- **Attenzione ai Device!**
- **Eseguire periodicamente prove di ripristino**
- **Includere la @mail nei BUP**

Regola 25

Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

Archivi cartacei

- **Porre in armadi chiusi archivi contenenti dati sensibili (HR)**
- **Istituire un registro per l'accesso controllato ai locali contenenti dati sensibili**
- **Attenzione all'impresa di pulizie!!**
- **Come vengono smaltiti o distrutti i dati cartacei?**

Sanzioni

- **Amministrativa: dai 10.000 ai 120.000€**
- **Penale: arresto fino a 2 anni**
- **Civile (art.2050 c.c.)**

Accountability/1



il responsabile del trattamento adotta politiche e attua misure adeguate per garantire ed essere in grado di dimostrare che il trattamento dei dati personali effettuato è conforme allo stesso Regolamento

**M.O.P. Modello Organizzativo Privacy
(ex D.P.S ma molto più dettagliato)**

Accountability/2



Garantire maggiore trasparenza, verso gli Stakeholders, le Autorità competenti e gli Interessati

