

La «nuova» privacy:
le 10 cose indispensabili da sapere
per provare ad adeguarsi
(e un po' di appunti sulle novità)

Andrea Lisi

Avvocato, Presidente Anorc Professioni, DPO Ordine Avvocati e Ingegneri Lecce

Premessa:
l'Ansia da prestazione

***State tranquilli il 25 maggio non è successo nulla
(ma sta solo continuando un laborioso cammino)***

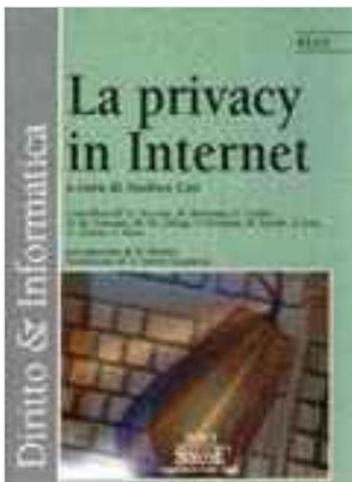
**Finché
c'è
VITA
c'è ANSIA.**



LEI NON SA
CHI SONO IO!



Un po' di volumi pubblicati... 😊



La privacy in Internet

Autori A. Lisi

Anno Edizione: 2003

Formato: 13 x 19

Pagine: 272

Codice: 41/25

Isbn: 9788824490153

Prezzo: € 15,00



Internet: profili giuridici e opportunità di mercato

di Andrea Lisi edito da Maggioli Editore, 2002



Attualmente l'articolo è fuori catalogo

Informazioni bibliografiche

Titolo del Libro: Internet: profili giuridici e opportunità di mercato
Collana: **Legate**
Genere: **Diritto**
ISBN-10: 8838721610

Autore: **Andrea Lisi**
Editore: **Maggioli Editore**
Data di Pubblicazione: 2002
Pagine: 436
ISBN-13: **9788838721618**

Pubblica amministrazione e privacy. Istruzioni per l'uso

di Andrea Lisi Federica Bertoni edito da CieRre, 2006



Disponibilità incerta

Informazioni bibliografiche del Libro

Titolo del Libro: Pubblica amministrazione e privacy. Istruzioni per l'uso
Data di Pubblicazione: 2006
Argomenti: **Privacy Amministrazione pubblica**
ISBN-13: **9788871377018**

Autori: **Andrea Lisi Federica Bertoni**
Editore: **CieRre**
Genere: **diritto**
Pagine: 347
ISBN-10: 887137701X

Il negozio telematico. I profili giuridici di un e-shop

di Andrea Lisi edito da Halley Editrice, 2007



Il negozio telematico. I profili giuridici di un e-shop: Con l'informatica e Internet si è potuto prescindere per la prima volta dal supporto cartaceo nello scambio di informazioni e comunicazioni a distanza, passando alle novità e alle comodità della trasmissione e conservazione della documentazione elettronica. Il testo si propone, così, di rendere comprensibile a tutti la materia e di fornire le risposte per capire come è regolamentato lo spazio commerciale telematico e quali sono le regole giuridiche per la realizzazione di un e-shop. L'opera affronta le seguenti tematiche: l'e-commerce nel world wide web: profili giuridici; i contratti informatici e telematici nel mercato digitale; la tutela del consumatore nei contratti B2C; i contratti B2B e l'e-marketplace; la tutela della privacy nei contratti on-line; i sistemi di e-payment; le problematiche nazionali di Internet. Conclude il libro un'esauriva appendice normativa e giurisprudenziale.

Attualmente l'articolo è fuori catalogo

GIURISPRUDENZA CRITICA
Collana diretta da Paolo Cendon

I CONTRATTI DI INTERNET

Sottoscrizione, nuovi contratti,
tutela del consumatore,
privacy e mezzi di pagamento

a cura di
Andrea Lisi

UTET
UNIVERSITÀ TORINO

PROFESSIONISTA
DELLA PRIVACY



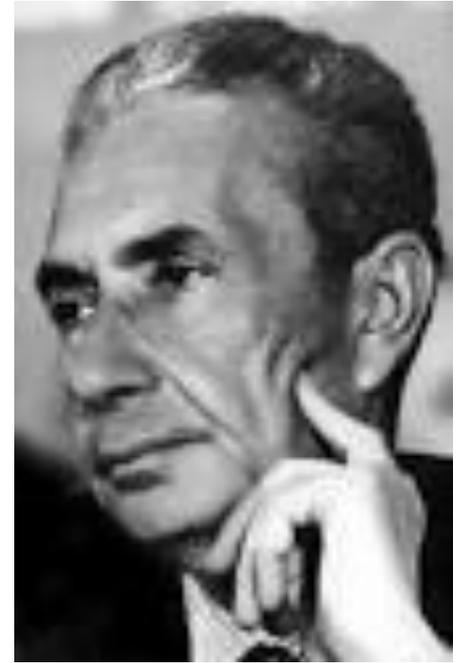
Andrea Lisi
EXPERT

Tesserina n° 13

L'iscrizione ad ANORC Professioni è da intendersi quale attestazione di qualità e di qualificazione professionale dei servizi prestati dall'associato conforme ai requisiti previsti dagli articoli 4, 7, 8 della Legge 4/2013 (Disposizioni in materia di professioni non organizzate in ordini o collegi).

Il presente tesserino professionale è rilasciato il 07/02/2018 e firmato digitalmente dalla Direzione

Siate indipendenti. Non guardate al domani, ma al dopodomani
(Aldo Moro)



L'Archivio di Stato di Roma ha pubblicato il volume 'Le lettere di Aldo Moro dalla prigionia alla storia' a cura di Michele Di Sivo, volume che propone tutte le immagini delle lettere inviate nei 55 giorni più lunghi della prima Repubblica da Aldo Moro. Tutte queste lettere sono note nel loro contenuto, ma solo ora sono state versate all'Archivio di Stato in quanto beni culturali e fonti della ricerca storica, quindi tutelate come documenti della nostra storia.

Ci avviciniamo pericolosamente all'**uomo di vetro** sempre visibile dai detentori del potere politico ed economico, con un rischio evidente per la libertà e la democrazia.

La legittimazione sociale della tecnologia, allora, non può essere affidata soltanto all'imperativo della sicurezza o alla logica dell'efficienza economica. Deve essere sempre misurata con il metro della democrazia e del rispetto della persona.



Stefano Rodotà

La «nuova privacy»: i principi generali

Art. 5 Qualità dei dati

I dati a carattere personale oggetto di un'elaborazione automatizzata sono:

- a) ottenuti e elaborati in modo lecito e corretto;
- b) registrati per scopi determinati e legittimi ed impiegati in una maniera non incompatibile con detti fini;
- c) adeguati, pertinenti e non eccessivi riguardo ai fini per i quali vengono registrati;
- d) esatti e, se necessario, aggiornati;
- e) conservati in una forma che consenta l'identificazione delle persone interessate per una durata non superiore a quella necessaria ai fini per i quali sono registrati.

Art. 6 Categorie speciali di dati

I dati di carattere personale indicanti l'origine razziale, le opinioni politiche, le convinzioni religiose o altri credo, nonché i dati a carattere personale relativi allo stato di salute ed alla vita sessuale, non possono essere elaborati automaticamente a meno che il diritto interno non preveda garanzie adatte. Lo stesso dicasi dei dati di carattere personale relativi alle condanne penali.

Art. 7 Sicurezza dei dati

Adeguate misure di sicurezza vengono adottate per la protezione di dati di carattere personale registrati nei casellari automatizzati contro la distruzione accidentale o non autorizzata, ovvero la perdita accidentale così come contro l'accesso ai dati, la modifica o la diffusione non autorizzate.

La «nuova privacy»: i principi generali

Art. 7 – Rispetto della vita privata e della vita familiare

Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni (riservatezza)

Art. 8 – Protezione dei dati di carattere personale

1. Ogni individuo ha **diritto alla protezione dei dati** di carattere personale che lo riguardano.
2. Tali dati devono essere trattati secondo il **principio di lealtà**, per **finalità determinate** e in base al **consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge**. Ogni individuo ha il **diritto di accedere** ai dati raccolti che lo riguardano e di **ottenerne la rettifica**.
3. Il rispetto di tali regole è soggetto al **controllo di un'autorità indipendente**.



Cosa è cambiato veramente con il GDPR?

*Persona
analogica*



[adapt to survive]

*Persona
digitale*

- Hai Facebook ?
- No
- Whatsapp ?
- No
- Instagram ?
- No
- Telegram ?
- No niente, però se vuoi sono proprio qui di fronte a te

@Ty_il_nano



Quello che le donne dicono



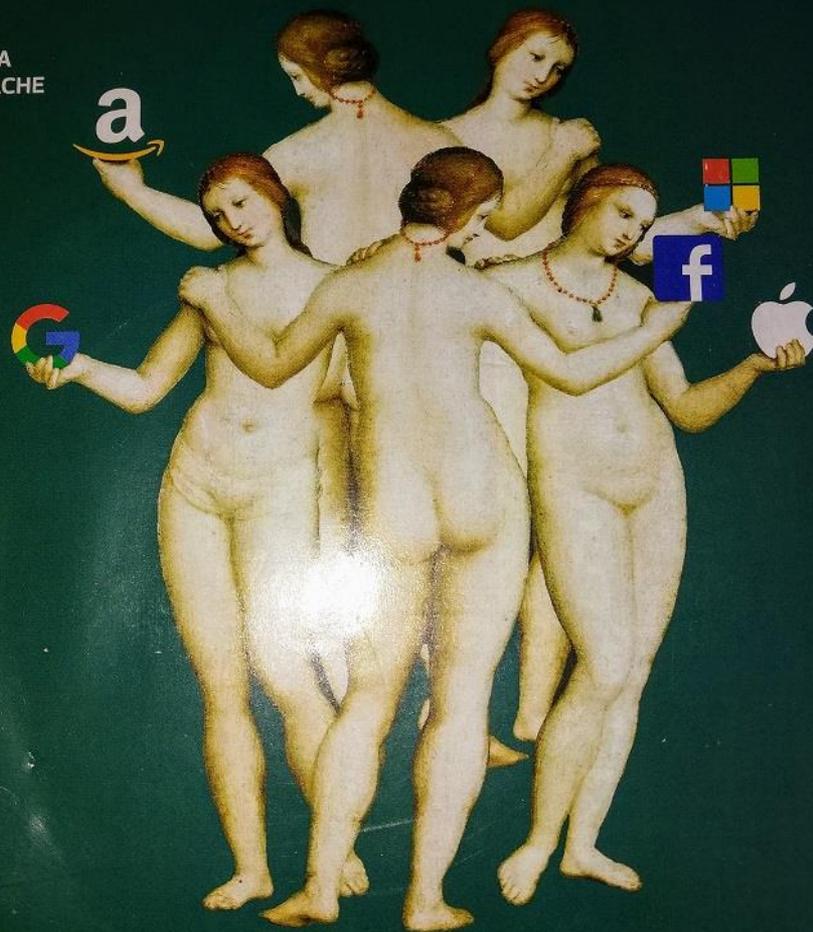
Inquadra la copertina
con l'app e cambiala come vuoi
Istruzioni a pagina 2

**FIPRONIL, L'INSETTICIDA
SPARITO DALLE CRONACHE
MA NON DALLE UOVA**

**FIBRA OTTICA
LA VELOCITÀ È SUPER
SOLO NELLO SPOT**

TEST

- Riso Arborio
- Televisori Oled
- Pneumatici
- Seggioloni
- Antivirus
- Scaldabagno



LE GRANDI SORELLE

APPLE. GOOGLE. MICROSOFT. FACEBOOK. AMAZON.
SUADENTI, RICCHE E POTENTI GRAZIE AI TUOI DATI

«Quello che mettete in rete resta. Per sempre. E tra chi lo guarda oggi e chi lo vedrà fra anni, c'è anche chi non vi conosce e potrebbe usarlo contro di voi»
(Antonello Soro, presidente Garante della privacy)



Cambridge Analytica, il caso dalla A alla Zuckerberg



(afp)

Dalla raccolta dei dati tramite il test sul social network alle scuse di Mark Zuckerberg manovre dello stregone Steve Bannon e le rivelazioni dell'analista Christopher Wylie: caso che sta scuotendo Facebook

di SIMONE COSIMI

QUANTO SONO AL SICURO I NOSTRI DATI? IL CASO CAMBRIDGE ANALYTICA

Mercoledì, 21 Marzo 2018

di Paolo Spagna, avvocato - contributor D&L Department

Il recente scandalo di portata internazionale, legato alle dichiarazioni di Christopher Wylie, venute alla luce negli ultimi giorni e relative alle metodologie di rilevazione statistica adottate nell'ultima campagna presidenziale Americana, hanno contribuito ad avvalorare il significato dell'identificazione dei dati personali a "nuovo petrolio". L'ex dipendente di Cambridge Analytica ha denunciato pubblicamente il **tacito meccanismo fraudolento relativo al trattamento dei dati compiuto su larga scala, senza consenso degli interessati**, realizzato durante la campagna elettorale di Donald Trump.



Leggendo quanto dichiarato dal [whistleblower\[1\]](#) americano si apprende infatti che **la campagna politica del candidato vincitore delle elezioni**



AGI > Innovazione



Facebook ci ascolta attraverso lo smartphone per poi mandarci la pubblicità?

Il social di Mark Zuckerberg ha già smentito a più riprese. Che cos'è l'illusione della frequenza di cui parla il Telegraph

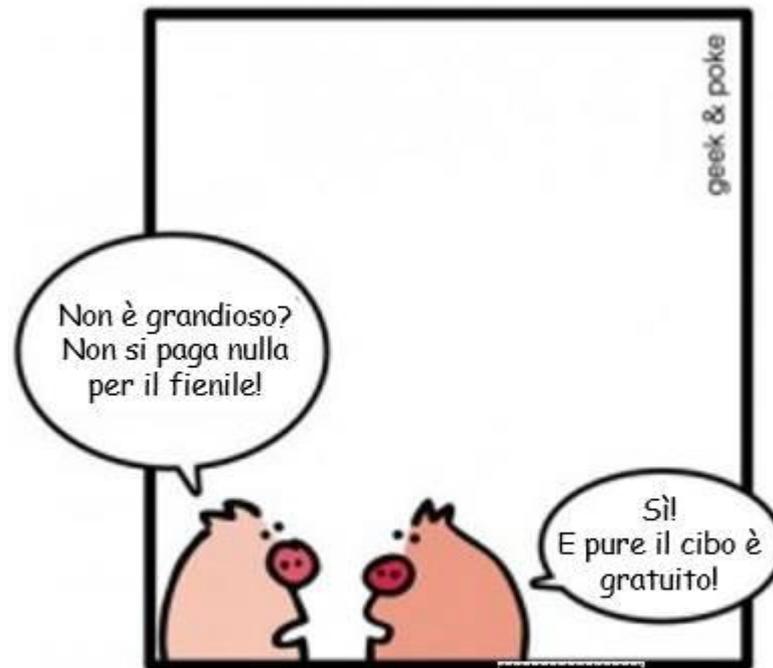
di **RAFFAELE ANGIUS** | 31 ottobre 2017, 07:50



agi **video**



Il valore delle informazioni



Se qualcosa è gratis, tu non
sei il cliente di un servizio.
Sei il prodotto finale.



Il valore delle informazioni

La conoscenza è potere – FRANCESCO BACONE



Oggi anche i dati e le informazioni sono potere
Più l'informazione è personale più ha potere chi la detiene



Oggetto delle informazioni: hobby, gusti, desideri, età, capacità economica,
orientamento politico e sessuale
in 60 secondi su facebook sono caricati 2 milioni di contenuti!

 ✕

We've selected shipping to

ITALY
(Change country)

OK

YOOX

SHOP FASHION / DESIGN+ART



DONNA



UOMO



BAMBINI



DESIGN+ART

 ✕

YOOX NEWS

ISCRIVITI ALLA NEWSLETTER
E SCOPRI LE ULTIME NOVITÀ
E PROMOZIONI

INSERISCI LA TUA E-MAIL

Donna Uomo

ISCRIVITI

MYOOX REGISTRAZIONE

Completa i tuoi ordini più velocemente e approfitta delle promozioni dedicate ai clienti registrati

Scopri tutti i vantaggi



REGISTRATI CON LA TUA E-MAIL

NOME

COGNOME

E-MAIL



Andrea Lisi

Aggiorna informazioni

Visualizza Registro attività 10+ ...

Diario Informazioni Amici 3901 Foto Altro

Cosa hai studiato presso Università Cattolica? x

15 elementi in sospeso

In breve

io sono ovviamente un italian digital minion! 😊

- Fondatore e Titolare presso Anorc
- Titolare presso Studio Legale Lisi
- Ha studiato presso Università Cattolica del Sacro Cuore - Sede di Milano
- Ha studiato presso Sapienza Università di Roma
- Ha studiato presso Università Cattolica

Stato Foto/video Avvenimento importante



A cosa stai pensando?

Tutti Pubblica



Andrea Lisi

1 h

SI o NO? Pillola Blu o Pillola Rossa?
Ricordate tutti la scena di Matrix?
Mi permetto di rinfrescarvi la memoria qui: <https://www.youtube.com/watch?v=C52iPuvbPUA> e Vi prego di guardarla adesso con attenzione, dopo aver visto tutti questi inutili dibattiti televisivi con Renzi onnipresente da una parte (ormai nel suo immenso egocentrismo il nostro Presidente del Consiglio si fida

Sponsorizzata



PosteID abilitato a SPID. POSTEID.POSTE.IT

PosteID è l'identità digitale di



235 x 263 - topnegozi.it
ma nel posto giusto può cambiare una vita.



«da un grande potere derivano
grandi responsabilità»





La fiducia nel mercato digitale...

Regolamento eIDAS (electronic IDentification Authentication and Signature):
Regolamento (UE) N. 910/2014 del PARLAMENTO EUROPEO e del CONSIGLIO del
23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le
transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE

Regolamento GDPR (General Data Protection Regulation): Regolamento (UE) N.
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

I principi ispiratori dei due Regolamenti

Regolamento eIDAS:

*(1) Instaurare **la fiducia negli ambienti online è fondamentale per lo sviluppo economico e sociale**. La mancanza di fiducia, dovuta in particolare a una percepita assenza di certezza giuridica, scoraggia i consumatori, le imprese e le autorità pubbliche dall'effettuare transazioni per via elettronica e dall'adottare nuovi servizi.*

(2) Il presente regolamento mira a rafforzare la fiducia nelle transazioni elettroniche nel mercato interno fornendo una base comune per interazioni elettroniche sicure fra cittadini, imprese e autorità pubbliche, in modo da migliorare l'efficacia dei servizi elettronici pubblici e privati, nonché dell'eBusiness e del commercio elettronico, nell'Unione europea.

Regolamento GDPR:

(1) La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

(6) La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali.

*(7) Tale evoluzione richiede un quadro più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, **data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno**.*

Punto 1)

Che cos'è la «privacy»?

Ormai la privacy come “Diritto ad essere lasciati soli” (*Right to be let alone* - articolo di Warren e Brandeis, *Right to Privacy* 1890), quindi diritto alla riservatezza della propria sfera privata e a non subire intrusioni indesiderate nella propria vita intima, non esiste più
(privacy statica)



il GDPR si occupa del diritto alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Quindi il GDPR fa riferimento principalmente a un diritto alla trasparenza sulla circolazione dei propri propri dati e cioè al diritto di controllare la diffusione dell'informazione circa se stessi
(privacy dinamica e partecipativa)

Punto 2)

Occorre fare tutto di nuovo?

«Il regolamento non ha modificato in modo sostanziale i concetti e i principi fondamentali della legislazione in materia di protezione dei dati introdotta nel 1995. La grande maggioranza dei titolari del trattamento e dei responsabili del trattamento che rispettano già le attuali disposizioni dell'UE non dovrà quindi introdurre importanti modifiche nelle proprie operazioni di trattamento dei dati per conformarsi al regolamento»

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO - Bruxelles, 24.1.2018 COM(2018) - Maggiore protezione, nuove opportunità – Orientamenti della Commissione per l'applicazione diretta del regolamento generale sulla protezione dei dati a partire dal 25 maggio 2018

[Home](#) / [News](#) / Ora che il Regolamento 679/2016 è pienamente esecutivo il Codice della protezione dei dati personali è da considerarsi abrogato?

ORA CHE IL REGOLAMENTO 679/2016 È PIENAMENTE ESECUTIVO IL CODICE DELLA PROTEZIONE DEI DATI PERSONALI È DA CONSIDERARSI ABROGATO?

di Andrea Lisi, avvocato - Presidente di ANORC Professioni e Coordinatore Digital&Law Department

Lunedì, 28 Maggio 2018

25 maggio 2018: una data che ha ridefinito i confini normativi Europei, finora tracciati in ambito Privacy.

Sebbene il Regolamento generale sulla protezione dei dati (General Data Protection Regulation, emanato con il Regolamento UE 2016/679) abbia acquisito piena applicabilità, **il processo di adeguamento della normativa nazionale al GDPR risulta ancora ben lontano dal potersi considerare concluso.**

Il GDPR, pur essendo **self-executing**, richiede



Punto 3)

È questione solo informatica?



Punto 4)

Esistono soluzioni «chiavi in mano»?



Punto 5)

Devo farmi certificare «DPO»?



Punto 6)

Non posso più trattare i dati personali dei miei clienti e devo richiedere «di nuovo» il consenso?

La «privacy» **non è un diritto assoluto** ma si contempera con gli altri diritti dell'ordinamento e con le altre attività, ad esempio:

- **diritto di difesa**
- diritto di cronaca
- diritto dell'impresa
- attività di ricerca
- attività di marketing
- diritto alla trasparenza
- ... «legittimo interesse»

Punto 7)

Devo cambiare tutte le informative e le vecchie non sono più valide?



Punto 8)

Devo modificare i contratti?
Ci sono tanti documenti da preparare?



Informative e contratti...

LE BUGIE PIÙ COMUNI



Punto 10)

Devo avere un «team privacy»?



Cosa fare allora?



NEL REGOLAMENTO PRIVACY UE:

- **adempimenti generali:** trasparenza
(informativa, consenso, diritto di accesso, diritto alla portabilità dei dati, diritto alla limitazione del trattamento, diritto all'oblio, registro trattamenti, analisi dei rischi)
- **adempimenti speciali:** accountability
(notifica «data breach», consultazione preventiva e PIA)
- **adempimenti organizzativi:** organizzazione
(formalizzazione rapporti tra titolari e contitolari, titolari e responsabili, responsabili e subresponsabili, responsabili e incaricati, incarico DPO, formazione/istruzioni e misure di sicurezza)

Le principali obbligazioni di compliance previste nel Regolamento UE 2016/679

Consultazione preventiva
Art. 36

Configurazione ruoli
Artt. 26, 27, 28, 29

Privacy by design e privacy by default
Art. 25

Valutazione d'impatto sulla protezione dei dati
Art. 35

Responsabile della protezione dei dati (DPO)
Artt. 37, 38 e 39

Registri delle attività di trattamento
Art. 30

Notifica e comunicazione "data breach"
Artt. 33 e 34

Sicurezza dei dati
Art. 32

I RUOLI e LE RESPONSABILITÀ:

Con il Regolamento UE viene in parte ridisegnato l'organigramma privacy, con l'introduzione di nuove figure soggettive e l'attribuzione di nuovi compiti e responsabilità:

- Titolare del trattamento (*data controller*);
- Contitolare (*joint controller*);
- Responsabile del trattamento (*data processor*);
- Sub-responsabile (*subprocessor*);
- Responsabile della protezione dei dati o *Data Protection Officer* (DPO).

I RUOLI e LE RESPONSABILITÀ nel Regolamento UE:

Con il Regolamento UE viene in parte ridisegnato l'organigramma privacy, con l'introduzione di nuove figure soggettive e l'attribuzione di nuovi compiti e responsabilità:

- **Titolare del trattamento** (*data controller*) (art 4 punto 7): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, *singolarmente o insieme ad altri*, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (ved. Artt. 24 e ss) ;
- **Contitolare** (*joint controller*) (art. 26);
- **Responsabile del trattamento** (*data processor*) (art. 4 punto 8): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (ved. art 28);
- **Sub-responsabile** (*subprocessor*) (vd. Art. 28) ;
- **Responsabile della protezione dei dati** o *Data Protection Officer* (DPO) (artt. 37 e seguenti).

Responsabile del trattamento (art. 28)

- deve essere individuato sulla base dell'esperienza, della capacità e dell'affidabilità e, quindi, deve presentare **garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate**, in modo tale che il trattamento soddisfi i requisiti del regolamento e garantisca la tutela dei diritti dell'interessato.
- I trattamenti da parte di un responsabile del trattamento devono essere disciplinati da un **contratto** o da **altro atto giuridico** che **vincoli** il responsabile al titolare del trattamento e che regoli l'oggetto e la durata del trattamento, la finalità perseguita, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.
- Il responsabile può ricorrere a un altro responsabile **solo previa autorizzazione scritta**, specifica o generale, del titolare del trattamento.

Trattamento sotto l'autorità del titolare o del responsabile del trattamento (art. 29)

Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento (gli attuali incaricati) che abbia accesso a dati personali **non può** trattare tali dati **se non è istruito** in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.



è consigliabile continuare ad applicare quanto previsto dall'attuale art. 30 del D.Lgs. 196/03

Il responsabile della protezione dei dati (DPO) (art. 37 - designazione)

La designazione del DPO da parte del titolare e del responsabile è **obbligatoria** quando il trattamento:

- è effettuato da un'**autorità pubblica** o da un **organismo pubblico**, eccettuate le autorità giurisdizionali;
- consiste in attività di monitoraggio **regolare** e **sistematico** su **larga scala**;
- riguarda dati sensibili e giudiziari su **larga scala**;



Il diritto dell'Unione o degli Stati membri **possono** prevedere altri casi per i quali è obbligatorio designare un DPO

Il responsabile della protezione dei dati (DPO) (art. 37 – designazione)

- è designato in funzione della **conoscenza specialistica** della normativa in materia di protezione dei dati personali e della **qualificata esperienza** sull'applicazione della stessa;
- può essere **un dipendente** del titolare o del responsabile del trattamento oppure **un professionista o una società** sulla base di un contratto di servizi (assenza conflitto di interessi);
- i dati di contatto del DPO devono essere resi pubblici e comunicati all'autorità di controllo.

Il responsabile della protezione dei dati (DPO) (art. 37 – designazione)

- è designato in funzione della **conoscenza specialistica** della normativa in materia di protezione dei dati personali e della **qualificata esperienza** sull'applicazione della stessa;
- può essere **un dipendente** del titolare o del responsabile del trattamento oppure **un professionista o una società** sulla base di un contratto di servizi (assenza conflitto di interessi);
- i dati di contatto del DPO devono essere resi pubblici e comunicati all'autorità di controllo.

Il responsabile della protezione dei dati (DPO) (art. 38 – posizione)

- **deve essere tempestivamente e adeguatamente coinvolto** in tutte le questioni riguardanti la protezione dei dati personali;
- **deve essere sostenuto** nell'esecuzione dei suoi compiti con le necessarie risorse umane, tecnologiche e finanziarie;
- **non deve ricevere** alcuna istruzione per quanto riguarda l'esecuzione dei propri compiti;
- **non può** essere rimosso o penalizzato per l'adempimento dei propri compiti;
- **riferisce** direttamente al vertice gerarchico;
- **funge** da punto di contatto per gli interessati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti.

Il responsabile della protezione dei dati (DPO) (art. 39 – compiti)

Il responsabile della protezione dei dati è incaricato **almeno** dei seguenti compiti:

- **informa** e **fornisce consulenza**, anche ai dipendenti che eseguono il trattamento, in merito agli obblighi previsti in materia di protezione dei dati personali;
- **sorveglia** l'osservanza dei predetti obblighi e degli eventuali disciplinari interni, incluso il riparto delle responsabilità e la formazione del personale;
- **fornisce**, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati personali e ne **sorveglia** lo svolgimento ai sensi dell'art. 35;
- **funge** da punto di contatto per l'autorità di controllo e **coopera** con la medesima per tutte le questioni connesse al trattamento dei dati personali, inclusa la consultazione preventiva di cui all'art. 36.



Nell'eseguire i propri compiti il DPO deve valutare attentamente i rischi inerenti al trattamento posto in essere, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo

I soggetti del trattamento

```
graph TD; A[I soggetti del trattamento] --> B[Soggetti attivi]; A --> C[Soggetti passivi interessati]; A --> D[Responsabile della protezione dei dati personali (DPO)];
```

Soggetti attivi

- ✓ Titolare del trattamento e gli eventuali contitolari
- ✓ Responsabile del trattamento
- ✓ Rappresentante del titolare o del responsabile del trattamento
- ✓ Personale dipendente del titolare o del responsabile del trattamento

Soggetti passivi

interessati

Responsabile della protezione dei dati personali (DPO)

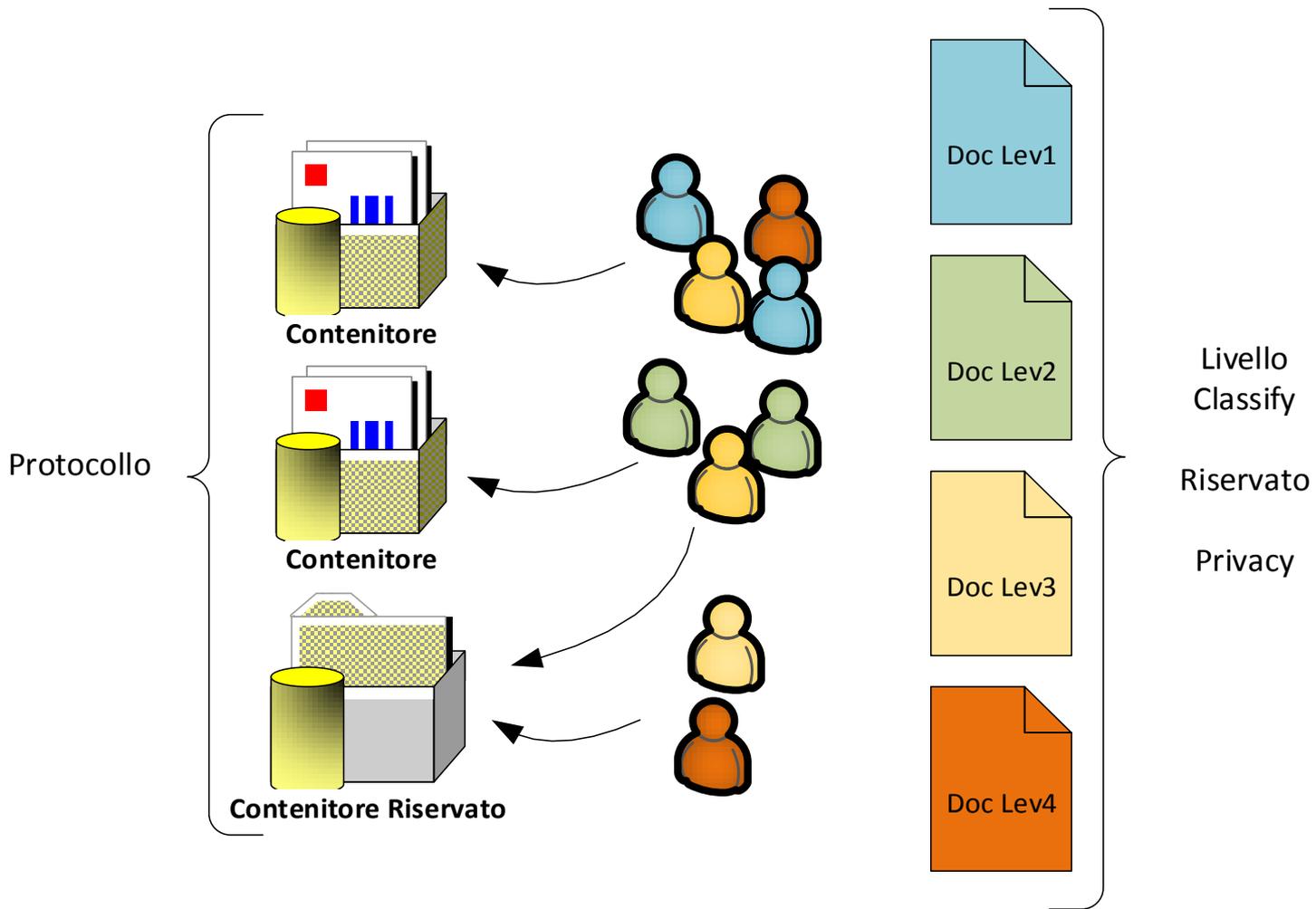
Privacy “by design” e privacy “by default” (art. 25)

- Le **applicazioni** e i **servizi** che comportano il trattamento di dati personali devono tener conto, **fin dalla loro progettazione** dei principi e delle regole previste dal Regolamento in modo da **minimizzare a priori** non solo la raccolta dei dati, ma anche le operazioni di trattamento successive (cfr. considerando 78)
- Utilizzo di tecniche, quali ad esempio la **minimizzazione** e la **pseudonimizzazione**, che consentano di garantire che vengano trattati solo i dati personali strettamente necessari alle finalità perseguite, secondo i principi di necessità, pertinenza adeguatezza e non eccedenza (cfr. art. 3 D.Lgs. 196/03)

Considerando 78

.....In fase di sviluppo, progettazione, selezione e utilizzo di **applicazioni**, **servizi** e **prodotti** basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati. I principi della protezione dei dati fin dalla progettazione e di default dovrebbero essere presi in considerazione **anche nell'ambito degli appalti pubblici**.

Esempio di privacy by design e privacy by default



Registri delle attività di trattamento (art. 30)

- Il titolare e il responsabile del trattamento **devono tenere**, in forma scritta, anche in formato elettronico, un registro delle attività di trattamento svolte sotto la propria responsabilità i cui contenuti sono elencati rispettivamente nei paragrafi 1 e 2 dell'art. 30;
- Questo obbligo **non si applica** alle imprese o organizzazioni con meno di 250 dipendenti, **a meno che** il trattamento che esse effettuano possa rappresentare un rischio per i diritti e le libertà degli interessati, non sia occasionale o includa il trattamento di dati sensibili o giudiziari;
- In caso di eventuali ispezioni il registro delle attività di trattamento **deve essere** messo a disposizione dell'autorità di controllo;

Contenuti del registro tenuto dal titolare del trattamento (art. 30.1)

- il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del DPO;
- le finalità del trattamento;
- la descrizione delle categorie di interessati e della natura dei dati personali (identificativi, relativi alla salute, biometrici, genetici, giudiziari)
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

Contenuti del registro tenuto dal titolare del trattamento (art. 30.1)

- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale (compresa la loro identificazione). Per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.



Cfr. art. 38, comma 2, del D.lgs. 196/03 – contenuti della notifica al Garante

Contenuti del registro tenuto dal responsabile del trattamento (art. 30.2)

- a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
- b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
- c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
- d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'art. 30.1;

Guida del Garante per la protezione dei dati personali all'applicazione del GDPR (luglio 2017)

- La tenuta del registro dei trattamenti **non costituisce un adempimento formale** bensì **parte integrante di un sistema di corretta gestione dei dati personali**. Per tale motivo, si invitano tutti i titolari e i responsabili del trattamento, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro e, in ogni caso, a compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche.
- Niente vieta a un titolare o responsabile di inserire - oltre a quelle previste dall'art. 30 del GDPR - ulteriori informazioni proprio nell'ottica della complessiva valutazione di impatto dei trattamenti svolti.

Suggerimento: ulteriori opportune informazioni che si potrebbero inserire nel registro

L'obbligo di tenere il registro delle attività di trattamento **potrebbe essere l'occasione** per raccogliere ulteriori utili informazioni rispetto a quelle indicate nell'art. 30 del GDPR, quali ad esempio;

- attività effettuate
- base giuridica del trattamento
- elenco terzi coinvolti
- analisi del rischio per singolo applicativo e/o servizio
- esistenza di valutazione d'impatto e consultazione preventiva
- documentazione a supporto del trattamento (es. informativa e consenso)
- procedure per l'esercizio dei diritti dell'interessato
- provvedimenti specifici dell'autorità di controllo

Come costruirlo

- **Gestione centralizzata** del registro assicurando però il coinvolgimento costante nella procedura di redazione - ma soprattutto di aggiornamento - dei soggetti che hanno una più ampia visione delle attività di trattamento e che devono essere responsabilizzati e formati in ordine al valore aggiunto che tale documento può apportare al fine di assicurare una gestione corretta e trasparente dei flussi di dati personali;
- Il Registro è prima di tutto uno **strumento per mappare i flussi dei trattamenti di dati all'interno dell'organizzazione** e, quindi, è opportuno aggiungere ulteriori informazioni inerenti ai database che contengono le informazioni trattate, i software mediante i quali i dati vengono processati e i server utilizzati nei trattamenti.

Aggiornamento del registro delle attività di trattamento

- diversamente da quanto prevedeva il Codice privacy per il Documento Programmatico sulla Sicurezza, il GDPR non prevede una data e neppure un obbligo espresso di aggiornamento del registro delle attività di trattamento.
- ma allora.....il registro delle attività di trattamento bisogna aggiornarlo periodicamente? e con quale periodicità?



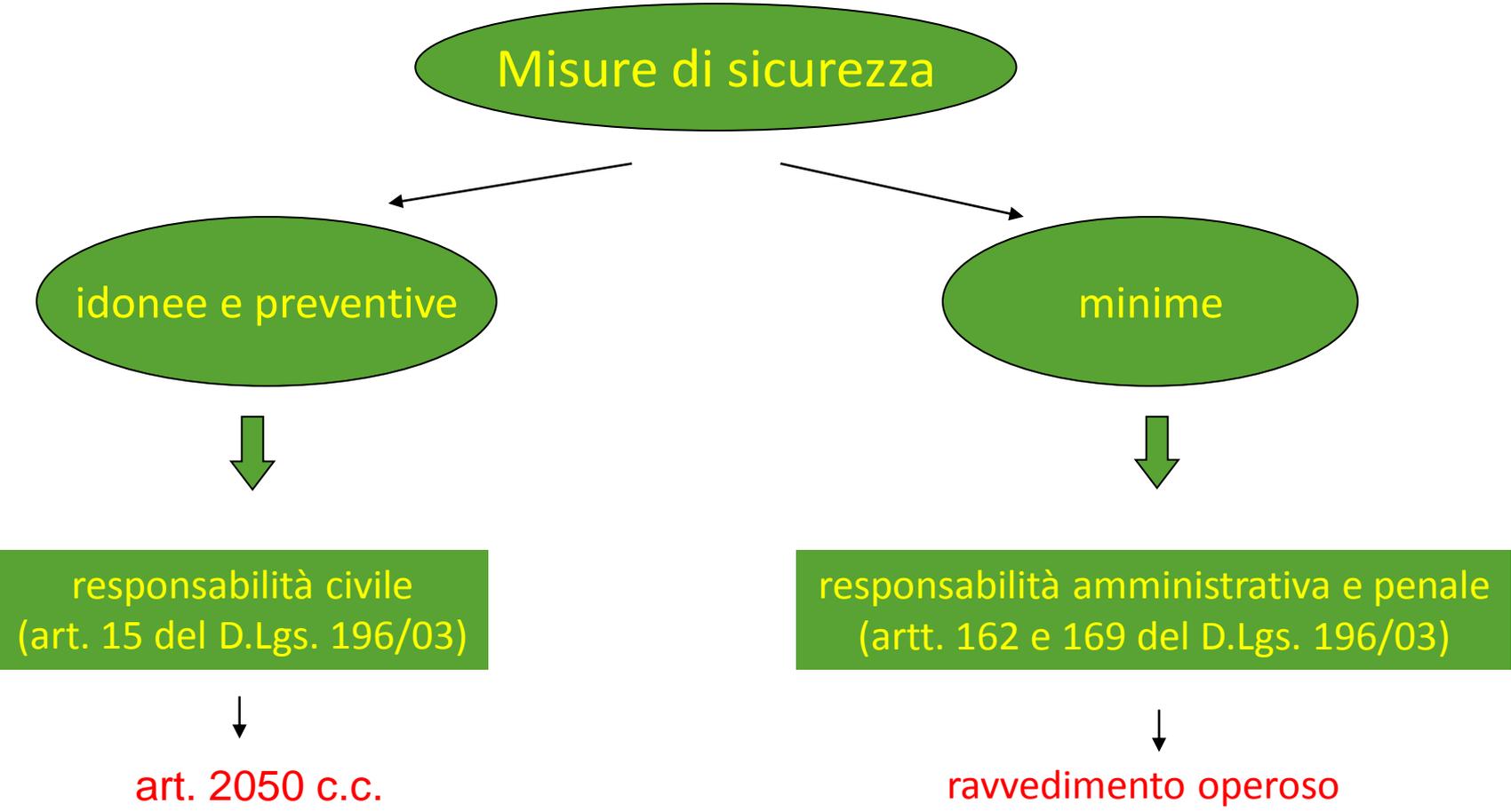
Principio di accountability: il titolare deve non solo garantire che i trattamenti che effettua sono conformi al GDPR, **ma anche essere in grado di dimostrarlo!!!!**

Le misure di sicurezza
confronto tra D.Lgs. 196/03 e GDPR

Le misure di sicurezza nel D.Lgs. 196/03

- Misure idonee e preventive (art. 31)
- Misure minime (artt. 33, 34 e 35 – Disciplinare tecnico allegato B)
- Misure “necessarie” prescritte dal Garante per la protezione dei dati personali ai sensi dell’art. 154, comma 1, lett.c) del D.Lgs. 196/03 con propri provvedimenti di carattere generale riguardanti particolari categorie di titolari e di attività di trattamento, oppure provvedimenti specifici nei confronti di singoli titolari

Misure di sicurezza e responsabilità nel D.lgs. 196/03



Sicurezza del trattamento (art. 32 GDPR)

Il titolare e il responsabile del trattamento, tenuto conto:

dello stato dell'arte e
dei costi di
attuazione

della natura, dell'oggetto, del
contesto e delle finalità
perseguite dal trattamento

dei rischi di varia probabilità
e gravità per i diritti e le
libertà delle persone fisiche

mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

- a) la pseudonimizzazione e la cifratura dei dati personali;
- b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- d) una procedura per **testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative** al fine di garantire la sicurezza del trattamento.

Scalabilità e adeguatezza delle misure di sicurezza al caso concreto

WP29, Opinione 3/2010, p. 13, § 45: “... nel determinare i tipi di azioni da attuare, non esistono alternative valide alle soluzioni “su misura”. Infatti, le misure specifiche da applicare devono essere determinate in funzione dei fatti e delle circostanze di **ciascun caso specifico**, con particolare attenzione al **rischio** inerente al trattamento e al **tipo di dati**. Un approccio uguale per tutti avrebbe il solo effetto di costringere i titolari del trattamento all'interno di strutture inadatte e si rivelerebbe quindi fallimentare”

Scalabilità e adeguatezza delle misure di sicurezza al caso concreto

Garante per la protezione dei dati personali - Guida all'applicazione del Regolamento europeo p. 27:

“Non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure ‘minime’ di sicurezza (ex art. 33 Codice) poiché tale valutazione sarà rimessa, **caso per caso**, al titolare e al responsabile in rapporto ai rischi specificamente individuati come dall’art. 32 del regolamento”

Le 7 misure minime di sicurezza previste nel Codice per la protezione dei dati personali:

1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

a) autenticazione informatica;

b) adozione di procedure di gestione delle credenziali di autenticazione;

c) utilizzazione di un sistema di autorizzazione;

d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o manutenzione degli strumenti elettronici;

e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;

f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;

g) *abrogato*

h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Allegato B al d.lgs. 196/2003: tra le misure minime di sicurezza è previsto, al numero 18, che il titolare fornisca agli incaricati istruzioni relative al salvataggio almeno settimanale dei dati. L'unico obbligo, quindi, era quello di prevedere opportuni sistemi di back-up che permettessero di duplicare su differenti supporti di memoria le informazioni e, quindi, mettere al sicuro tali dati!

Cosa chiede il D.Lgs. n° 196/2003, Allegato B (1/4)

Un sistema di Autenticazione informatica:

1. Credenziali per il superamento di una procedura di autenticazione relativa ad un trattamento o un insieme di trattamenti
2. Credenziali costituite da:
 - Codice e parola chiave
 - Dispositivo di autenticazione
 - Caratteristica biometrica
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali
4. Istruzioni per assicurare la segretezza
5. La Parola chiave:
 - Deve essere composta da almeno 8 caratteri o, se lo strumento non lo consente, da un numero pari al massimo consentito
 - Non deve contenere riferimenti riconducibili all'incaricato
 - Deve essere modificata dall'incaricato al primo utilizzo e almeno ogni sei mesi (nel caso di dati sensibili e giudiziari tre mesi)

Cosa chiede il D.Lgs.196/2003, Allegato B (2/4)

6. Il codice di autenticazione (Login) non può essere assegnato ad altri incaricati, neppure in tempi diversi
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica
8. Credenziali disattivate anche in caso di perdita della qualità
9. Istruzioni per non lasciare incustodito e accessibile lo strumento elettronico
10. Modalità con le quali il titolare può assicurare la disponibilità in caso di assenza o impedimento dell'incaricato
 - Da applicare solo nei casi in cui si utilizzi la componente riservata
 - Sono impartite idonee e preventive disposizioni scritte
 - Custodia delle copie delle credenziali e relativo accesso
11. Le disposizioni precedenti non si applicano per dati personali destinati alla diffusione

Cosa chiede il D.Lgs.196/2003, Allegato B (3/4)

Un sistema di Autorizzazione informatica:

- Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione
- Profili individuati e configurati anteriormente all'inizio del trattamento
- Periodicamente e comunque almeno annualmente è verificata la sussistenza delle condizioni

Altre misure di sicurezza:

- La lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione
- Dati personali protetti contro il rischio di intrusione e dell'azione di programmi mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale
- Aggiornamenti periodici dei programmi per prevenire la vulnerabilità di strumenti e per correggere difetti dovranno essere effettuati almeno annualmente (semestralmente per dati sensibili o giudiziari)
- Istruzioni organizzative e tecniche per il salvataggio dei dati con frequenza almeno settimanale

Cosa chiede il D.Lgs.196/2003, Allegato B (4/4)

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari:

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo mediante l'utilizzo di idonei strumenti elettronici
21. Istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili
22. Riutilizzo dei supporti rimovibili
23. Ripristino dell'accesso ai dati
24. Trattamento disgiunto di dati idonei a rilevare lo stato di salute e la vita sessuale per gli organismi sanitari e gli esercenti le professioni sanitarie. Trattamento di dati relativi all'identità genetica.

Misure di tutela e garanzia

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

Cosa chiede il D.Lgs.196/2003, Allegato B (4/4)

Già fare il minimo e comprenderlo è una prima (buona) base di partenza per avviare un percorso complesso verso l'accountability...



Notifica e comunicazione delle violazioni dei dati personali (data breach)

Definizione di violazione di dati personali (art. 4.12 del GDPR)

la violazione di sicurezza che comporta accidentalmente o in modo illecito la **distruzione**, la **perdita**, la **modifica**, la **divulgazione non autorizzata** o **l'accesso ai dati personali** trasmessi, conservati o comunque trattati;

L'obbligo di notificare gli eventi di data breach non è una novità assoluta

Violazioni di dati personali (data breach)
Gli adempimenti previsti

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Il Garante per la protezione dei dati personali ha adottato una serie di provvedimenti che fissano per amministrazioni pubbliche e aziende l'obbligo di comunicazione nei casi in cui - a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi o altre calamità - si dovesse verificare la perdita, la distruzione o la diffusione indebita di dati personali conservati, trasmessi o comunque trattati. La scheda, che ha mere finalità divulgative, riassume i casi finora esaminati.

SOCIETA' TELEFONICHE E INTERNET PROVIDER
Art. 32-bis del Codice in materia di protezione dei dati personali (d. lgs. 196/2003), Regolamento UE 611/13, Provvedimento del Garante n. 161 del 4 aprile 2013 [doc. web n. 2388260]

- L'obbligo di comunicazione al Garante (mediante un apposito modello di comunicazione) riguarda i fornitori di servizi telefonici e di accesso a Internet (e non, ad esempio, i siti internet che diffondono contenuti, i motori di ricerca, gli internet point, le reti aziendali).
- In caso di violazione dei dati personali, società di tic e isp devono:
 - a. entro 24 ore dalla scoperta dell'evento, fornire al Garante le informazioni necessarie a consentire una prima valutazione dell'entità della violazione
 - b. entro 3 giorni dalla scoperta, informare anche ciascun utente coinvolto, comunicando gli elementi previsti dal Regolamento 611/2013 e dal provvedimento del Garante n. 361 del 4 aprile 2013.
- La comunicazione agli utenti non è dovuta se si dimostra di aver utilizzato misure di sicurezza nonché sistemi di cifratura e di anonimizzazione che rendono inintelligibili i dati. Nei casi più gravi, il Garante può comunque imporre la comunicazione agli interessati.
- Per consentire l'attività di accertamento del Garante, società telefoniche e provider devono tenere un inventario costantemente aggiornato delle violazioni subite.
- **SANZIONI AMMINISTRATIVE PREVISTE** (art. 162-bis del Codice in materia di protezione dei dati personali)
 - per mancata o ritardata comunicazione al Garante: da 25mila a 150mila euro;
 - per omissione o mancata comunicazione agli utenti: da 150 euro a 1000 euro per ogni società, ente o persona interessata;
 - per mancata tenuta dell'inventario delle violazioni aggiornato: da 20mila a 120mila euro.

BIOMETRIA
Provvedimento n. 513 del 12 novembre 2014 [doc. web n. 3556992]

- Entro 24 ore dalla conoscenza del fatto, i titolari del trattamento (scienze, amministrazioni pubbliche, ecc.) comunicano al Garante (tramite il modello allegato al provvedimento) tutte le violazioni dei dati o gli incidenti informativi che possano avere un impatto significativo sui sistemi biometrici installati o sui dati personali custoditi.

DOSSIER SANITARIO ELETTRONICO
Provvedimento n. 333 del 4 giugno 2015 [doc. web n. 4084632]

- Entro 48 ore dalla conoscenza del fatto, le strutture sanitarie pubbliche e private sono tenute a comunicare al Garante (tramite il modello allegato al provvedimento) tutte le violazioni dei dati o gli incidenti informativi che possano avere un impatto significativo sui dati personali trattati attraverso il dossier sanitario.

AMMINISTRAZIONI PUBBLICHE
Provvedimento n. 392 del 2 luglio 2015 [doc. web n. 4129029]

- Entro 48 ore dalla conoscenza del fatto, le amministrazioni pubbliche sono tenute a comunicare al Garante (tramite il modello allegato al provvedimento) tutte le violazioni dei dati o gli incidenti informativi che possano avere un impatto significativo sui dati personali contenuti nelle proprie banche dati.

Per approfondimenti, consultare i provvedimenti pubblicati sul sito: www.garanteprivacy.it

I PROVVEDIMENTI CITATI NELL'INFOGRAFICA

- Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach) 4 aprile 2013
- Provvedimento generale prescrittivo in tema di biometria 12 novembre 2014
- Linee guida in materia di Dossier sanitario 4 giugno 2015
- Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche 2 luglio 2015

Quando è necessario effettuare la notifica di una violazione dei dati personali all'autorità di controllo? (art. 33)

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo **senza ingiustificato ritardo** e, ove possibile, **entro 72** ore dal momento in cui ne è venuto a conoscenza, **a meno che** sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, **è corredata dei motivi del ritardo**.
2. Il responsabile del trattamento **informa il titolare del trattamento senza ingiustificato ritardo** dopo essere venuto a conoscenza della violazione.

Comunicazione di una violazione dei dati personali all'interessato (art. 34)

1. Quando la violazione dei dati personali è suscettibile di presentare un **rischio elevato per i diritti e le libertà delle persone fisiche**, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.
2. La comunicazione all'interessato **descrive con un linguaggio semplice e chiaro** la natura della violazione dei dati personali e contiene **almeno:**
 - il nome e i dati di contatto del DPO o altri soggetti dai quali poter ottenere ulteriori informazioni;
 - la descrizione delle probabili conseguenze della violazione;
 - le misure adottate per porvi rimedio e attenuarne i possibili effetti negativi;

Casi per i quali la comunicazione di una violazione dei dati personali all'interessato non è dovuta (art. 34.3)

- il titolare del trattamento **aveva adottato** misure tecniche ed organizzative adeguate per proteggere i dati personali oggetto della violazione (es. pseudonimizzazione o cifratura);
- il titolare del trattamento **ha successivamente adottato** misure in grado di scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- la comunicazione **richiederebbe sforzi sproporzionati**. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Obbligo di documentazione (art. 33.5)

Il titolare del trattamento **documenta qualsiasi violazione dei dati personali**, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.



Tale documentazione **consente all'autorità di controllo di verificare il rispetto del presente articolo.**

Cosa è cambiato dal 25 maggio 2018?

- **tutti i titolari** dovranno notificare all'autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo";
- la notifica all'autorità di controllo dell'avvenuta violazione non è obbligatoria, essendo subordinata **alla valutazione del rischio** per gli interessati, che spetta al titolare.
- tutti i titolari **dovranno in ogni caso documentare** le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative conseguenze e i provvedimenti adottati (in caso di accertamento la documentazione va fornita all'autorità di controllo);

Responsabilità civile e sistema sanzionatorio

Diritto al risarcimento e responsabilità (art. 82)

- Chiunque subisca un danno **materiale** o **immateriale** (*patrimoniale e non patrimoniale*) causato da una violazione del presente regolamento **ha il diritto di ottenere il risarcimento del danno** dal titolare del trattamento o dal responsabile del trattamento;
- Un **titolare del trattamento** risponde per il danno cagionato dal **su**o trattamento che violi il regolamento.
- Un **responsabile del trattamento** risponde per il danno causato **solo se non ha adempiuto** gli obblighi del regolamento specificatamente diretti ai responsabili del trattamento **o ha agito in modo difforme o contrario** rispetto alle legittime istruzioni del titolare del trattamento;

Diritto al risarcimento e responsabilità (art. 82)

- Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità **se dimostra** che l'evento dannoso non gli è in alcun modo imputabile;
- Qualora più titolari del trattamento o responsabili del trattamento, oppure entrambi, siano coinvolti nello stesso trattamento e siano responsabili dell'eventuale danno causato, ogni titolare del trattamento o responsabile del trattamento **è responsabile in solido per l'intero ammontare del danno**, al fine di garantire il risarcimento effettivo dell'interessato;



Importanza della corretta contrattualizzazione dei rapporti tra contitolari o tra titolari e responsabili

Diritto al risarcimento e responsabilità (art. 82)

- Il titolare o il responsabile del trattamento che ha risarcito l'intero danno, **ha il diritto di rivalersi** sugli altri titolari o responsabili, coinvolti nello stesso trattamento, della parte del risarcimento corrispondente alla loro parte di responsabilità per il medesimo danno;
- Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno **sono promosse** dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro.

Condizioni generali per infliggere sanzioni amministrative pecuniarie (art. 83)

- Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte in relazione alle violazioni del regolamento siano in ogni singolo caso **effettive**, **proporzionate** e **dissuasive**;
- Le sanzioni amministrative pecuniarie sono inflitte **in aggiunta** o **in luogo** delle misure imposte dall'autorità di controllo nell'ambito dell'esercizio dei propri poteri correttivi;

Condizioni generali per infliggere sanzioni amministrative pecuniarie (art. 83.4)

La violazione delle seguenti disposizioni è soggetta a sanzioni amministrative pecuniarie **fino a 10.000.000 di euro**, o per le imprese, **fino al 2 % del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore:

- a) obblighi del titolare del trattamento e del responsabile del trattamento
- consenso dei minori (**art. 8**);
 - trattamento che non richiede l'identificazione (**art. 11**);
 - principi di privacy by design e by default (**art. 25**);
 - accordo interno per determinare responsabilità tra contitolari (**art. 26**);
 - nomina del rappresentante di titolari o dei responsabili non stabiliti nell'Unione e i suoi compiti (**art. 27**);
 - compiti e responsabilità del responsabile del trattamento (**art. 28**);
 - trattamento da parte dei dipendenti e collaboratori del titolare o del responsabile (**art. 29**);

Condizioni generali per infliggere sanzioni amministrative pecuniarie (art. 83.4)

- tenuta dei registri delle attività di trattamento (art. 30);
- cooperazione del titolare o del responsabile del trattamento con l'autorità di controllo (art. 31);
- adozione di misure di sicurezza adeguate (art. 32);
- notifica all'autorità di controllo di una violazione di dati personali (art.33);
- comunicazione all'interessato di una violazione di dati personali (art. 34);
- valutazione d'impatto (art. 35);
- consultazione preventiva (art. 36);
- designazione del DPO (art. 37);
- obblighi del titolare e del responsabile nei confronti del DPO (art. 38);
- compiti assegnati al DPO (art. 39);
- obblighi in materia di certificazione (art. 42).

Condizioni generali per infliggere sanzioni amministrative pecuniarie (art. 83.5)

La violazione delle seguenti disposizioni è soggetta a sanzioni amministrative pecuniarie **fino a 20.000.000 di euro**, o per le imprese, **fino al 4 % del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore:

- a) principi generali applicabili al trattamento (**art. 5**), condizioni di liceità del trattamento (**art. 6**), condizioni per il consenso (**art. 7**) e trattamento di categorie particolari di dati personali (**art. 9**);
- b) diritti degli interessati (**artt. da 12 a 22**);
- c) trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale (**artt. da 44 a 49**);
- d) obblighi previsti dalle legislazioni degli Stati membri adottate a norma del capo IX (giornalismo, espressione accademica o letteraria, accesso ai documenti delle PA, rapporti di lavoro, archiviazione nel pubblico interesse, ricerca scientifica, storica o statistica);
- e) negato accesso all'autorità di controllo durante l'esercizio dei propri poteri di indagine o inosservanza di un suo provvedimento di carattere correttivo;

un piano di «assessment» per il nostro Studio

FASE - 1
Valutazione della compliance

FASE - 2
Impostazione del registro
dei trattamenti

FASE - 3
Individuazione dei ruoli
e delle responsabilità

FASE - 4
Stesura e/o modifica della
documentazione

FASE - 5
Valutazione dei rischi e
definizione delle politiche
di sicurezza

FASE - 6
Implementazione del
processo di data breach

FASE - 7
Definizione delle modalità
per la valutazione di
impatto

FASE - 8
Implementazione delle procedure per
garantire l'esercizio dei diritti degli
interessati

formazione obbligatoria e documentazione

L'accountability non è (solo) questione di hardware, software, o information security, ma è prima di tutto organizzazione delle risorse umane (che vanno formate e rese consapevoli) e documentazione adeguata delle scelte effettuate



Prime Conclusioni

Posso usare formati elettronici per i miei «documenti privacy»?



Seconde Conclusioni

E dropbox?





GRAZIE PER L'ATTENZIONE

andrealisi@studiolegalelisi.it