Il Regolamento UE 2016/679

Protezione delle persone fisiche con riguardo al trattamento dei dati personali e libera circolazione di tali dati

Genova, 10 luglio 2017

Avv. Giacomo Maccaferro
Studio Legale Guerrini

Data is everywhere

- The amount of data on the global level is growing by 50 per cent annually

- Acxion is one of the big data brokers. It is a US Company which collects, analyses and interprets customer business information for its clients

- It is said that it has 20 billion customer records and information on 96% of the house-holds in the United States

- Fonte: International Working Group on Data Protection in Telecomunications 55th Meeting, 5-6 May 2014, Skopie

- Insurance companies use tracking technology to monitor their clients and to offer financial rewards in return for data showing physical activities

- Fonte: International Working Group on Data Protection in Telecomunications 57th Meeting 27-28 April 2015, Seoul

Quadro sintetico del diritto europeo e internazionale in materia di protezione dei dati personali

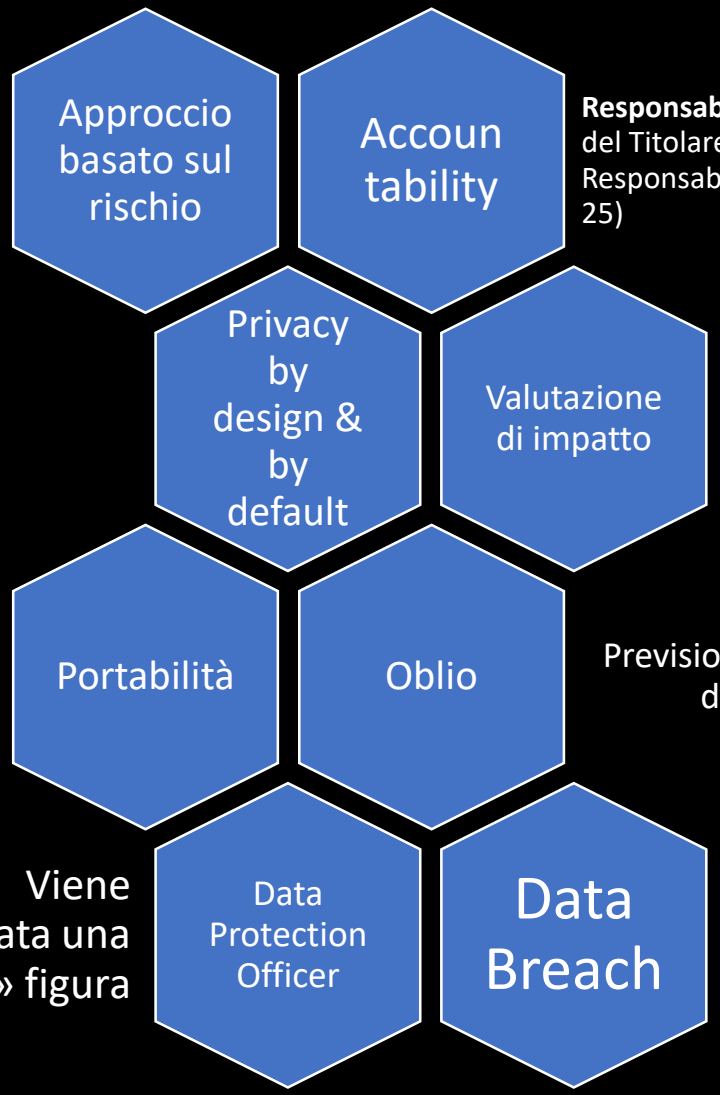
Unione Europea

- La **Carta dei diritti fondamentali dell'Unione Europea** (artt. 7 e 8 Protezione dei dati di carattere personale. Carta Europea di Nizza 2001). TFUE art. 16
- **Direttiva 95/46/CE** (c.d. Direttiva Madre) sarà abrogata nel maggio 2018
- Le **Direttive Comunitarie 2002/58/CE e 2009/136/UE** relative al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche
- **Regolamento (UE) 2016/679 Regolamento generale sulla protezione dei dati** che abroga la direttiva 95/46/CE
- **Direttiva (UE) 2016/680** relativa al trattamento dei dati personali da parte delle autorità competenti a fini del perseguimento di reati

Consiglio d'Europa

- Convenzione europea dei diritti dell'uomo **CEDU** (art. 8 Diritto al rispetto della vita privata e familiare) 4.11.1950
- Convenzione n. 108/1981 protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale

Le principali novità introdotte dal Regolamento UE



Responsabilizzazione del Titolare e Responsabile (artt. 24 e 25)

Previsione di nuovi diritti

Viene individuata una «nuova» figura

Principio di Accountability

Accountability

- **Responsabilità del titolare del trattamento artt. 5 comma 2 e 24** (C74-C78)
- *«Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed* ***essere in grado di dimostrare****, che il trattamento è effettuato conformemente al presente regolamento»*
- L'azienda dovrà determinare autonomamente Modi, Garanzie e Limiti del Trattamento.

Approccio bassato sul rischio

- Il Regolamento sceglie un approccio di «**Responsabilizzazione**» (Accountability) dei soggetti (Titolari e Responsabili) che controllano il Sistema di Gestione Privacy; (art. 5 comma 2)
- L'ottica è quella del Comportamento Proattivo, Valutazione ex ante del Rischio. **Do not wait for privacy risks to materialize** (Ann. Cavoukian)

Criteri

- Privacy by design e by default (art. 25)
- Valutazione d'impatto sulla protezione dei dati (*Data Protection Impact Assessment, art. 35*)
- Data Breach Notication (art. 33)

Privacy by design e by default art. 25 RGPD

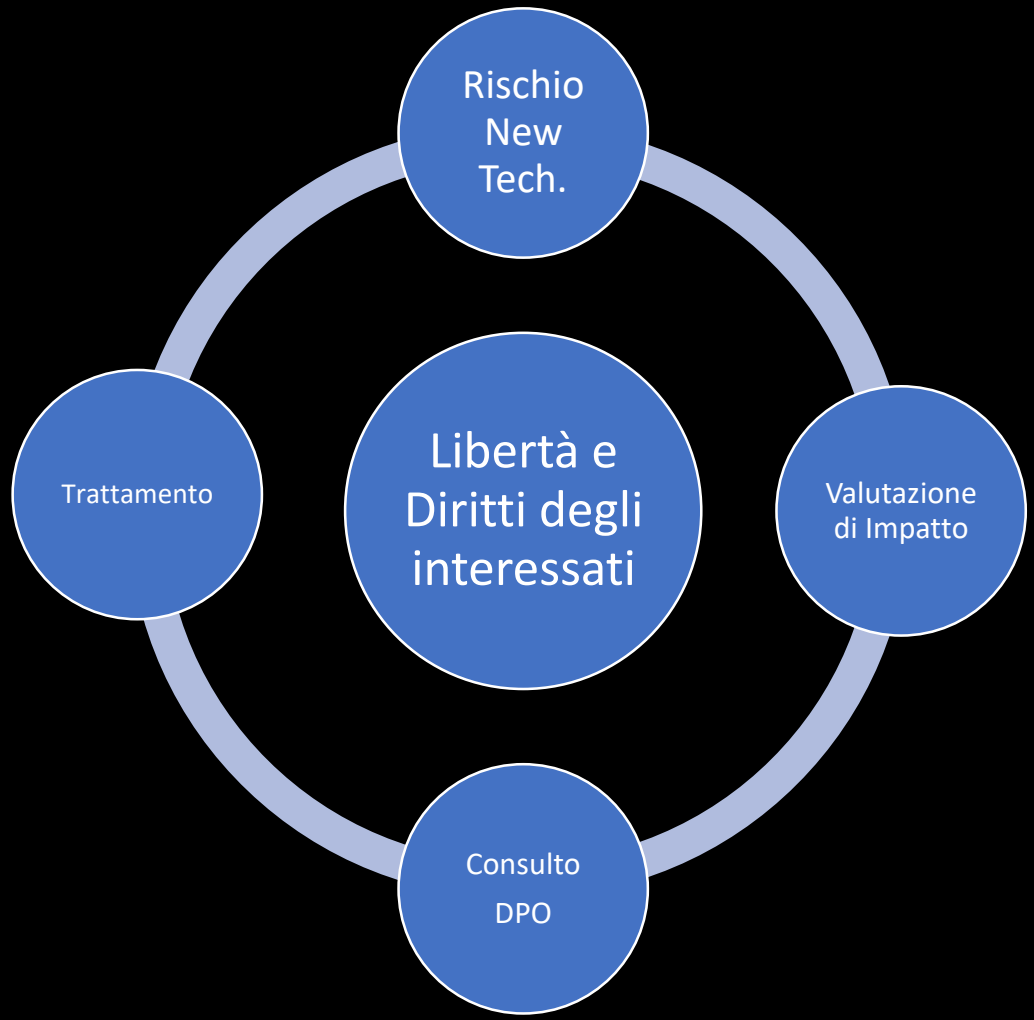
Protezione dei dati fin dalla progettazione

- «sia al **momento di determinare i mezzi del trattamento sia all'atto del trattamento** stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la **pseudonimizzazione** …»

Protezione per impostazione predefinita

- Default Setting
- Il Titolare adotta **misure tecniche/organizzative** per garantire che siano trattati, per **impostazione predefinita**, solo i dati personali **necessari** per ogni specifica finalità del trattamento.

Valutazione di impatto sulla protezione dei dati artt. 35 e 36



Valutazione di impatto sulla protezione dei dati art. 35

Quando:

- Valutazione sistematica aspetti personali **trattamento automatizzato «Profilazione»**
- Trattamento su larga scala **particolari dati** ex artt. 9 e 10
- **Sorveglianza** su larga scala zona accessibile al pubblico

Contenuto:

1. **Descrizione dei Trattamenti**/Finalità/Interesse legittimo del Titolare
2. **Valutazione della necessità** e proporzionalità dei trattamenti/**Finalità**

3. **Valutazione del Rischio Impatto**

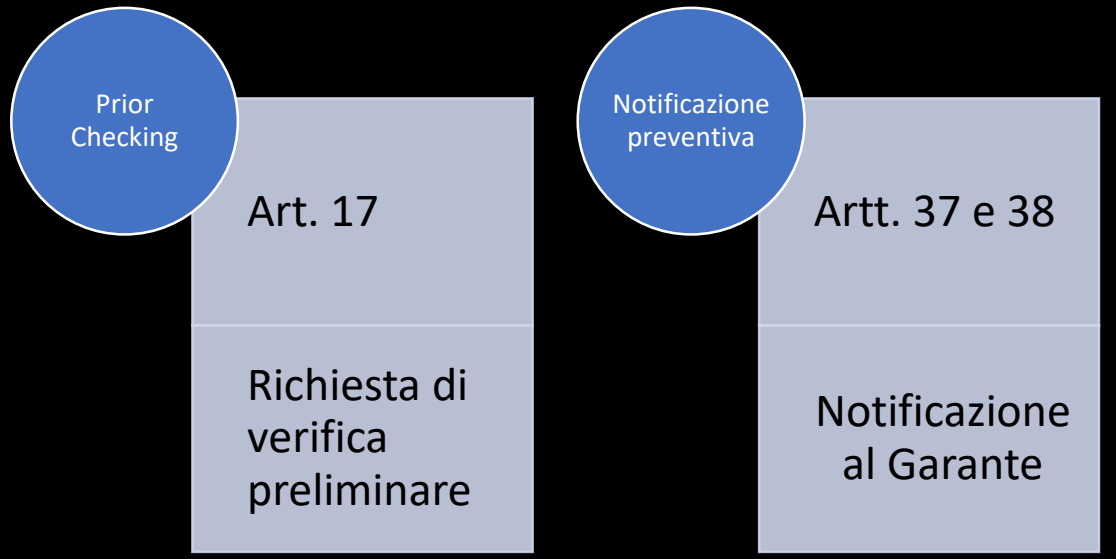
4. Comportamento Proattivo/Misure previste per affrontare i rischi:

- Garanzie per la libertà e dignità interessato
- Misure di Sicurezza per la protezione dei dati personali

Consultazione Preventiva art. 36

Regolamento Europeo

Codice Privacy



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

Il DPO sta al centro del sistema basato sull'Accountability

Facilita l'osservanza del Regolamento all'interno dell'azienda

Il WP29 incoraggia la designazione di DPO

Obbligo di nomina (art. 37 RGPD)

-Autorità Pubblica eccezione Autorità giurisdizionali

-Attività principale: monitoraggio regolare e sistematico su larga scala degli interessati

-Trattamento su larga scala di categorie particolari di dati o dati relativi a condanne penali (Artt. 9 e10)

- Attività principali: Trattamento di dati sanitari per gli ospedali

- Larga scala: numero di soggetti interessati dal trattamento/volume dati/durata/estensione

-monitoraggio: tracciamento/profilazione internet

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

Chi è: «*Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati*» (art. 37 c. 5)

Competenze:
1. conoscenza della normativa e prassi nazionale
2. Familiarità con le operazioni di trattamento svolte dall'azienda
3. Familiarità con tecnologie informatiche e misure di sicurezza dei dati
4. Conoscenza del settore di attività dell'azienda

Autonomia: Il DPO opera in maniera autonoma ma integrata con le funzioni aziendali, senza ricevere istruzioni dal Responsabile che lo informa in merito a tutte le decisioni a impatto privacy

Il DPO all'interno dell'azienda

Posizione

- va «*tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali*» (Art. 38).
- Va consultato nelle valutazioni di impatto sulla protezione dei dati (Art. 35)

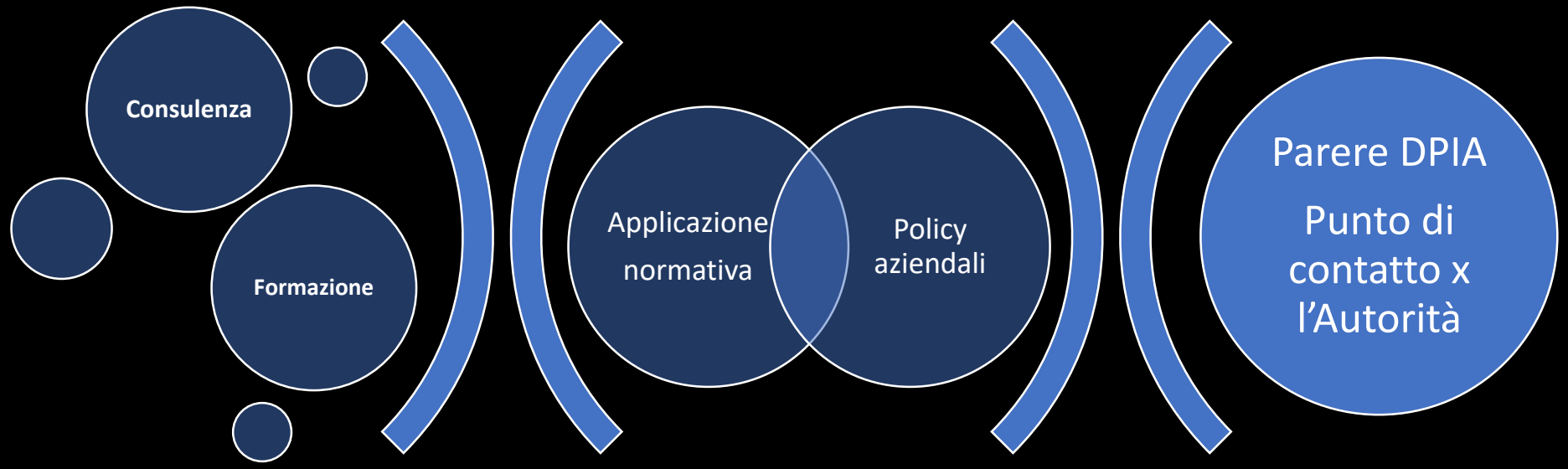
Ruolo

- Se informato e consultato adeguatamente il DPO garantirà l'attuazione dei principi privacy fin dalla fase di **Progettazione** del Sistema di Gestione Privacy
- Attuazione del Principio Privacy by design (Art. 25)

Attività

- Partecipazione regolare alle Riunioni del management (**Vertici Aziendali**)
- Intervento del DPO su decisioni che impattano sulla protezione dei dati personali
- Fornire **Pareri** in materia Privacy-Documentazione dell'esito negativo della consultazione

I compiti del DPO



Informare Sorvegliare Cooperare

Registro dei Trattamenti art. 30

Che cos'è

E' un registro delle attività di trattamento svolte dal Titolare del Trattamento

Strumento indispensabile di valutazione e analisi del rischio

Elemento fondamentale per la corretta mappatura dei processi e la conseguente indicazione delle procedure

Parte integrante del sistema di gestione dei dati

Strumento fondamentale per una corretta impostazione del rapporto con l'Autorità di controllo

Obbligatorio per imprese con non meno di 250 dipendenti

Il Garante ha invitato tutti i Titolari del Trattamento a dotarsi di un Registro Trattamenti a prescindere dalla dimensione dell'impresa

Il Modello Organizzativo in Azienda

MAPPATURA DEI PROCESSI

per comprendere come viene attuato il trattamento in azienda

GAP ANALYSIS

Per identificare eventuali falle nel Sistema di Gestione Privacy

CHECK LIST

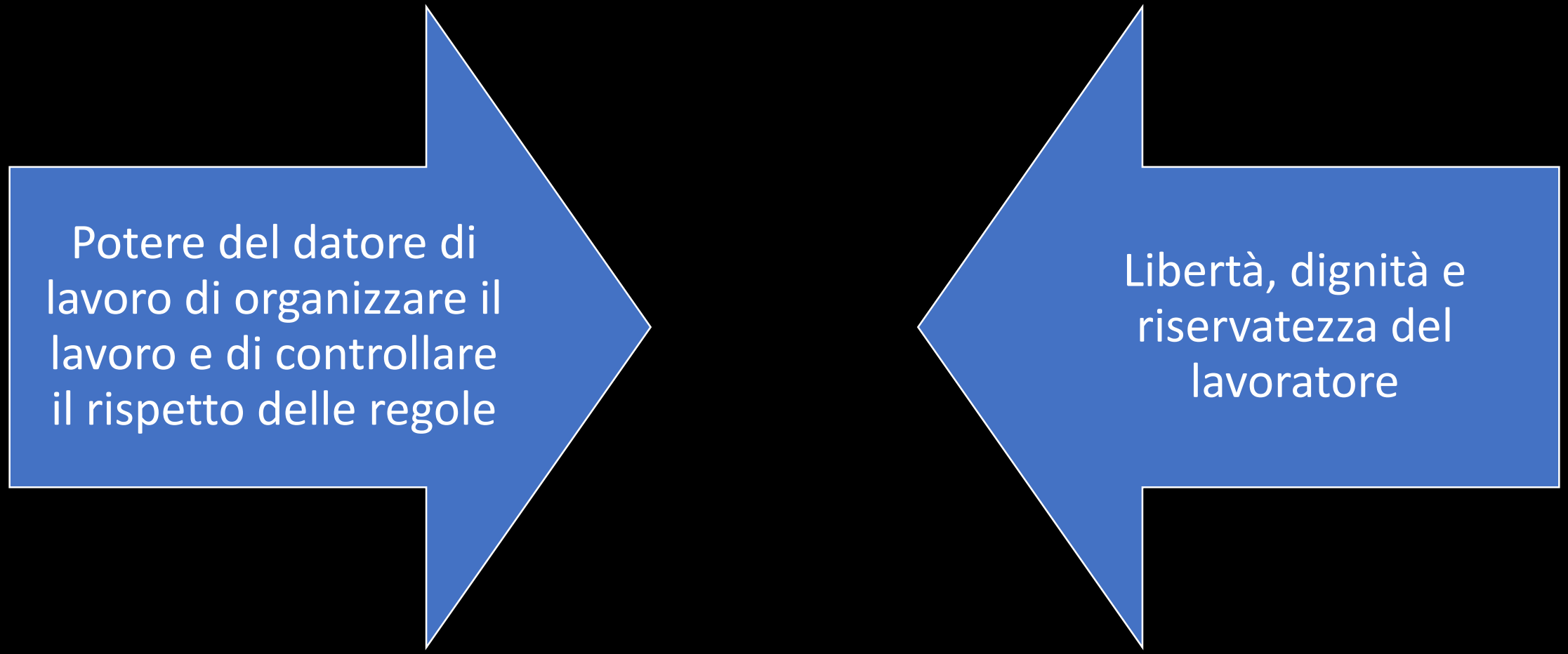
degli adempimenti da compiere

FEED BACK

Conformità ai criteri previsti nella Normativa Privacy

(Sanzioni artt. 83 e 84)

Il controllo sui lavoratori
Bilanciamento degli interessi in gioco



Il controllo del lavoratore integra un trattamento di dati

Statuto dei Lavoratori l. 300/70

guardie giurate (art.2)

personale di vigilanza (art.3)

impianti audiovisivi (art. 4)

accertamenti sanitari (art.5)

visite personali (art.6)

divieto di indagini sulle opinioni (art. 8)

Codice Privacy

principio di necessità (art. 3)
liceità/correttezza (art. 11)
informativa (art. 13)
consenso (art. 23)
garanzie per i **dati sensibili**, ovvero consenso scritto + autorizzazione del Garante, (art. 26)
garanzie per i **dati giudiziari**, ovvero espressa disp. di legge/aut. Garante (art. 27)
Artt. 113,114, 184 c.3

Il controllo: quando è lecito?

Il controllo sui lavoratori implica un trattamento di dati e dovrà avvenire in conformità ai **Principi** dettati in materia di protezione dei dati personali pena l'INUTILIZZABILITA' DEI DATI

Il Controllo a Distanza

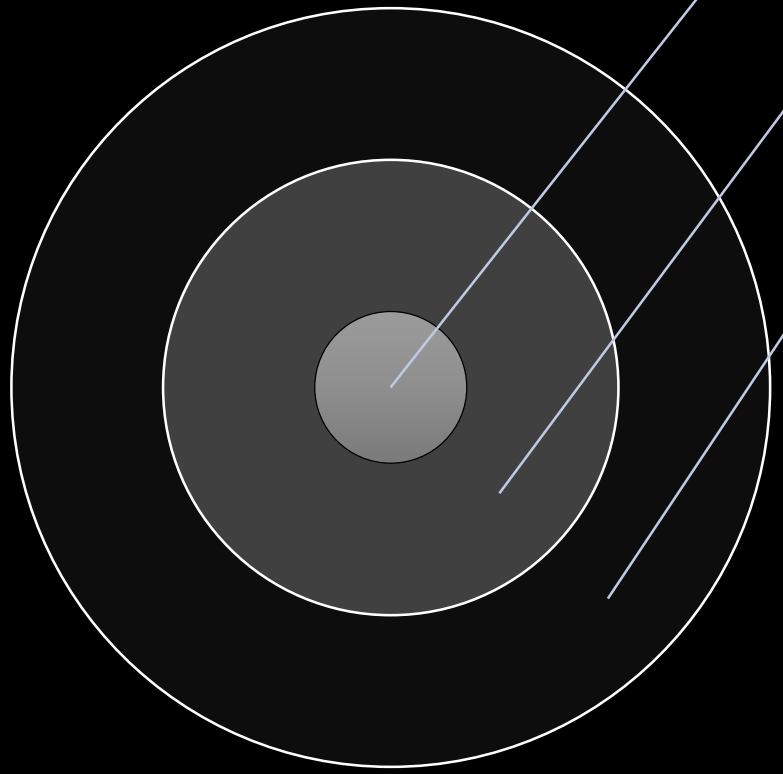
Art. 4 (Impianti audiovisivi e altri strumenti di controllo)

1. «Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di **controllo a distanza** dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive sicurezza del lavoro tutela del patrimonio aziendale» previo accordo collettivo RSU/RSA/ Aut. INL

2. «La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze».

Garante provv.to 13.07.2016 n. 303; Circolare INL n. 2 del 7.11.2016 uso GPS ex art.4 commi 1 e 2 St. Lav.

3. Obbligo di Informazione sulle modalità d'uso degli strumenti e sui controlli pena l'inutilizzabilità delle informazioni



Approfondimenti

Domande

Chiarimenti

maccaferro@studioguerrini.eu