



Città di Pescara
Medaglia d'oro al Merito Civile



SICUREZZA URBANA INTEGRATA

Formazione e consulenza al servizio della città

LE BUONE PRATICHE PER LA
VALORIZZAZIONE DI PERCORSI CONDIVISI

**VDS URBANA INTEGRATA E
CORRETTO TRATTAMENTO
DEI DATI PERSONALI**

Giovanna Panucci - Avvocato e Data Protection Officer

LA DIRETTIVA POLIZIA
ED IL RUOLO
ESSENZIALE DEL DATA
PROTECTION OFFICER

PRIVACY O PROTEZIONE DEI DATI PERSONALI?

Privacy → Termine ombrello che rimanda ad un grappolo di diritti fondamentali ed inviolabili che noi chiamiamo in maniera generica *privacy*. Nel grappolo ci sono diritti fondamentali differenti.

Protezione dei dati personali → specie
Privacy → genere

Da dove è partito tutto?

- 1890 Warren e Bràndeis ?
- Antico testamento - Genesi?

La nascita dei diritti privacy è **recente**, dal diciannovesimo in poi.

Sono diritti naturali o diritti positivi nuovi?

Si può essere insieme **giusnaturalisti** e **giuspositivisti** guardando la privacy e la sua evoluzione?



PRIVACY? O PROTEZIONE DEI DATI PERSONALI?

Direttiva 95 n. 46 → introduce a livello comunitario una normativa in materia di trattamento dati personali che sembra adottata per ragioni economiche, circolazione dati strumentale alle altre libertà di circolazione comunitarie.

Opportunismo economico VS Tutela dei diritti fondamentali inviolabili

Perché in Europa si intuisce una declinazione del right to privacy differente, che va verso la protezione dei dati personali, da tenere confidenziali, protetti, riservati?

PRIMA RIFLESSIONE: L'Europa nella prima metà del '900

SECONDA RIFLESSIONE: Siamo la culla dell'informatizzazione

Due enormi motivi per iniziare a ragionare di privacy come (ma non solo) protezione dei dati personali [**VISIONE EUROCENTRICA**]

Dobbiamo tenere a mente queste premesse per capire perché ci stiamo occupando di questa materia.



PROFILAZIONE

Che cosa vuol dire **profilazione** per il GDPR?

= elaborazione di dati automatizzata di dati personali

Quindi, tecnicamente, se usiamo strumenti non automatizzati non siamo nel perimetro della profilazione come fissato dal GDPR
Se elaboro dati pur con strumenti automatizzati ma non sono personali non sto facendo profilazione ai sensi del GDPR

Tuttavia i risultati di tali elaborazioni hanno una ricaduta sugli esseri umani.

Il perimetro definitorio del GDPR rischia di essere insufficiente rispetto ad elaborazione di dati come avviene con l'intelligenza artificiale, impattanti sulle libertà fondamentali degli individui ma non normati.

La profilazione del GDPR si compone di **due fasi**:

1. raccolta di dati con strumenti automatizzati +
2. analisi delle informazioni raccolte per produrre una valutazione ulteriore del soggetto.

Restano fuori parecchie cose.

Perché? Una **scelta di TUTELA**



SOLO ALCUNE DELLE FONTI DI RIFERIMENTO

Art. 2 costituzione italiana

Art. 12 Dichiarazione universale dei diritti umani

Convenzione 108

Carta dei diritti fondamentali dell'UE, artt. 7 (tutela della vita privata e delle comunicazioni) e 8 (dedicato più alla protezione dati personali)

Art. 16 Trattato sul funzionamento dell'UE

GDPR (entrato in vigore il 24 maggio 2016, applicato completamente dal 25 maggio 2018).

Direttiva Polizia 680/2018

Codice privacy, all'interno del quale c'è il recepimento di molte direttive. Con il GDPR il codice ha subito una pesante mutilazione ma continua ad essere il nostro testo italiano di riferimento da leggersi in combinato col resto.

Direttiva 2002/58 CE cd. e-Privacy, tutt'ora in vigore. Presentato 4 anni fa un testo di regolamento e-Privacy, che se approvato andrà a sostituire la direttiva

D. lgs 101 del 2018, in vigore dal 19.09.2018, introduce pesanti modifiche al Codice Privacy per adeguarlo al GDPR. Modifiche fatte con superficialità.

Tutte le prescrizioni generali ed astratte che provengono dal Garante e dallo EDPB.

Standard e linee guida: es. ENISA, ISO/IEC 27001,27701:2019 e 29134



LA DIRETTIVA POLIZIA ED IL RUOLO ESSENZIALE DEL DPO

Senza contare che la Commissione Europea negli ultimi mesi ha prodotto dei testi spiazzanti:

- **Data Governance Act**
- **Digital Market Act**
- **Digital Services Act**
- **Regolamento sull'IA**



LA DIRETTIVA POLIZIA ED IL RUOLO ESSENZIALE DEL DPO

Abbiamo capito che la privacy c'entra con le problematiche di convergenza.

Se fossimo in possesso di strumenti che sfruttano l'intelligenza artificiale, se fossimo in possesso di telecamere capaci di leggere sui volti l'intenzionalità del crimine, non vorremmo fare accordi che tutelano i dati oggetto di trattamento?

Questi **Accordi** hanno ad oggetto la convergenza di problematiche giuridiche impressionanti.

- Una struttura sanitaria potrebbe dire, oltre alla privacy c'è un problema di intellectual property o di proprietà industriali.
- Un comando di polizia locale potrebbe dire che oltre alla privacy c'è un problema di tutela della sicurezza urbana

...e così via.



Bisogna aver paura di un DPO
che non si pone il dubbio della
convergenza delle regolazioni

La privacy, oggi, è una
questione di convergenza

QUINDI IL RUOLO ESSENZIALE DEL DPO...

- E' un ruolo di mera conformità o di consulenza?
- E' un DPO cane da guardia o DPO stratega?



LA DIRETTIVA POLIZIA ED IL RUOLO ESSENZIALE DEL DPO

→ Documento di indirizzo su designazione, posizione e compiti del Responsabile della protezione dei dati (RPD) in ambito pubblico del 29 aprile 2021

→ DPO come FACILITATORE



2. Una considerazione preliminare: il RPD quale "punto di contatto" per l'Autorità

L'art. 39, par. 1, lett. d) ed e), del Regolamento prevede che il RPD, tra i suoi compiti, cooperi con l'Autorità e funga da punto di contatto per questioni connesse ai trattamenti. Come indicato nelle **Linee guida del WP29**, in questo modo il **RPD svolge un ruolo di "facilitatore"**, in quanto facilita l'accesso, da parte dell'Autorità, ai documenti e alle informazioni necessarie "per l'adempimento dei compiti attribuiti dall'articolo 57 nonché ai fini dell'esercizio dei poteri di indagine, correttivi, autorizzativi e consultivi di cui all'articolo 58" (par. 4.3, pp. 23-24).



A PROPOSITO DI
CONVERGENZA...

DIRETTIVA POLIZIA E GDPR

PRINCIPI GENERALI GDPR (ma non solo)

Articolo 5

"Principi applicabili al trattamento di dati personali»

I dati personali sono:

- a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
 - b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
 - c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
 - d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
 - e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
 - f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).
- Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di **comprovarlo** («responsabilizzazione»).



I PRINCIPI GENERALI NEI PROCESSI PIU' AVANZATI

L' Applicazione dei principi generali sta diventando sempre più difficile

Esempi

- *Machine Learning*: come spiegare l'algoritmo che tratta dati personali? Trasparenza e correttezza garantite?
- *Big data processing*: come minimizzare i dati se elementi stessi del big data solo volume e velocità di elaborazione? Come gestire l'accountability?

Questioni che prima o poi dovremo affrontare



IL «PACCHETTO DELL'UNIONE EUROPEA»

Regolamento UE 2016/679 → d. lgs n. 101 del 2018

- Per rispondere alle sfide lanciate dalle **nuove tecnologie** e dai **servizi** annessi;
- Necessario **un livello forte ed elevato di protezione dei dati** come *conditio sine qua non* per creare un clima di **fiducia** nell'ambiente online, fattore chiave dello sviluppo economico;
- Un regolamento **Generale**. Si applica in tutta l'UE ma nel regolamento stesso è previsto un margine di manovra per i singoli stati membri per determinate materie e ambiti di trattamento dei dati personali. Es. Art. 6 paragrafo 3 (Liceità del trattamento) ci dice che gli stati membri hanno margine di manovra per dire la loro (base giuridica la legge statale) quando si tratta di *trattamenti di dati svolti per adempimento di obblighi legali, di interesse pubblico o connessi all'esercizio di pubblici poteri.*



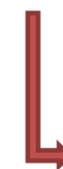
IL PACCHETTO DELL'UNIONE EUROPEA

Regolamento UE 2016/679

Art. 2

Ambito di applicazione MATERIALE

1. Il presente regolamento si **applica** al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.
2. Il presente regolamento **non si applica** ai trattamenti di dati personali:
 - a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;
 - b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE;
 - c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;
 - d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.



Considerando 19 del GDPR



IL PACCHETTO DELL'UNIONE EUROPEA

Regolamento UE 2016/679

Considerando 19

- (19) La protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro, e la prevenzione di, minacce alla sicurezza pubblica, e la libera circolazione di tali dati **sono oggetto di uno specifico atto dell'Unione**. Il presente regolamento non dovrebbe pertanto applicarsi ai trattamenti effettuati per tali finalità. **I dati personali trattati dalle autorità pubbliche** in forza del presente regolamento, **quando utilizzati per tali finalità, dovrebbero invece essere disciplinati da un più specifico atto dell'Unione**, segnatamente **la direttiva (UE) 2016/680** del Parlamento europeo e del Consiglio ⁽¹⁾. Gli Stati membri possono conferire alle autorità competenti ai sensi della direttiva (UE) 2016/680 altri compiti che non siano necessariamente svolti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro, e la prevenzione di, minacce alla sicurezza pubblica, affinché il trattamento di dati personali per tali altre finalità, nella misura in cui ricada nell'ambito di applicazione del diritto dell'Unione, rientri nell'ambito di applicazione del presente regolamento.

Il mondo del **law and enforcement** applica un'altra disciplina, la **Direttiva 680/2018**, negli stati che l'hanno recepita con **d.lgs 51/2018**.



IL PACCHETTO DELL'UNIONE EUROPEA

Direttiva 680/2018 → d. lgs n. 51 del 2018

- Trattasi di direttiva, quindi **non è di diretta applicazione** (non esplica un “effetto diretto”) necessitando di un recepimento nel diritto interno.
- Ha **ampliato** il concetto di c.d. **dato personale di reato**. Anche i fatti umani costituenti o valutabili come reato possono rappresentare delicati dati personali riferibili a persone fisiche e, quindi, essere una parte significativa di quel diritto fondamentale di protezione dell'uomo previsto dall'art.8 della Carta dei Diritti Fondamentale dell'Unione Europea. Fino al 2016 si poteva ancora sostenere (non sempre a ragione) che il dato personale afferente ai reati era esclusivamente quello c.d. “giudiziario” e l'ambito di trattamento era solo quello riservato alle forze dell'ordine per l'attuazione delle finalità (dirette o indirette) di polizia.
- Ha **esteso il novero dei soggetti** tenuti, individualmente e/o con le forze dell'ordine istituzionali, all'applicazione delle disposizioni interne di recepimento



CASI BORDERLINE: SPUNTI DI RIFLESSIONE

Difficoltà → capire non solo **quando ci si trovi ad avere a che fare con un c.d. “dato di reato”** ma anche **quale normativa (primaria e secondaria) applicare esattamente al corretto trattamento di tale tipologia di dati**

Art. 10 GDPR → chiaro sul “quando e come” si possono trattare i dati personali di reato al di fuori dell’ambito di applicazione del DLgs.51/2018, ossia sotto controllo dell’autorità pubblica o perché esiste una norma che ci autorizza.

Casistica:

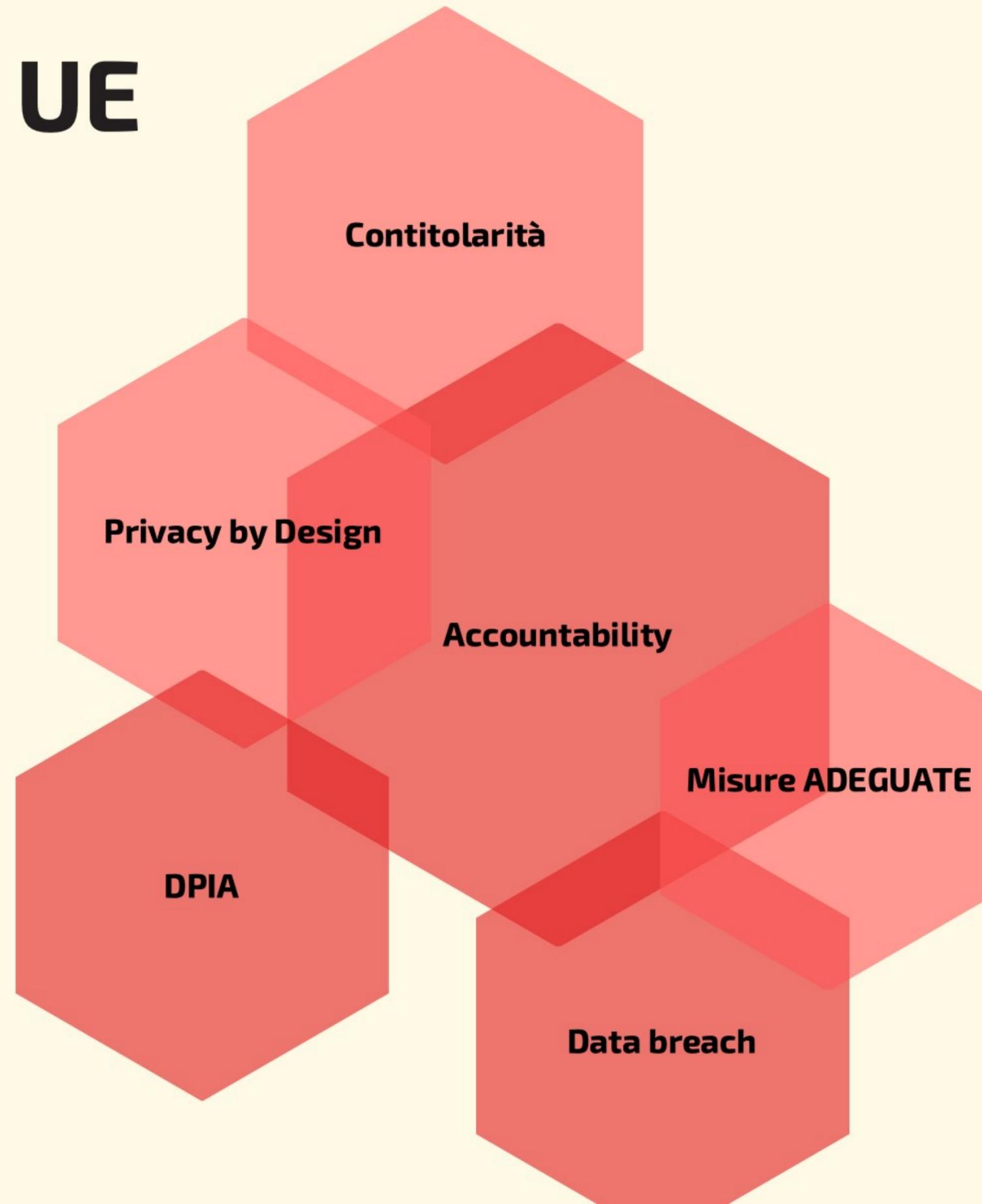
- Un privato denuncia alle forze dell’ordine l’autore riconoscibile di una aggressione → **FATTO**
- Un soggetto comunica la targa di un autoveicolo alle forze dell’ordine in quanto si ha il **mero sospetto** che appartenga ad un soggetto che si ritiene possa commettere un furto, ovvero perché **pensa** che un individuo identificabile abbia già commesso un atto criminoso utilizzando quel veicolo → **VALUTAZIONE SOGGETTIVA**

Capiamo quanto il confine sia sottile.



Regolamento UE 2016/679

Il **Regolamento UE 2016/679** ridisegna, la normativa nazionale in materia di privacy, fino a qualche anno fa costituita principalmente dal D. Lgs 196/2003. Il Regolamento, nei suoi 99 articoli, fornisce numerose conferme dei principi già esistenti della disciplina nazionale, ma non manca di introdurre **novità** di cui si deve tener presente nel trattamento dei dati personali



Direttiva UE 2016/680

La Direttiva UE 2016/6780, attuata in Italia dal D. Lgs n. 51 del 2018, disciplina i dati personali trattati dalle amministrazioni pubbliche ai fini di prevenzione, accertamento e perseguimento dei reati, ovvero i dati trattati a fini giudiziari e di polizia. La Direttiva è strutturata in maniera speculare al Regolamento. Si compone di 50 articoli suddivisi in 8 capi.



DIRETTIVA POLIZIA: AMBITO OGGETTIVO

Articolo 1

Oggetto e obiettivi

1. La presente direttiva stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle **autorità competenti** a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica.

[...]

Articolo 2

Ambito di applicazione

1. La presente direttiva si applica al trattamento dei dati personali **da parte delle autorità competenti** per le finalità di cui all'articolo 1, paragrafo 1.
2. La presente direttiva si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.
3. La presente direttiva **non si applica** ai trattamenti di dati personali:
 - a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;
 - b) effettuati da istituzioni, organi, uffici e agenzie dell'Unione.

Linee di confine fra i trattamenti svolti ai sensi del GDPR e quelli svolti ai sensi della Direttiva
(Considerando 12 della DIRETTIVA)



IL PACCHETTO DELL'UNIONE EUROPEA

Direttiva 680/2018

Considerando 12

(12) Le attività svolte **dalla polizia** o **da altre autorità** preposte all'applicazione della legge vertono principalmente sulla prevenzione, l'indagine, l'accertamento o il perseguimento di reati, comprese le attività di polizia condotte senza previa conoscenza della rilevanza penale di un fatto. Tali attività possono comprendere anche l'esercizio di poteri mediante l'adozione di misure coercitive quali le attività di polizia in occasione di manifestazioni, grandi eventi sportivi e sommosse. Esse comprendono anche il mantenimento dell'ordine pubblico quale compito conferito alla polizia o ad altre autorità incaricate dell'applicazione della legge ove necessario per la salvaguardia contro e la

⁽¹⁾ Decisione quadro 2008/977/GAI del Consiglio, del 27 novembre 2008, sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale (GUL 350 del 30.12.2008, pag. 60).

⁽²⁾ Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (cfr. pagina 1 della presente Gazzetta ufficiale).

4.5.2016

IT

Gazzetta ufficiale dell'Unione europea

L 119/91

prevenzione di minacce alla sicurezza pubblica e agli interessi fondamentali della società tutelati dalla legge che possono dar luogo a reati. **Gli Stati membri possono conferire alle autorità competenti altri compiti** che non siano necessariamente svolti a fini di prevenzione, indagine, accertamento o perseguimento di reati, **includere** la salvaguardia contro e la **prevenzione di minacce alla sicurezza pubblica, cosicché il trattamento di dati personali per tali altre finalità, nella misura in cui ricada nell'ambito di applicazione del diritto dell'Unione, rientra nell'ambito di applicazione del regolamento (UE) 2016/679.**



I DPO che operano presso le autorità competenti dovranno assistere nel compiere le scelte necessarie così da garantire in ogni caso il livello adeguato di protezione.

DIRETTIVA POLIZIA: AMBITO SOGGETTIVO

Chi sono le «autorità competenti»?

Articolo 3

Definizioni

[....]

7) «*autorità competente*»:

- a) *qualsiasi autorità pubblica competente in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica; o*
- b) *qualsiasi altro organismo o entità incaricati dal diritto dello Stato membro di esercitare l'autorità pubblica e i poteri pubblici a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica.*

→ In precedenza la disciplina del trattamento in ambito di polizia era affidata alla parte II, Titolo II del Codice Privacy (art. 53). Oggi l'art. 49 del d.lgs 51/2018 ha abrogato gli articoli da 53 a 57 (quest'ultimo a distanza di 1 anno dall'entrata in vigore del d.lgs 51)

↓
Art. 1.

Oggetto e ambito di applicazione

1. Il presente decreto **attua nell'ordinamento interno le disposizioni della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali,** nonché alla libera circolazione di tali dati, e che abroga la decisione quadro 2008/977/GAI del Consiglio.



ANCHE LA POLIZIA LOCALE RIENTRA TRA QUESTE?

Assolutamente si!

La definizione contenuta del **decreto** e relativa a «autorità competenti» ricalca quella contenuta nella **Direttiva 680** che abbiamo visto in precedenza.

g) **autorità competente:**

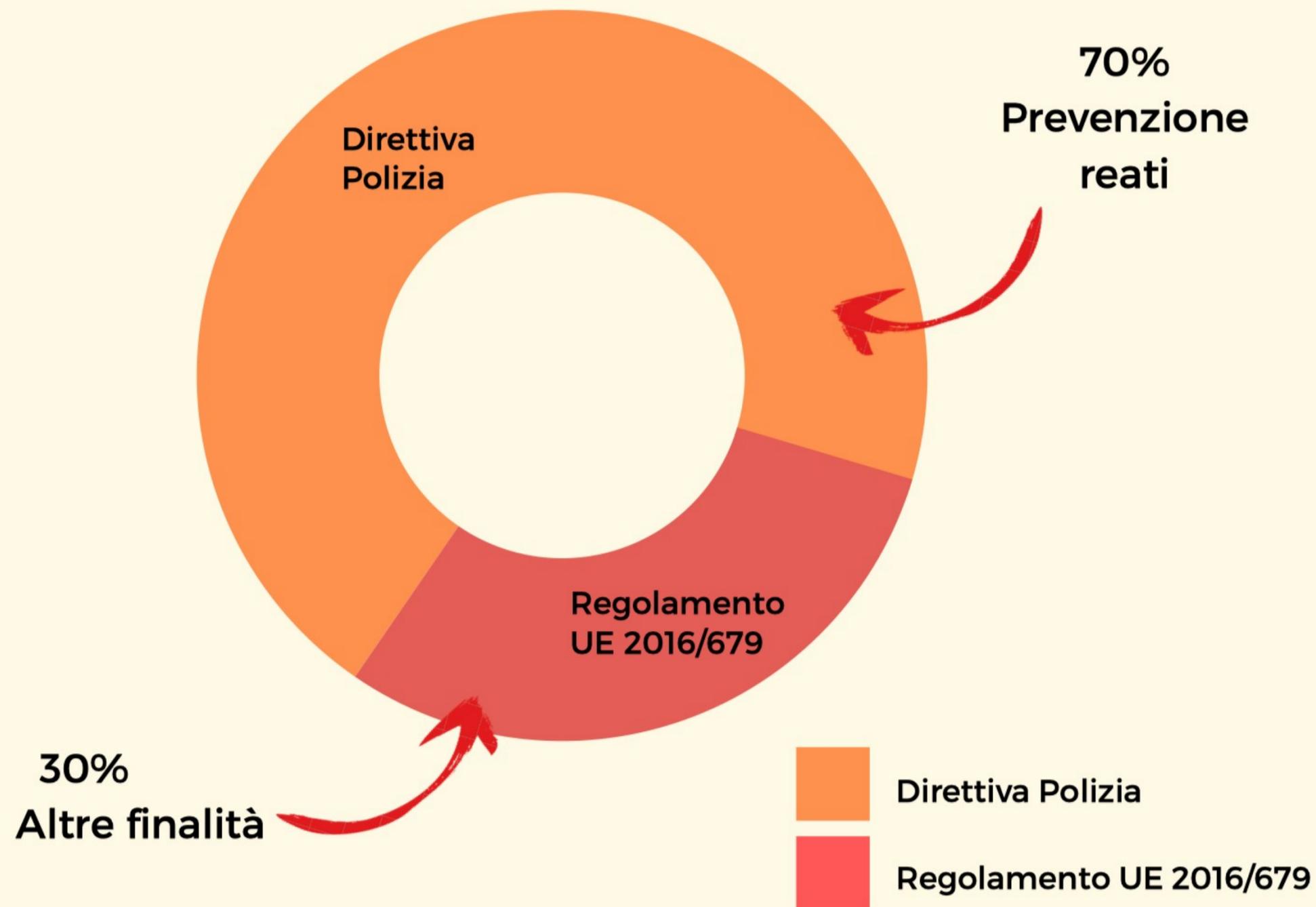
1) **qualsiasi autorità pubblica dello Stato**, di uno Stato membro dell'Unione europea o di uno Stato terzo **competente in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica;**

2) **qualsiasi altro organismo o entità incaricato dagli ordinamenti interni di esercitare l'autorità pubblica e i poteri pubblici a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica;**

- Le amministrazioni locali devono adeguare le proprie procedure di protezione e trattamento dei dati, non solo in funzione del GDPR ma anche in ordine alla disciplina specifica in materia di applicazione delle sanzioni penali, che interessa in modo peculiare i comandi di polizia locale.
- Tenere in considerazione la specificità della titolarità del trattamento che in virtù della specificità delle informazioni gestite ed elaborate non dovrà essere confusa con quella relativa agli altri dati trattati dall'ente
- Esempio tipico i trattamenti effettuati mediante impianti videosorveglianza dotati di sistemi evoluti di analisi video

LE FINALITA' IMPIANTO VDS

PER CAPIRNE LA VESTE GIURIDICA



DIRETTIVA POLIZIA: PRINCIPALI DISPOSIZIONI

In generale troviamo disposizioni simili a quelle del RGPD con alcuni distinguo che riflettono il particolare contesto delle attività di contrasto e di prevenzione delle minacce penali alla sicurezza pubblica.

Le **definizioni dei concetti fondamentali** di cui all'Art. 3 (“dato personale”, “trattamento”, “limitazione del trattamento”, “profilazione”, “pseudonimizzazione”, “archivio”, “titolare”, “responsabile”, “destinatario”, “violazione di dati personali”, “dati genetici”, “dati biometrici”, “dati relativi alla salute”) sono identiche a quelle contenute nel RGPD.

Anche i **principi fondamentali**, fissati all'Articolo 4, sono simili.

Il **principio di “liceità”** (assente nella Decisione-quadro del 2008, adesso è citato espressamente).

Il **principio di “trasparenza”** (connesso al **principio di liceità e correttezza** nel RGPD) è espresso, ad esempio, nel paragrafo 2 dell'Art. 8 (“Il diritto dello Stato membro che disciplina il trattamento nell'ambito di applicazione della presente direttiva specifica quanto meno gli obiettivi del trattamento, i dati personali da trattare e le finalità del trattamento”) e nelle disposizioni sulle informazioni da fornire agli interessati e sull'accesso da parte di questi ultimi ai dati che li riguardano.

Il **principio di finalità è soggetto a limitazioni**, nel senso che i dati personali raccolti da qualsivoglia delle autorità competenti di cui sopra per finalità di applicazione della legge o di sicurezza pubblica possono essere utilizzati per altri scopi, a condizione che tale utilizzo sia “autorizzato dal diritto dell'Unione o dello Stato membro” (Art. 9, paragrafo 1, primo periodo), e salvo quanto previsto dal secondo periodo di tale paragrafo, ossia che qualora i dati personali siano trattati per tali finalità diverse, si applica il regolamento (UE) 2016/679.



DIRETTIVA POLIZIA: PRINCIPALI DISPOSIZIONI

La direttiva impone agli Stati membri di prevedere termini per la **conservazione** dei dati trattati in base alle sue disposizioni (Art. 5);

La direttiva impone ai titolari l'adozione di **misure di sicurezza in linea con lo "stato dell'arte"**, tenendo conto del contesto, degli scopi, ecc. del trattamento (Art. 29, paragrafo 1);

I titolari devono condurre una **valutazione del rischio**, per stabilire quale sia il livello adeguato di sicurezza (Art. 29, paragrafo 2);

Sussiste poi **l'obbligo di notificare all'autorità di controllo le violazioni di dati personali**, entro 72 h;

Le norme della direttiva concernenti il trattamento di **dati sensibili** (ossia, dei dati che rivelano l'origine razziale o etnica, le opinioni politiche, le credenze filosofiche o religiose, o l'appartenenza sindacale", dei dati genetici, dei dati biometrici, dei dati relativi alla salute" dei dati "relativi alla vita sessuale o all'orientamento sessuale di una persona fisica) **sono strutturate in modo parzialmente diverso** rispetto al RGPD (Art. 9). La direttiva consente il trattamento dei dati in questione:

Articolo 10

Trattamento di **categorie particolari di dati personali**

Il trattamento di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, e il trattamento di dati genetici, di dati biometrici intesi a identificare in modo univoco una persona fisica o di dati relativi alla salute o di dati relativi alla vita sessuale della persona fisica o all'orientamento sessuale **è autorizzato solo se strettamente necessario**, soggetto a **garanzie adeguate** per i diritti e le libertà dell'interessato **e** soltanto:

- a) **se autorizzato** dal diritto dell'Unione o dello Stato membro;
- b) **per salvaguardare un interesse vitale** dell'interessato o di un'altra persona fisica; o
- c) se il suddetto trattamento riguarda **dati resi manifestamente pubblici dall'interessato.**



DIRETTIVA POLIZIA: PRINCIPALI DISPOSIZIONI

«**Principio di responsabilizzazione**» → mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato ai sensi della presente direttiva. (Art. 19, paragrafo 1) + **“tali misure sono riesaminate e aggiornate qualora necessario”**;

Obblighi di tenuta di un **registro dei trattamenti** per assicurare la verificabilità della liceità dei trattamenti stessi;

“**Contitolarità**” del trattamento (Art. 21, paragrafo 2) e il ricorso a **responsabili del trattamento** (Art. 22).

DPIA → l’obbligo di condurre una valutazione d’impatto della protezione dei dati quando un tipo di trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche (Art. 27)

DPO → la direttiva prevede la designazione di un responsabile della protezione dei dati (DPO, Data Protection Officer) da parte di ogni titolare (Art. 32), ne illustra le caratteristiche soggettive (Art. 33) e ne elenca i compiti (Art. 34).

Il modello è il GDPR, il quale prevede la designazione di un DPO da parte di tutti i soggetti pubblici cui esso è applicabile, tuttavia, **la DIRETTIVA POLIZIA non richiede espressamente che il DPO sia in grado di agire in modo indipendente..**

DUBBIO: nomina del DPO ai sensi del GDPR o della direttiva? Cavillo giuridico



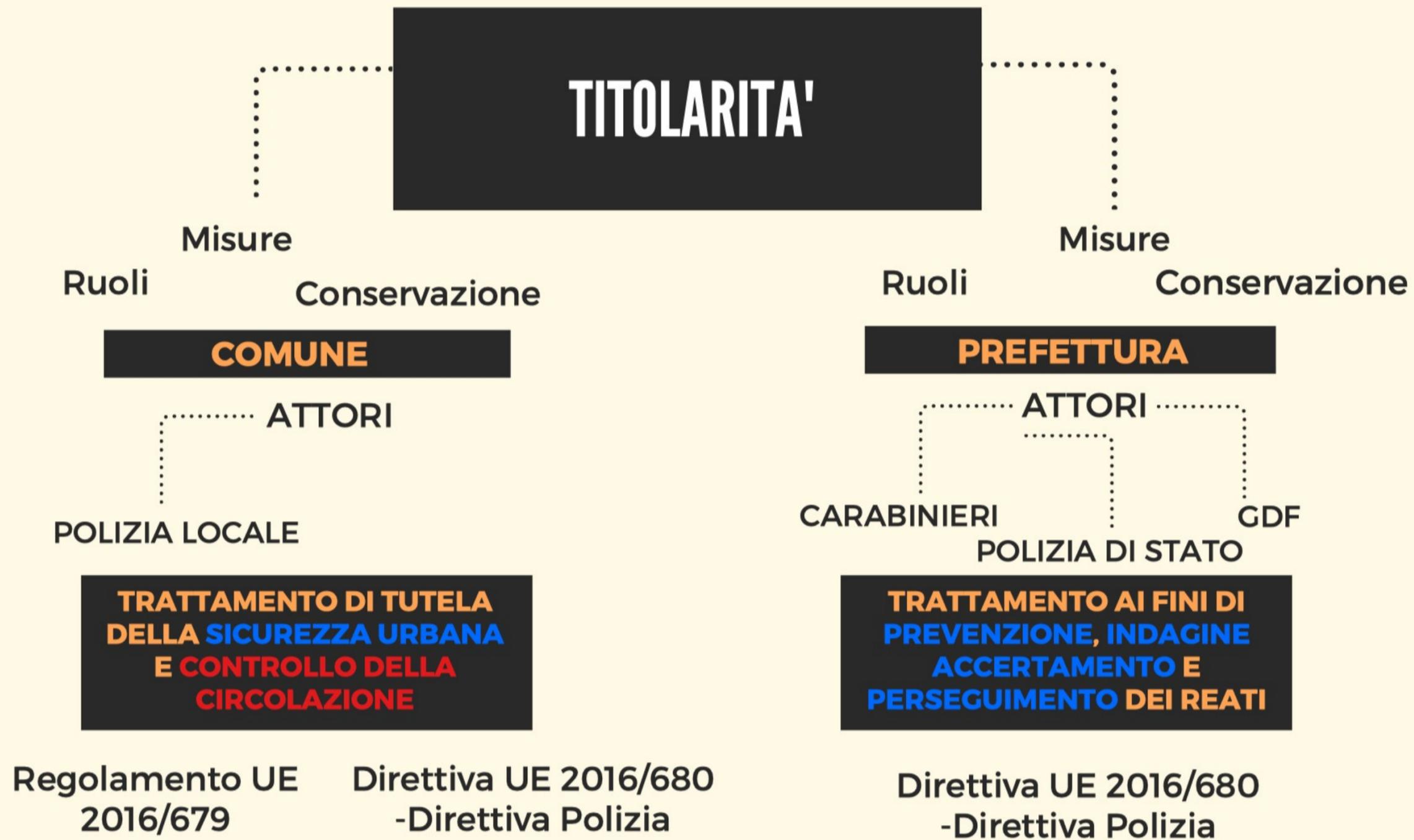
I DPO che operano presso le autorità competenti dovranno garantire l'osservanza del principio di responsabilizzazione e la revisione permanente delle misure adottate a tale scopo, nonché nella redazione degli "accordi" con *eventuali* contitolari di trattamento e dei contratti da stipulare con i responsabili di trattamento, nelle attività di consultazione della competente autorità di controllo, e nella conduzione di valutazioni di impatto ai sensi della
Direttiva

ARCHITETTURA DI UN MODERNO PROGETTO DI SICUREZZA URBANA INTEGRATA

ATTIVITA' DA TRAGUARDARE

Le amministrazioni locali nel brevissimo periodo dovranno adeguare le proprie procedure di trattamento e protezione dei dati, non solo in funzione del nuovo regolamento europeo, ma anche e soprattutto in ordine alla disciplina specifica in materia di applicazione delle sanzioni penali che interessa in modo peculiare i Comandi di Polizia Locale.





**AMBITO DI CONTITOLARITA'
CONDIVISIONE DI FINALITA' DEL
TRATTAMENTO**

Si dovrà tenere conto della specificità della titolarità del trattamento che, proprio per la particolarità delle informazioni gestite, non dovrà essere confusa con quella relativa agli altri dati trattati dall'ente.

GRAZIE PER L'ATTENZIONE

www.sicurezzaurbanaintegrata.it

Avvocato Giovanna Panucci



Rimani in collegamento con noi!



SITO WEB

Il portale dedicato alla sicurezza urbana integrata

sicurezzaurbanaintegrata.it



POLIZIA

MUNICIPALE.IT

Il portale di riferimento della polizia locale

poliziamunicipale.it



CANALE TELEGRAM

Videosorveglianza & Privacy



SICUREZZA URBANA INTEGRATA

Formazione e consulenza al servizio della città

LE BUONE PRATICHE PER LA
VALORIZZAZIONE DI PERCORSI CONDIVISI
**VDS URBANA INTEGRATA E
CORRETTO TRATTAMENTO DEI
DATI PERSONALI**

Grazie per l'attenzione

Giovanna Panucci - Avvocato e Data Protection Officer