

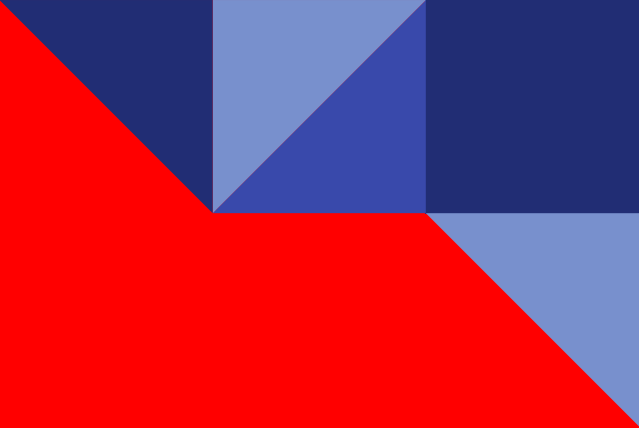
La protezione dei dati della P.A. nel GDPR



Relatore: **Simone Chiarelli**
simone.chiarelli@gmail.com
Cell. +39 3337663638

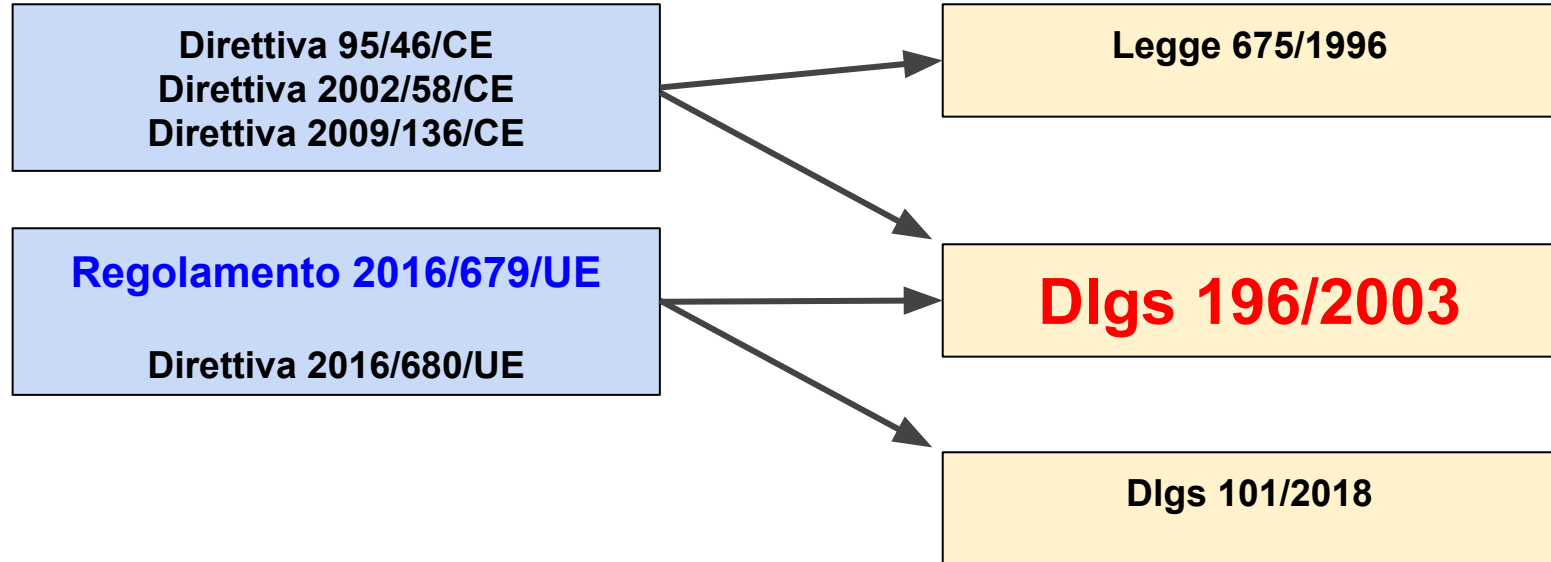


**Scuola di amministrazione
del Comune di Genova**

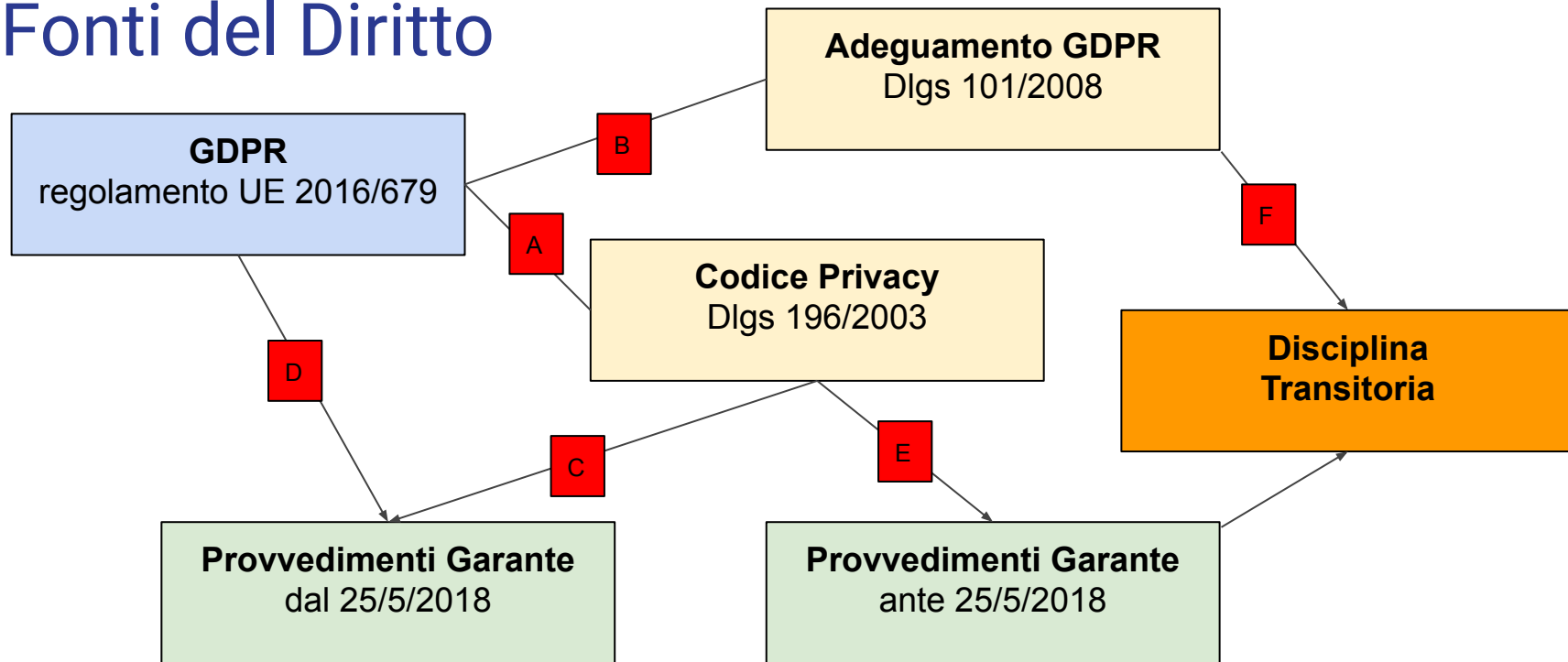


CONTESTO e DEFINIZIONI

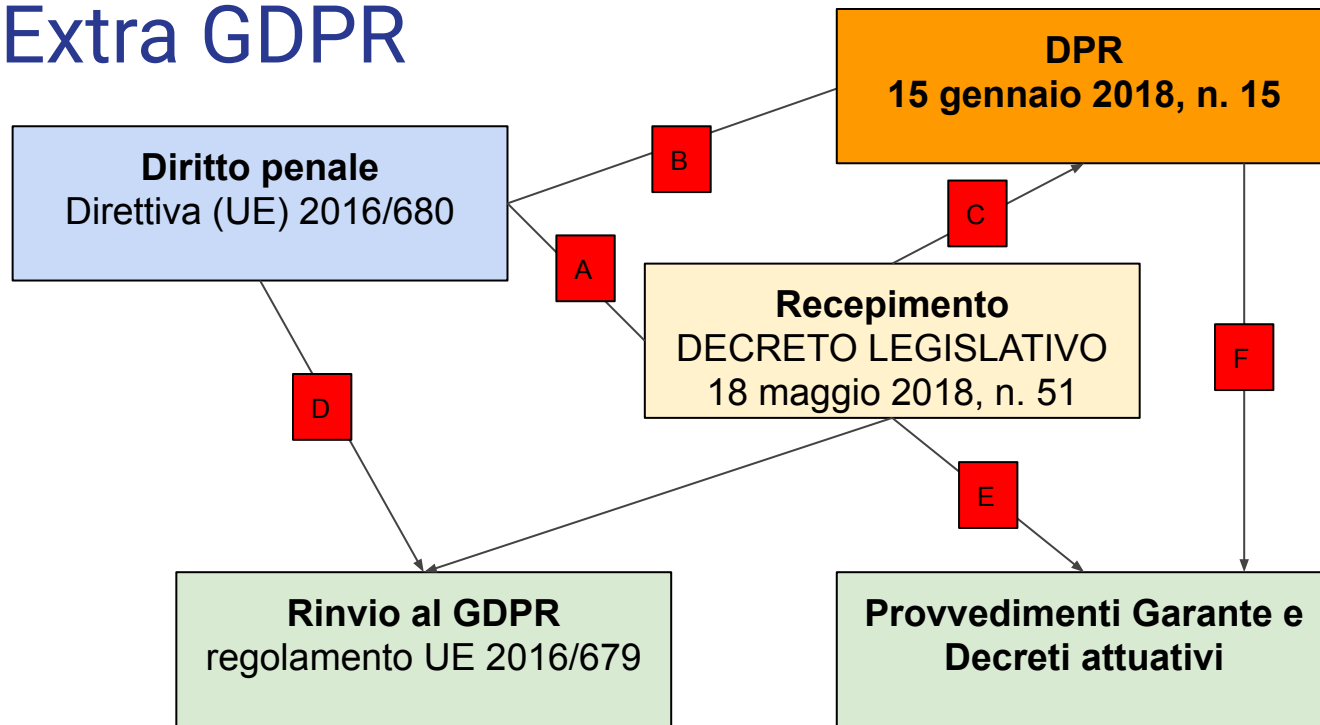
STORIA



Fonti del Diritto



Extra GDPR



Regolamento (UE) 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 (regolamento generale sulla protezione dei dati)

Art. 4 GDPR

«**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («**interessato**»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

Art. 4 GDPR

«**trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

Art. 4 GDPR

«**profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

Art. 4 GDPR

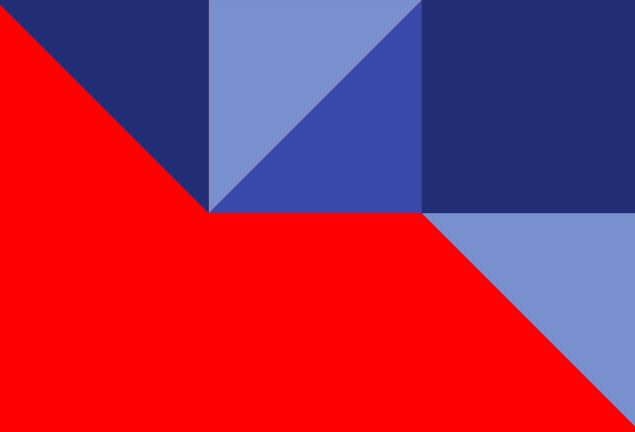
«**pseudonimizzazione**»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

Art. 4 GDPR [ex sensibili]

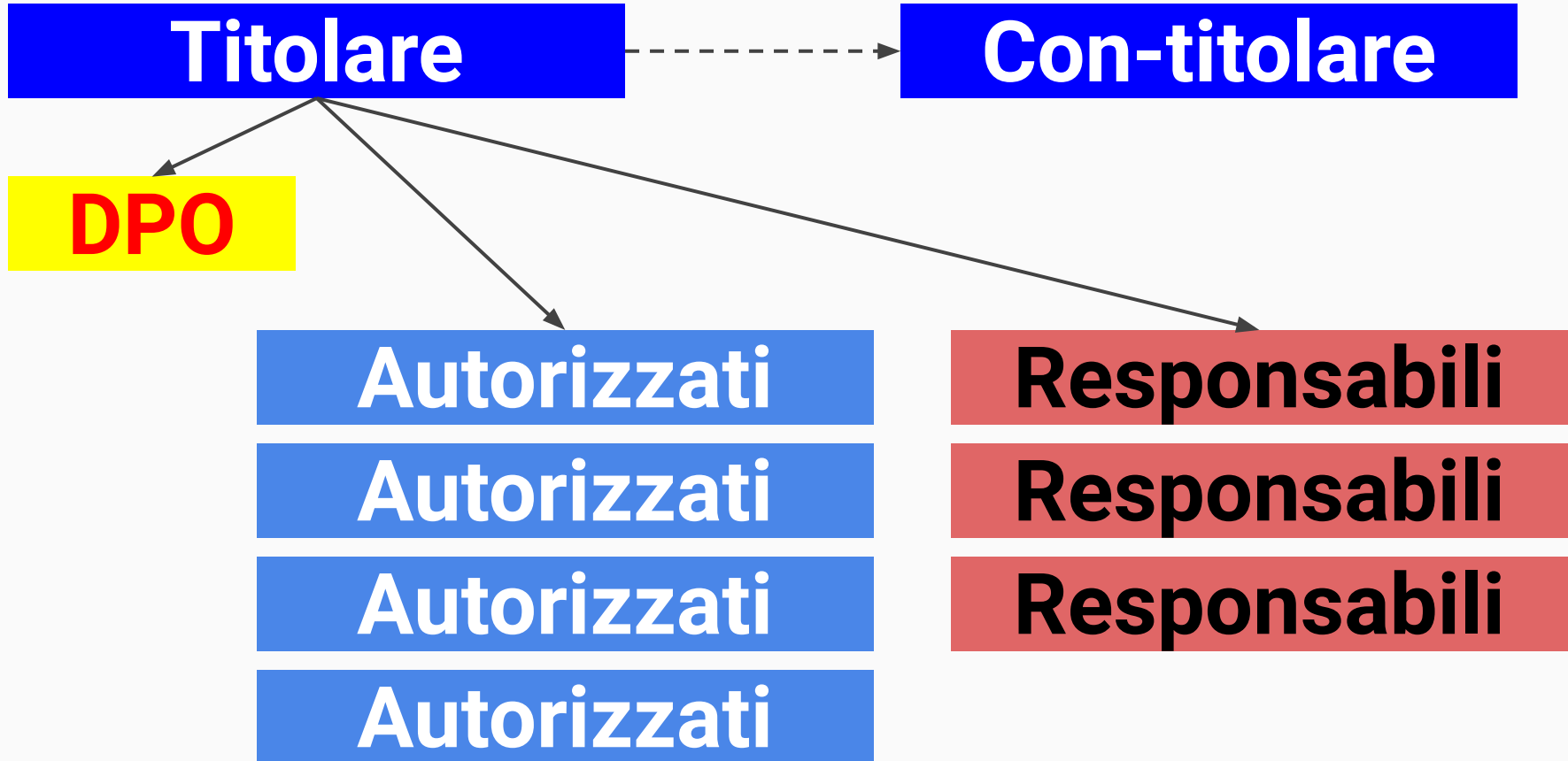
«**dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

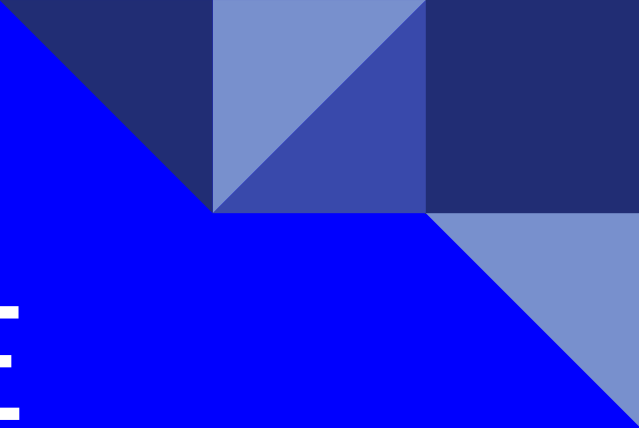
«**dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

«**dati relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;



RUOLI E ORGANIZZAZIONE

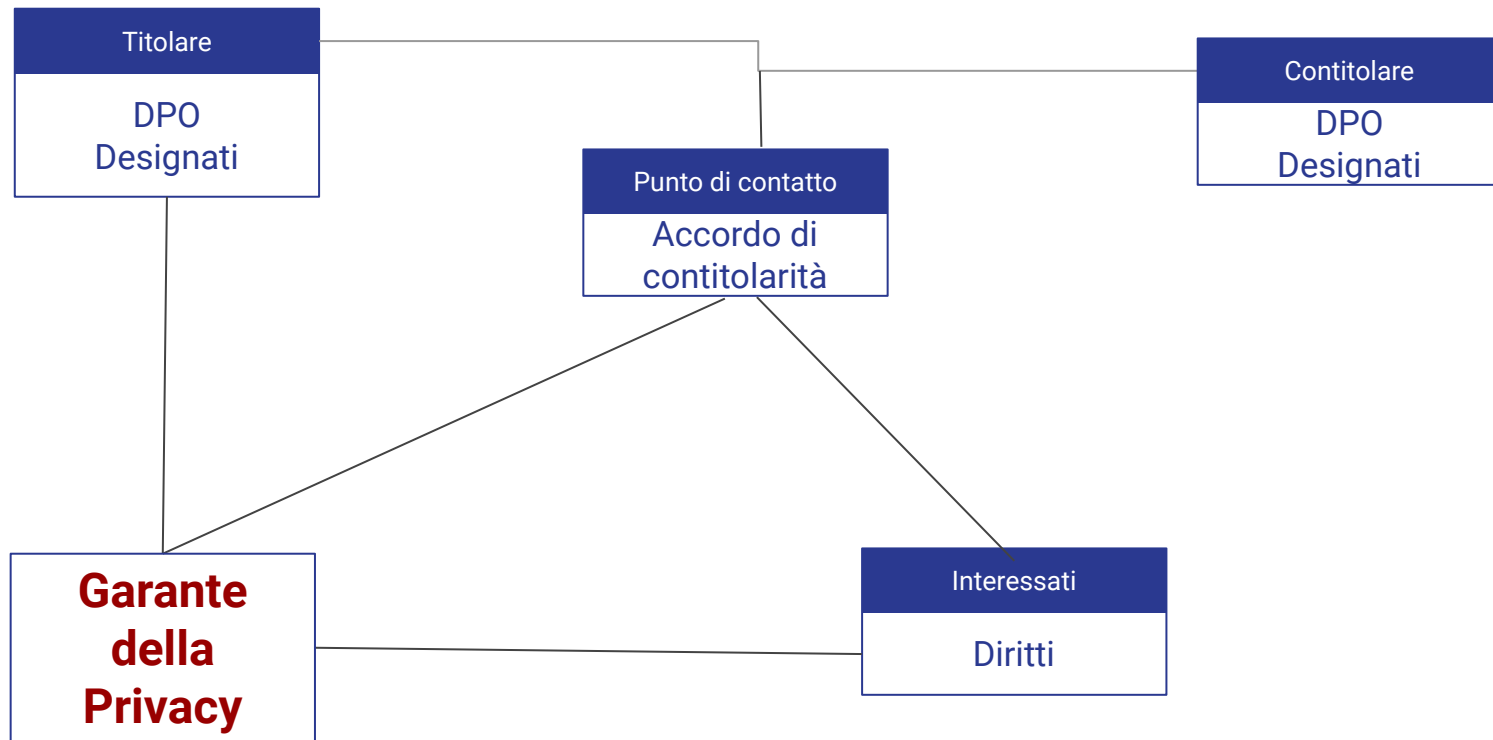


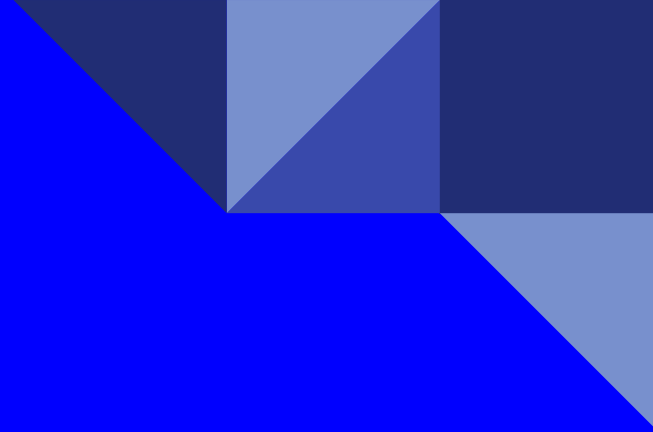


TITOLARE

CONTITOLARE

Titolare e contitolare





DPO-RPD
(responsabile protezione dati)

D.P.O. (R.P.D.)

Art. 37
regolamento UE 2016/679

PUBBLICA AMMINISTRAZIONE

- Qualora il titolare del trattamento o il responsabile del trattamento sia **un'autorità pubblica o un organismo pubblico**, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.
-

D.P.O. (R.P.D.)

Artt. 37-38
regolamento UE 2016/679

- ... tempestivamente e adeguatamente **coinvolto** in tutte le questioni riguardanti la protezione dei dati personali.
- ... fornendogli le **risorse necessarie** per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica
- ... **non riceva alcuna istruzione** per quanto riguarda l'esecuzione di tali compiti.
- ... può svolgere **altri compiti e funzioni**. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni
—— non diano adito a un **conflitto di interessi**.

D.P.O. (R.P.D.)

Artt. 37-38
regolamento UE 2016/679

- Il responsabile della protezione dei dati riferisce direttamente al **vertice gerarchico** del titolare del trattamento o del responsabile del trattamento.
 - Gli interessati **possono contattare** il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.
 - ... è tenuto al **segreto** o alla riservatezza in merito all'adempimento dei propri compiti
-

D.P.O. (R.P.D.)

Artt. 37-38
regolamento UE 2016/679

- informare e fornire **consulenza** al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
-

D.P.O. (R.P.D.)

Artt. 37-38
regolamento UE 2016/679

- **sorvegliare l'osservanza** del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, **la sensibilizzazione e la formazione** del personale che partecipa ai trattamenti e alle connesse attività di controllo;
-

D.P.O. (R.P.D.)

Artt. 37-38
regolamento UE 2016/679

- fornire, se richiesto, un **parere in merito alla valutazione d'impatto** sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
 - **cooperare con l'autorità di controllo**; e
 - fungere da **punto di contatto** per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.
-



RESPONSABILE
(esterno) DEL
TRATTAMENTO

Responsabile del trattamento

Art. 4 (definizione)

la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali **per conto del titolare** del trattamento

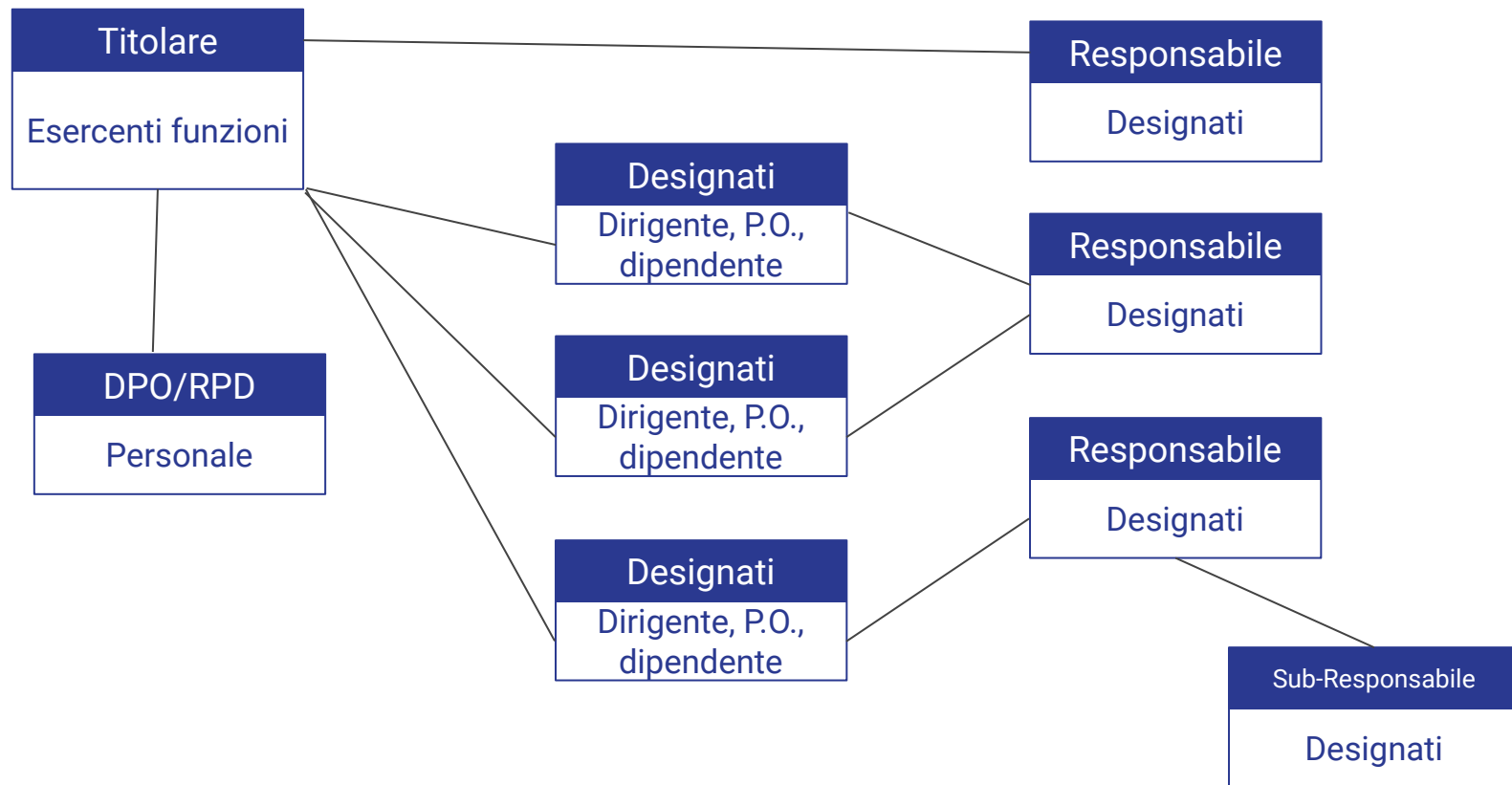
Titolare-Responsabile

ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate ...

Sub-responsabile

Il responsabile non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare. Nel caso di autorizzazione scritta generale, il responsabile informa il titolare

Titolare - Responsabile - Designati



Responsabile

Art. 28
regolamento UE 2016/679

- I trattamenti da parte di un responsabile del trattamento sono disciplinati da un **contratto** o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.
-

Responsabile

Art. 28
regolamento UE 2016/679

- il responsabile del trattamento **informa immediatamente il titolare** del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.
L'adesione da parte del responsabile del trattamento a un codice di condotta o a un meccanismo di certificazione può essere utilizzata come elemento per dimostrare le garanzie sufficienti
-

Responsabile

Art. 29
regolamento UE 2016/679

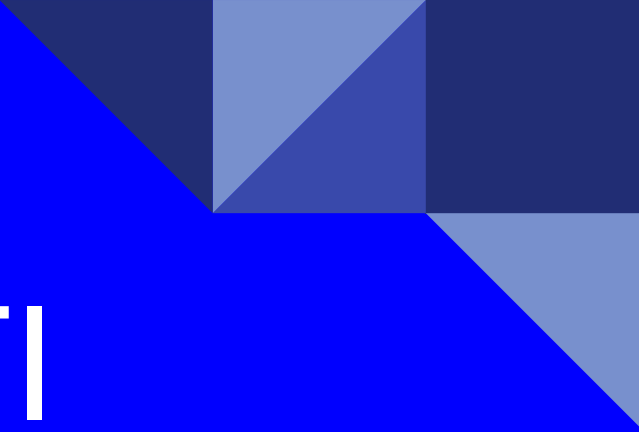
- Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati **se non è istruito** in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati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

Responsabile

Art. 33
regolamento UE 2016/679

DATA BREACH

- Il responsabile del trattamento informa il titolare del trattamento **senza ingiustificato ritardo** dopo essere venuto a conoscenza della violazione.



DESIGNATI
AUTORIZZATI
(interni)

Art. 2-quaterdecies “CODICE PRIVACY” (Attribuzione di funzioni e compiti a soggetti designati)

Chi sono

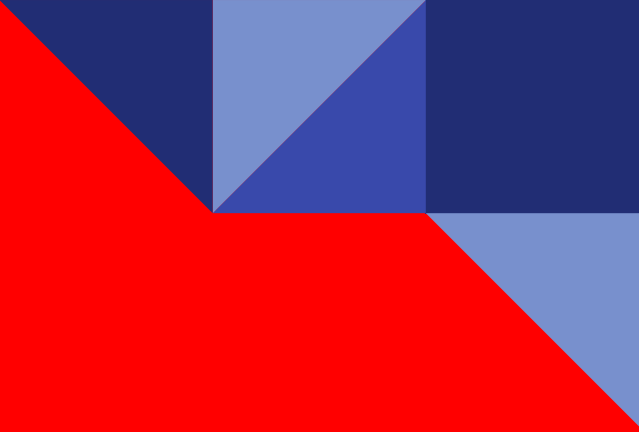
Il **titolare** o il **responsabile** del trattamento **possono** prevedere **persone fisiche, espressamente** designate, che operano sotto la loro **autorità**

Cosa fanno

specifici compiti e funzioni connessi al trattamento di dati personali

Come designarli

Il titolare o il responsabile del trattamento individuano le **modalita' piu' opportune**



ATTI,
DOCUMENTI,
REGISTRI



REGISTRO DEI TRATTAMENTI

Analisi delle problematiche

Analisi rischi

Analisi dei rischi derivanti
dalla propria attività

Focalizzazione sui
trattamenti a rischio

Collegamento a PIA
(valutazione impatto)

Analisi trattamenti

Analisi e censimento dei
trattamenti effettuati ad
un livello di dettaglio
adeguato

Selezione dei trattamenti
in PIA

Registro

Elaborazione del registro
dei trattamenti

Elaborazione delle
informative collegate ai
trattamenti

Inserimento dei
trattamenti PIA nella
valutazione

Il registro dei trattamenti

GDPR (preambolo 82)

Per **dimostrare** che si conforma al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe tenere un registro delle attività di trattamento effettuate sotto la sua responsabilità

Elementi

Titolare e Responsabile

Registro - **Accountability**

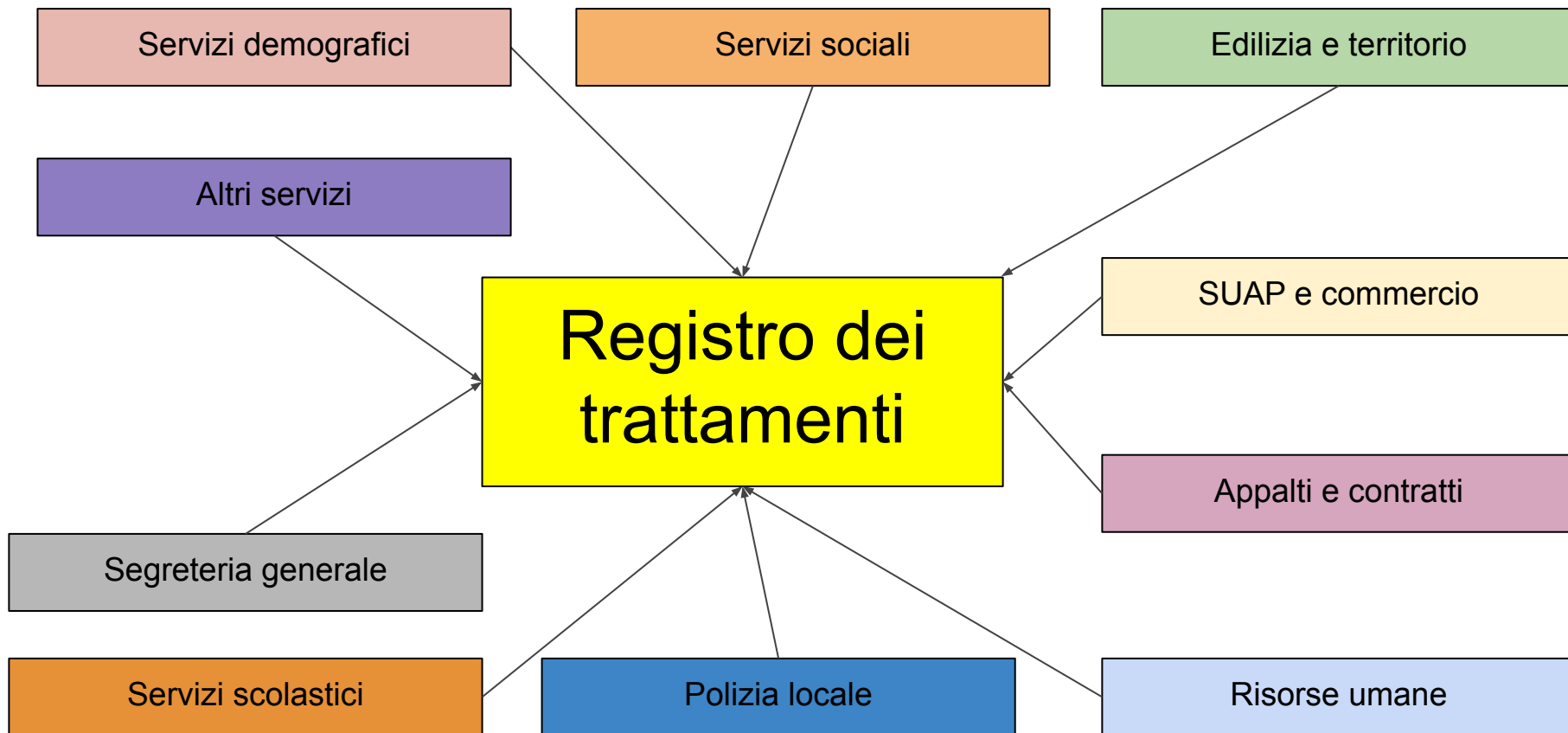
forma **scritta**, anche in formato elettronico

a disposizione dell'autorità di controllo

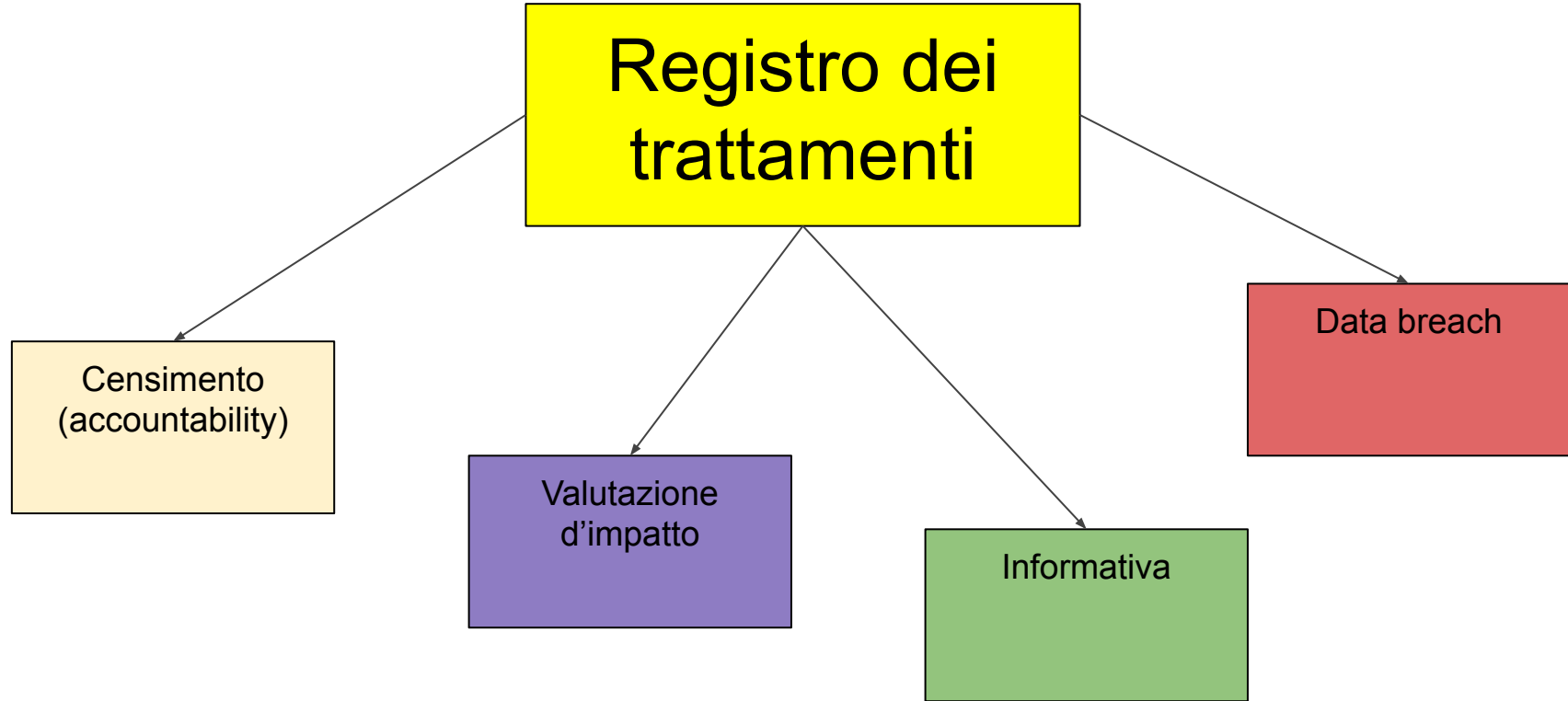
GDPR (art. 30)

+ di 250 dipendenti,
- **tutti** se rischio per i diritti e le libertà dell'interessato o categorie particolari di dati (dati sensibili e penali)

Registro e complessità organizzativa degli EELL



Registro (strumento base dell'accountability)



Registro

Approfondimenti

- coinvolgimento organizzazione
- tecniche di redazione
- modalità di approvazione
- modalità di aggiornamento
- coinvolgimento DPO
- benchmarking

Registro

Esempi

- Consiglio Nazionale Forense

<http://www.consiglionazionaleforense.it/documents/20182/431068/All.+B+-+FAO+privacy+-+Schema+di+registro+dei+trattamenti+%2828-3-2018%29.xls/4dc82b2c-0723-4909-9dd9-767708b92245>

- Comune di Firenze

https://accessoconcertificato.comune.fi.it/OdeProduzione/FIODEWeb4.nsf/PRG_V001_Allegati/2018_G_00186?OpenDocument

Istruzioni del Garante del 8/10/2018



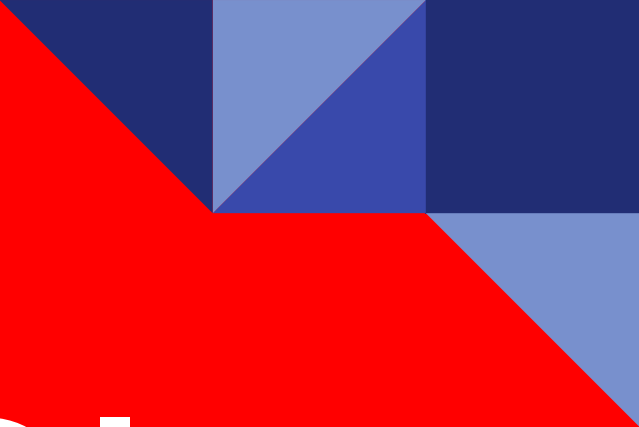
- imprese o organizzazioni con almeno **250 dipendenti**;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti che possano presentare un **rischio – anche non elevato** – per i diritti e le libertà dell'interessato;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui **trattamenti non occasionali**;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti delle **categorie particolari di dati** di cui all'articolo 9, paragrafo 1 RGPD, o di dati personali relativi a condanne penali e a reati di cui all'articolo 10 RGPD.

Esemplificazione di soggetti tenuti al registro

- **esercizi commerciali**, esercizi pubblici o artigiani con almeno un dipendente (bar, ristoranti, officine, negozi, piccola distribuzione, ecc.) e/o che trattino dati sanitari dei clienti (es. parrucchieri, estetisti, ottici, odontotecnici, tatuatori ecc.);
- **liberi professionisti** con almeno un dipendente e/o che trattino dati sanitari e/o dati relativi a condanne penali o reati (es. commercialisti, notai, avvocati, osteopati, fisioterapisti, farmacisti, medici in generale);
- **associazioni**, fondazioni e comitati ove trattino “categorie particolari di dati” e/o dati relativi a condanne penali o reati (i.e. organizzazioni di tendenza; associazioni a tutela di soggetti c.d. “vulnerabili” quali ad esempio malati, persone con disabilità, ex detenuti ecc.; associazioni che perseguono finalità di prevenzione e contrasto delle discriminazioni di genere, razziali, basate sull’orientamento sessuale, politico o religioso ecc.; associazioni sportive con riferimento ai dati sanitari trattati; partiti e movimenti politici; sindacati; associazioni e movimenti a carattere religioso);
- il **condominio** ove tratti “categorie particolari di dati” (es. delibere per interventi volti al superamento e all’abbattimento delle barriere architettoniche ai sensi della L. n. 13/1989; richieste di risarcimento danni comprensive di spese mediche relativi a sinistri avvenuti all’interno dei locali condominiali).



REGISTRO DEI ACCOUNTABILITY



PRINCIPI

Art. 5

1. 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**»);

Art. 5

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**»);

Art. 5

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**»);

Art. 5

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**»).

Art. 5 GDPR (Principi applicabili al trattamento di dati personali)

Il titolare del trattamento è competente per il rispetto dei principi e in grado di provarlo (**«responsabilizzazione»**).

LICEITA' DEL TRATTAMENTO

Art. 6 - Liceità del trattamento

1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:
 - a) l'interessato ha espresso il **consenso** al trattamento dei propri dati personali per una o più specifiche finalità;
 - b) il trattamento è necessario all'esecuzione di un **contratto** di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
 - c) il trattamento è necessario per adempiere un **obbligo legale** al quale è soggetto il titolare del trattamento;

Art. 6 - Liceità del trattamento

- d) il trattamento è necessario per la **salvaguardia degli interessi vitali** dell'interessato o di un'altra persona fisica;
- e) il trattamento è necessario per l'esecuzione di un **compito di interesse pubblico o connesso all'esercizio di pubblici poteri** di cui è investito il titolare del trattamento;
- f) il trattamento è necessario per il **perseguimento del legittimo interesse del titolare del trattamento o di terzi**, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Art. 2-sexies (Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante)

1. I trattamenti delle categorie **particolari di dati personali di cui all'articolo 9**, paragrafo 1, del Regolamento, necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g), del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di **legge** o, nei casi previsti dalla legge, di regolamento che specifichino **i tipi di dati che possono essere trattati**, le **operazioni** eseguibili e il **motivo** di interesse pubblico rilevante, nonché le **misure appropriate e specifiche** per tutelare i diritti fondamentali e gli interessi dell'interessato.

2. Fermo quanto previsto dal comma 1, **si considera rilevante l'interesse pubblico** relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle seguenti materie:

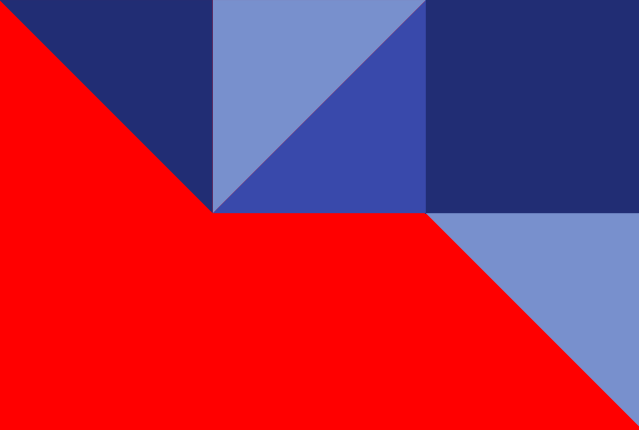
...

o) rapporti tra i soggetti pubblici e gli enti del terzo settore;

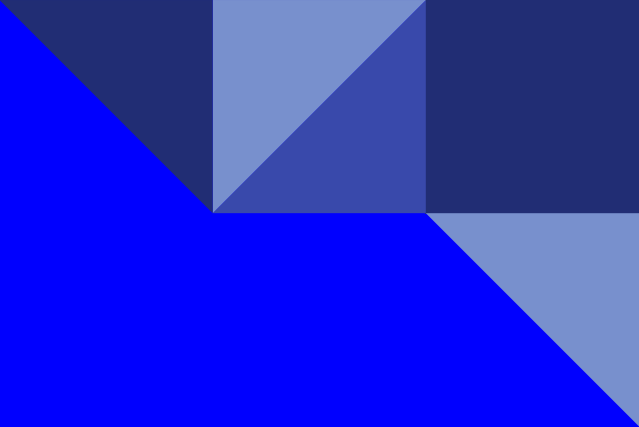
p) obiezione di coscienza;

...

s) attività socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci;



STRUMENTI



INFORMATIVA

Informazioni e informativa

GDPR (considerando 60)

I principi di trattamento corretto e trasparente implicano che l'interessato sia **informato** dell'esistenza del trattamento e delle sue finalità

Elementi

Identità e dati di contatto
del titolare, DPO

Finalità

Destinatari

Periodo di conservazione

Diritti

GDPR (art. 13-14)

Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato

Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato

Informazioni

Raccolta dati

In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, **nel momento in cui i dati personali sono ottenuti**

Informazioni

Le informazioni sono fornite **per iscritto** o con altri mezzi, anche, se del caso, con mezzi **elettronici**.

Consenso

Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere **in grado di dimostrare** che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.

Informazioni

Art. 13-14
regolamento UE 2016/679

- l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
 - i dati di contatto del responsabile della protezione dei dati, ove applicabile;
 - le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
 - qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
-

Informazioni

Art. 13-14
regolamento UE 2016/679

- gli eventuali destinatari o le eventuali categorie;
- l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo
- il periodo di conservazione dei dati personali oppure i criteri utilizzati per determinare tale periodo;
- l'esistenza dei diritti dell'interessato
- il diritto di proporre reclamo a un'autorità di controllo;
- le possibili conseguenze della mancata comunicazione di tali dati
- l'esistenza di un processo
_____decisionale automatizzato

SETTORE "Entrate, sviluppo economico, sport e servizi amministrativi"
INFORMATIVA AI SENSI DEGLI ART. 13-14 DEL GDPR (GENERAL DATA PROTECTION
REGULATION) 2016/679 E DELLA NORMATIVA NAZIONALE

INFORMATIVA SEMPLIFICATA

Il Comune di Scandicci, in qualità di titolare (con sede in Piazzale della Resistenza, 1 - 50018 Scandicci (FI); Email: puntocomune@comune.scandicci.fi.it ; Centralino: +39 055055 PEC: comune.scandicci@postacert.toscana.it , tratterà i dati personali conferiti con il presente modulo, con modalità prevalentemente informatiche e telematiche, per le finalità previste dal Regolamento (UE) 2016/679 (RGPD), in particolare per l'esecuzione dei propri compiti di interesse pubblico o comunque connessi all'esercizio dei propri pubblici poteri, ivi incluse le finalità di archiviazione, di ricerca storica e di analisi per scopi statistici.	Chi tratta i miei dati?
Il conferimento dei dati al Settore è generalmente obbligatorio in quanto indispensabile per l'attivazione delle procedure di competenza relativamente ai vari uffici. In particolare saranno indicati come obbligatori i dati inseriti nella modulistica messa a disposizione contrassegnati da asterisco (*) ed il loro mancato inserimento non consente di procedere con la attivazione della procedura (in taluni casi a pena di diniego o esclusione). Per contro, il rilascio dei dati presenti nei campi non contrassegnati da asterisco o comunque non indispensabili in relazione alla specifica procedura, pur potendo risultare utile per agevolare la gestione della procedura e la fornitura del servizio, è facoltativo e la loro mancata indicazione non pregiudica il completamento della procedura stessa.	Ho l'obbligo di fornire i dati?
I dati saranno trattati per tutto il tempo necessario alla gestione della procedura nonché, successivamente, per finalità di archiviazione a tempo indeterminato. I dati saranno conservati in conformità alle norme sulla conservazione della documentazione amministrativa. Eventuali diverse indicazioni saranno contenute nella specifica modulistica.	Per quanto sono trattati i miei dati?
I dati saranno comunicati agli enti pubblici previsti dalla normativa per la verifica dei requisiti nonché negli altri casi previsti dalla normativa ivi compresa la pubblicazione nelle pagine dell'Ente (Amministrazione Trasparente, Albo Pretorio e simili) o in banche dati nazionali. I dati saranno trasmessi ad altri soggetti (es. controinteressati, partecipanti al procedimento, altri richiedenti) in particolare in caso di richiesta di accesso ai documenti amministrativi.	A chi vengono inviati i miei dati?
Gli interessati hanno il diritto di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento (artt. 15 e ss. del RGPD). L'apposita istanza all'Autorità è presentata contattando il Responsabile della protezione dei dati presso il Comune - avv. Marco Giuri. DATI DI CONTATTO Telefono – 055489464 - Cellulare – 3389642439 - e mail - marcogiuri@studiogiuri.it - pec - consolve@pec.it	Che diritti ho sui miei dati?
Gli interessati, ricorrendone i presupposti, hanno, altresì, il diritto di proporre reclamo al Garante quale autorità di controllo secondo le procedure previste. Per ulteriori informazioni https://www.garanteprivacy.it	A chi mi posso rivolgere?
Maggiori e più puntuali precisazioni sulle finalità di trattamento è fornito nella scheda "informativa dettagliata".	Tutto qui?

le informazioni destinate al pubblico o all'interessato siano **concise**, facilmente accessibili e **di facile comprensione** e che sia usato un **linguaggio semplice e chiaro**, oltre che, se del caso, una **visualizzazione**

**GARE E APPALTI
INFORMATIVA DETTAGLIATA
INFORMATIVA AI SENSI DEGLI ART. 13-14 DEL GDPR (GENERAL DATA PROTECTION
REGULATION) 2016/679 E DELLA NORMATIVA NAZIONALE**

Secondo la normativa indicata, il trattamento relativo al presente servizio sarà improntato ai principi di **correttezza, liceità, trasparenza e di tutela della Sua riservatezza e dei Suoi diritti**.

Ai sensi dell'articolo 13 del GDPR 2016/679, pertanto, Le forniamo le seguenti informazioni:

I dati personali che in occasione dell'attivazione del presente servizio saranno raccolti e trattati **riguardano**:

- ☒ dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro)
- ☐ situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale.
- ☐ dati inerenti lo stile di vita
- ☒ situazione economica
- ☒ situazione finanziaria
- ☒ situazione patrimoniale
- ☒ situazione fiscale
- ☒ dati di connessione: indirizzo IP, login, altro.
- ☒ dati di localizzazione: ubicazione, GPS, GSM, altro.

Sono richiesti dati personali relativi ai **sogetti che fanno parte dell'impresa (titolare, soci, procuratori) e/ o loro delegati o soggetti collegati (es. Procuratore, soci ecc...)**

In particolare sono previsti trattamenti di cui all'art. 9 e 10 GDPR (ex **dati sensibili e giudiziari**):

- ☐ Dati inerenti l'origine razziale o etnica
- ☐ opinioni politiche
- ☐ convinzioni religiose o filosofiche
- ☐ appartenenza sindacale
- ☐ salute, vita o orientamento sessuale
- ☐ dati genetici e biometrici

☒ dati relativi a condanne penali

Si tratta di dati riguardanti i requisiti morali dei soggetti con potere di amministrazione (casellario, carichi pendenti, requisiti antimafia)

I dati raccolti saranno trattati **in quanto**:

- ☐ l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità (in questo caso il consenso sarà acquisito con separato atto);
- ☒ il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

Dettagli: Ai sensi del Dlgs 50/2016 la partecipazione alle procedure per l'affidamento di appalti e concessioni determina l'attivazione di rapporti contrattuali e precontrattuali con la stazione appaltante

☒ Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

Dettagli: Il Dlgs 50/2016 (e relative disposizioni di attuazione) prevede l'obbligo per la stazione appaltante di acquisire i dati inerenti la partecipazione alle procedure di gara ed i conseguenti atti (ammissione, esclusione, aggiudicazione, stipulazione)

- ☐ il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- ☒ il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

Dettagli: Il Dlgs 50/2016 (e relative disposizioni di attuazione) prevede l'obbligo per la stazione appaltante di acquisire i dati inerenti la partecipazione alle procedure di gara ed i conseguenti atti (ammissione, esclusione, aggiudicazione, stipulazione)

- ☐ il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

I dati personali forniti saranno **oggetto** di:

- ☒ raccolta
- ☒ registrazione
- ☒ organizzazione
- ☒ strutturazione
- ☒ conservazione
- ☒ adattamento o modifica

- ☒ estrazione
- ☒ consultazione
- ☒ uso
- ☒ comunicazione mediante trasmissione
- ☒ diffusione o qualsiasi altra forma di messa a disposizione
- ☒ raffronto od interconnessione
- ☒ limitazione
- ☒ cancellazione o distruzione
- ☐ profilazione
- ☒ pseudonimizzazione
- ☐ ogni altra operazione applicata a dati personali

Dettagli: Il trattamento dei dati avviene tramite applicativo informatico centralizzato (Me.P.A., e applicativi dei mercati elettronici regionali o della stazione appaltante) e, episodicamente, con modalità cartacee. Le caratteristiche tecniche possono essere messe a disposizione degli interessati su richiesta e sono comunque in gran parte disponibili sulle piattaforme utilizzate.

In caso di comunicazione i dati saranno trasmessi a:

- ☒ Responsabili (esterni) del trattamento
- ☒ Enti Pubblici
- ☒ Privati (cointeressati, controinteressati)
- ☒ Organi di vigilanza e controllo
- ☒ Autorità giudiziaria

Il trattamento:

- ☐ comporta l'attivazione di un **processo decisionale automatizzato**, compresa la profilazione, consistente in
- ☒ non comporta l'attivazione di un processo decisionale automatizzato

Si informa che, tenuto conto delle finalità del trattamento come sopra illustrate, il conferimento dei dati è **obbligatorio** ed il loro mancato, parziale o inesatto conferimento potrà avere, come conseguenza, l'impossibilità di svolgere l'attività.

Il trattamento sarà effettuato sia **con strumenti manuali e/o informatici e telematici** con logiche di organizzazione ed elaborazione strettamente correlate alle finalità stesse e comunque in modo da garantire la sicurezza, l'integrità e la riservatezza dei dati stessi nel rispetto delle misure organizzative, fisiche e logiche previste dalle disposizioni vigenti.

In particolare sono state adottate le seguenti **misure di sicurezza**:

- ☒ misure specifiche poste in essere per fronteggiare rischi di distruzione, perdita, modifica, accesso, divulgazione non autorizzata, la cui efficacia va valutata regolarmente.
- ☒ Sistemi di autenticazione
- ☒ sistemi di autorizzazione
- ☒ sistemi di protezione (antivirus; firewall; antintrusione; altro) adottati per il trattamento
- ☒ Sicurezza anche logistica

I dati personali vengono conservati:

- ☒ a tempo illimitato nel rispetto della vigente normativa
- ☐ per un periodo di anni in quanto

Lei potrà, in qualsiasi momento, esercitare i **diritti**:

- di richiedere maggiori informazioni in relazione ai contenuti della presente informativa
- di accesso ai dati personali;
- di ottenere la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano (nei casi previsti dalla normativa);
- di opporsi al trattamento (nei casi previsti dalla normativa);
- alla portabilità dei dati (nei casi previsti dalla normativa);
- di revocare il consenso, ove previsto: la revoca del consenso non pregiudica la liceità del trattamento basata sul consenso conferito prima della revoca;
- di proporre reclamo all'autorità di controllo (Garante Privacy)
- di dare mandato a un organismo, un'organizzazione o un'associazione senza scopo di lucro per l'esercizio dei suoi diritti
- di richiedere il risarcimento dei danni conseguenti alla violazione della normativa (art. 82)

Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento verranno fornite informazioni in merito a tale



diversa finalità e ogni ulteriore informazione pertinente.

L'esercizio dei suoi diritti potrà avvenire attraverso contatto diretto e/o l'invio di una richiesta anche mediante email a:

Soggetto	Dati anagrafici	Contatto tel.	email
Titolare	Comune di Scandicci (FI)	+39 055055	puntocomune@comune.scandicci.fi.it
Responsabile trattamento (interno) del	Dott. Simone Chiarelli	+39 0557591213	s.chiarelli@comune.scandicci.fi.it
Responsabili trattamento (esterni) del	Consip SPA	+39 06 854491	postaconsip@postacert.consip.it
Responsabili trattamento (esterni) del	Regione Toscana	+39 055 4385621	urp_dpo@regione.toscana.it
DPO (Responsabile Protezione Dati)	avv. Marco Giuri	Telefono 055489464 Cellulare 3389642439	marcogiuri@studiogiuri.it - consolve@pec.it

La informiamo che potrà ottenere ulteriori informazioni sul trattamento dei dati e sull'esercizio dei suoi diritti nonché sulla disciplina normativa in materia ai seguenti link:

Descrizione	Link
Pagine web del Titolare	http://www.comune.scandicci.fi.it
Regolamento (UE) 2016/679 (GDPR)	https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ITA
Garante europeo della protezione dei dati (GEPD)	https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_it
Garante italiano della protezione dei dati	http://www.garanteprivacy.it/web/guest/home
Sito privacy del Comune di Scandicci	http://www.comune.scandicci.fi.it/index.php/privacy/6198-privacyregolamento-ue-6792016-e-diritti-dellinteressato.html



CONSENSO

CONSENSI

Consenso - GDPR (considerando 32)

Consenso espresso

Il consenso dovrebbe essere espresso mediante un **atto positivo inequivocabile** con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento

Silenzio

Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle

Mezzi elettronici

Se il consenso dell'interessato è richiesto attraverso **mezzi elettronici**, la richiesta deve essere chiara, concisa e **non interferire immotivatamente con il servizio** per il quale il consenso è espresso

Consenso - GDPR (considerando 42)

Accountability

Il titolare del trattamento dovrebbe essere in grado di **dimostrare** che l'interessato ha acconsentito al trattamento

Comprensibile

dichiarazione di consenso predisposta dal titolare del trattamento in una **forma comprensibile** e facilmente accessibile, che usi un **linguaggio semplice e chiaro** e non contenga clausole abusive

Evidente squilibrio

evidente squilibrio tra l'interessato e il titolare del trattamento, specie quando il titolare del trattamento è un'autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato espresso liberamente

Consenso

Art. 7

regolamento UE 2016/679

- Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo **chiaramente distinguibile** dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un **linguaggio semplice e chiaro**.
- Il consenso è revocato con la stessa facilità con cui è —accordato.

Consenso e “dati sensibili”

Art. 9
regolamento UE 2016/679

- È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
- **non si applica se l'interessato ha prestato il proprio consenso** esplicito al trattamento di tali dati personali per una o più finalità
——specifiche



VALUTAZIONE D'IMPATTO - DPIA

Valutazione d'impatto

GDPR (preambolo 84)

qualora i trattamenti possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche **il titolare** ... l'origine, la natura, la particolarità e la gravità di tale rischio

Autorità di controllo

Se rischio elevato che il **titolare** non può attenuare mediante misure opportune in termini di tecnologia disponibile e costi di attuazione, prima del trattamento si dovrebbe consultare l'autorità di controllo.

GDPR (art. 35)

PIA “discrezionale”

PIA “necessaria”

Valutazione d'impatto

“Discrezionale”

- Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

Valutazione d'impatto

Necessaria

- una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

Valutazione d'impatto

Necessaria

- il trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e a reati
- la sorveglianza sistematica su larga scala di una zona
____accessibile al pubblico

Valutazione d'impatto

Elenco PIA

elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto

Elenco NON-PIA

può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati

Parere del DPO

(art. 39) ... il DPO deve fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento

Valutazione d'impatto

Contenuto

- descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
 - valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
 - valutazione dei rischi per i diritti e le libertà degli interessati
-

Valutazione d'impatto

Contenuto

- le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione

Valutazione d'impatto

Riesame

- Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno **quando insorgono variazioni del rischio** rappresentato dalle attività relative al trattamento.

Valutazione d'impatto

**Valutazione preventiva
con il Garante**

- Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione indichi che il trattamento presenterebbe un **rischio elevato in assenza di misure** adottate dal titolare del trattamento per attenuare il rischio.
-



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

ALLEGATO 1 AL PROVVEDIMENTO N. 467 DELL'11 OTTOBRE 2018 [doc. web n. 9058979]

(Pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018)

Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto

1. Trattamenti valutativi o di *scoring* su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad *"aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato"*.
2. Trattamenti automatizzati finalizzati ad assumere decisioni che producono *"effetti giuridici"* oppure che incidono *"in modo analogo significativamente"* sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. *screening* dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi).
3. Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi *web*, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di *budget*, di *upgrade* tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.

4. Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).
5. Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).
6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).
7. Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi *wearable*; tracciamenti di prossimità come ad es. il *wi-fi tracking*) ogniquale volta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01 .
8. Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.
9. Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. *mobile payment*).

10. Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.

11. Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

12. Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

**Valutazione d'impatto sulla
protezione dei dati (DPIA)**

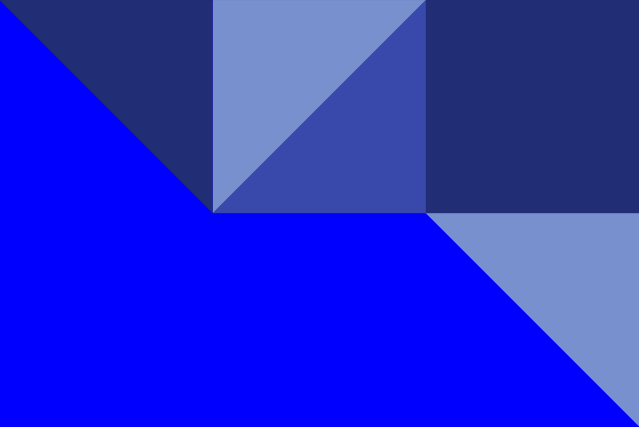


Valutazione d'impatto

Esempi

- <https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil>





DIRITTI

I diritti degli interessati

Richiesta di maggiori informazioni (art. 5)

Diritto di accesso (art. 15)

Diritto di rettifica (art. 16)

Diritto di cancellazione (diritto all'oblio) (art.17)

Diritto di limitazione del trattamento (art. 18)

Diritto alla portabilità dei dati (art. 20)

Diritto di mandato a terzi (art. 80)

Diritto al risarcimento (art. 82)

Diritto all'informazione per data breach (art. 33)

Diritto al contatto con il DPO (art. 26)

Diritto di proporre reclamo all'autorità di controllo (art. 77)

Reclamo (artt. 140-bis, 141, 142)

- “interessato” (soggetto qualificato)
- documentato
- scritto e sottoscritto
- 3 mesi (stato di avanzamento)
- 9 mesi (decisione)
- ricorribile

Segnalazione (art. 144)

- chiunque (anche anonimo)
- Garante può valutare (o meno)
- scritto/orale
- nessun termine
- anche d'ufficio
- poteri art. 58 GDPR

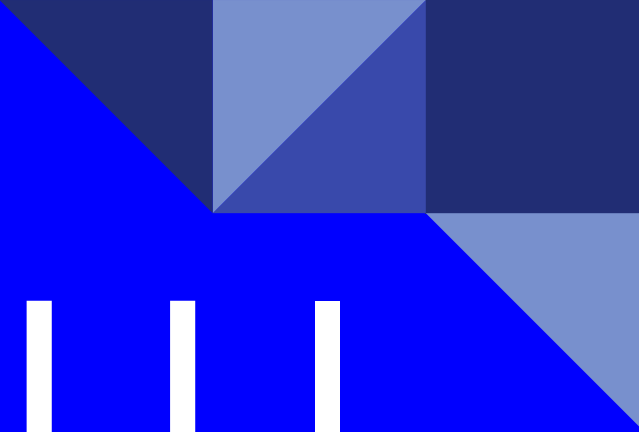
Art. 2-decies (Inutilizzabilità dei dati)

I dati personali trattati **in violazione** della disciplina **rilevante** in materia di trattamento dei dati personali **non possono essere utilizzati**,

salvo articolo 160- bis [**processo**].

Art. 2-terdecies (Diritti riguardanti le persone decedute)

3. La volonta' dell'interessato di vietare l'esercizio dei diritti di cui al comma 1 deve risultare **in modo non equivoco** e deve essere **specificata, libera e informata**; il divieto puo' riguardare l'esercizio soltanto di alcuni dei diritti di cui al predetto comma.
4. L'interessato ha **in ogni momento** il diritto di revocare o modificare il divieto di cui ai commi 2 e 3.
5. In ogni caso, il divieto **non puo' produrre effetti pregiudizievoli** per l'esercizio da parte dei terzi dei diritti patrimoniali che derivano dalla morte dell'interessato nonche' del diritto di difendere in giudizio i propri interessi.



CONTROLLI
SANZIONI

Art. 96 (Trattamento di dati relativi a studenti)

Indagine (art. 157)

il Garante puo' richiedere al **titolare**, al **responsabile**, al **rappresentante**, all'**interessato** o anche a **terzi** di fornire informazioni e di esibire documenti anche con riferimento al contenuto di banche di dati.

Accertamenti

Luogo pubblico

Internet

Luoghi di lavoro

Privata abitazione

Rinvio (art. 160-bis)

Validita', efficacia e utilizzabilita' nel procedimento giudiziario di atti, documenti e provvedimenti basati sul trattamento di dati personali non conforme restano disciplinate dalle pertinenti disposizioni processuali.

SANZIONI AMMINISTRATIVE PECUNIARIE

Procedimento

Indagine - accertamenti - verifiche

Avvio del procedimento

30 giorni per scritti difensivi e/o audizione

Ordinanza ingiunzione con criteri art. 83

Pagamento in misura ridotta (50%)

30 giorni per ricorso

Regolamento del Garante per la procedura

Rinvio a L. 689/1981 (articoli 1-9, 18-22, 24-28)

SANZIONI AMMINISTRATIVE PECUNIARIE

Entità

Fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente

SANZIONI PENALI “speciali”

Tipologie del Codice

Art. 167 (Trattamento illecito di dati)

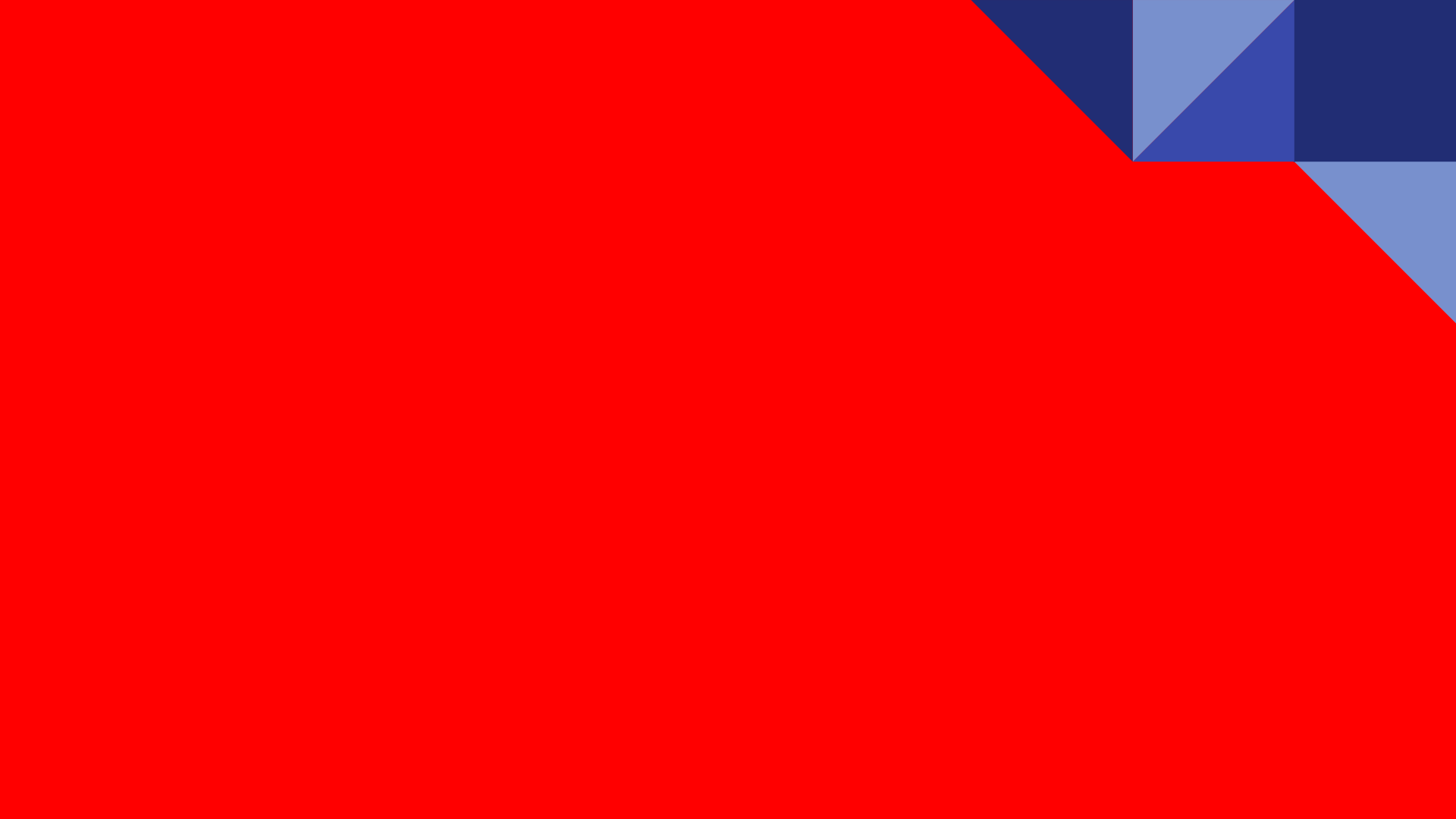
Art. 167- bis (Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala)

Art. 167- ter (Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala)

Art. 168 (Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante)

Art. 170 (Inosservanza di provvedimenti del Garante)

Art. 171 (Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori)



Accesso e riservatezza

Art. 59

Accesso ai **DOCUMENTI** rimane disciplinato dalla legge 7 agosto 1990, n. 241 e **regolamenti** di attuazione

Art. 59

I presupposti, le modalità e i limiti per l'esercizio del diritto di **accesso civico** restano disciplinati dal decreto legislativo 14 marzo 2013, n. 33.

Art. 60

salute - vita sessuale - orientamento sessuale

trattamento consentito **se** la situazione giuridicamente rilevante e' di rango almeno pari ai diritti dell'interessato, **ovvero** diritto della personalita' o libertà fondamentale

Accesso ai documenti amministrativi

- Accesso infraprocedimentale (art. 10)
- Accesso ai documenti (artt. 22 e ss.)

Accesso civico

- Ordinario (art. 5 comma 1 Dlgs 33/2013)
- generalizzato (art. 5 comma 2 Dlgs 33/2013)

Accesso privacy

- GDPR (art. 15 regolamento UE 2016/679)

Schema



Silenzio

Rifiuto

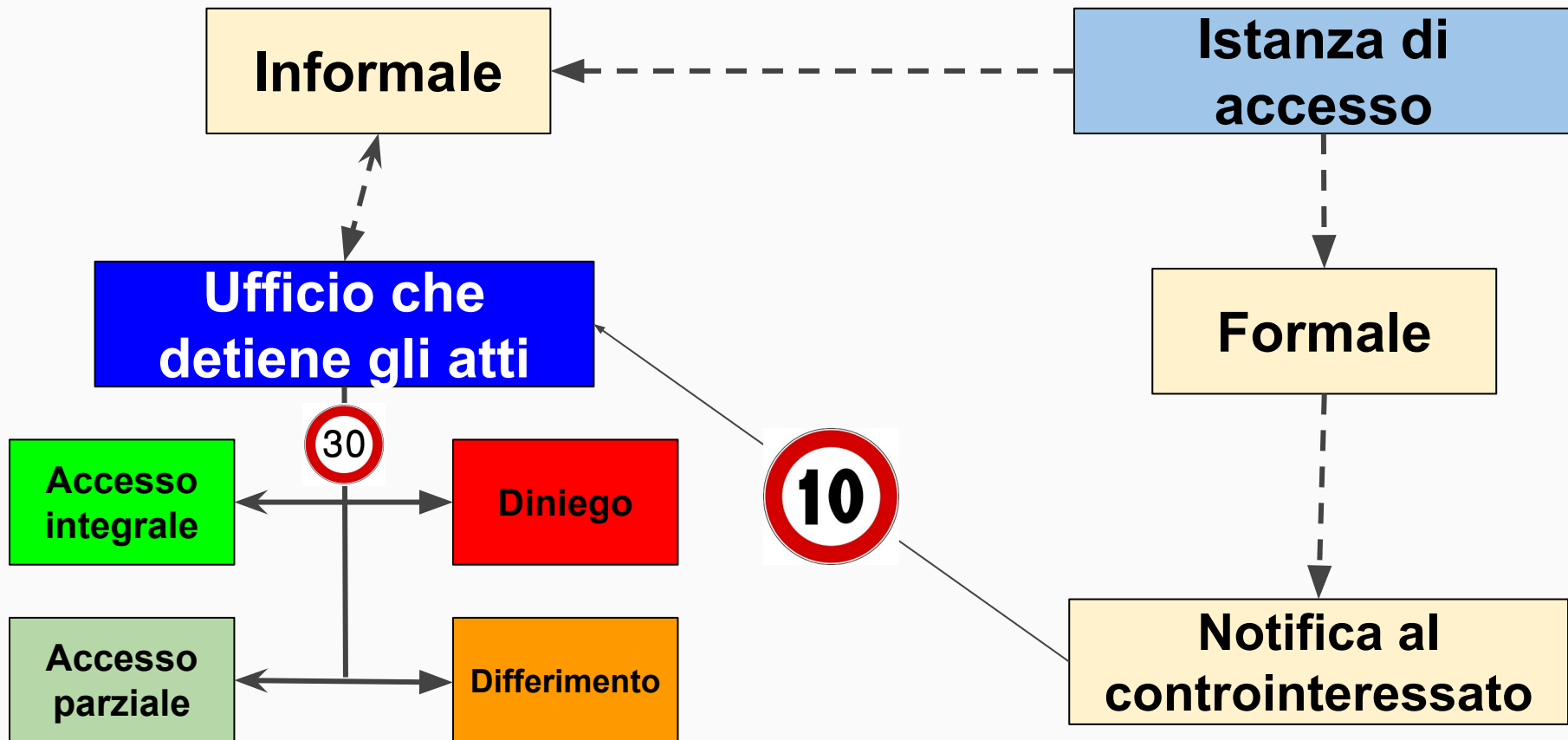
Limitazione

Differimento



Accoglimento

Accesso e procedura



Accesso Civico

Two thick, wavy horizontal lines, one green and one red, positioned below the 'Accesso Civico' text.

Informatica a servizio
del corretto
trattamento dei dati



Dall'analogico al
digitale



Dal digitale
all'analogico



Sei superato libro



Io sono il futuro



Basta una fiamma
per distruggerti



Click.



Spazio ai quesiti



“Per approfondimenti”

<https://www.youtube.com/user/simonechiarelli>

<https://www.facebook.com/simone.chiarelli>



Simone Chiarelli