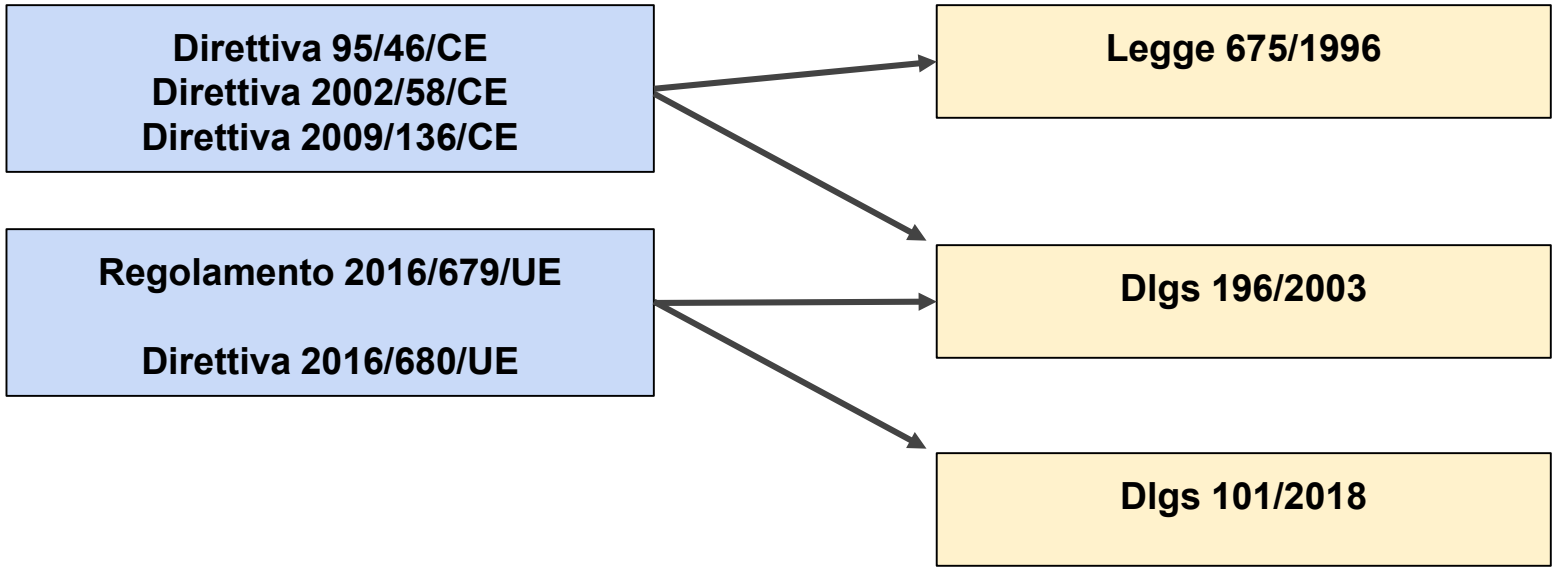
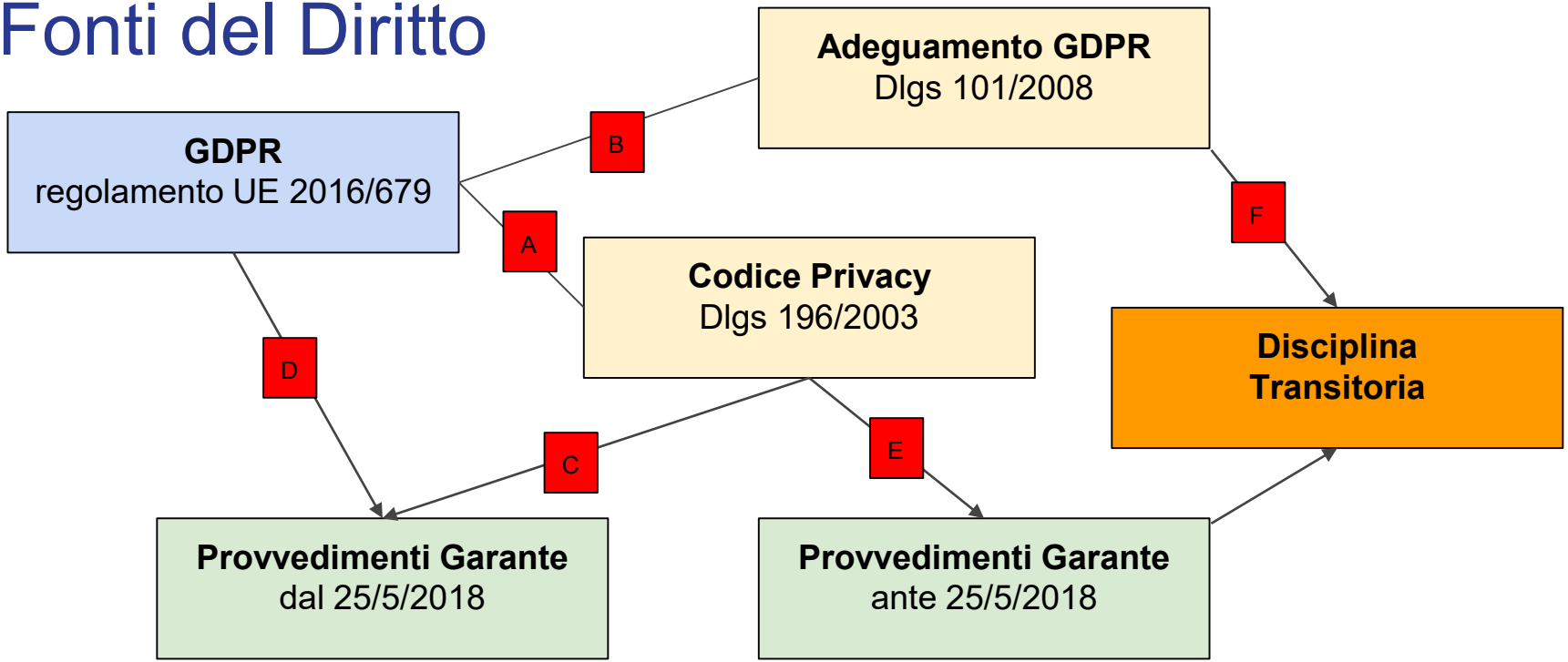
GDPR e privacy

La tutela delle persone nel trattamento dei dati nell'Amministrazione Pubblica

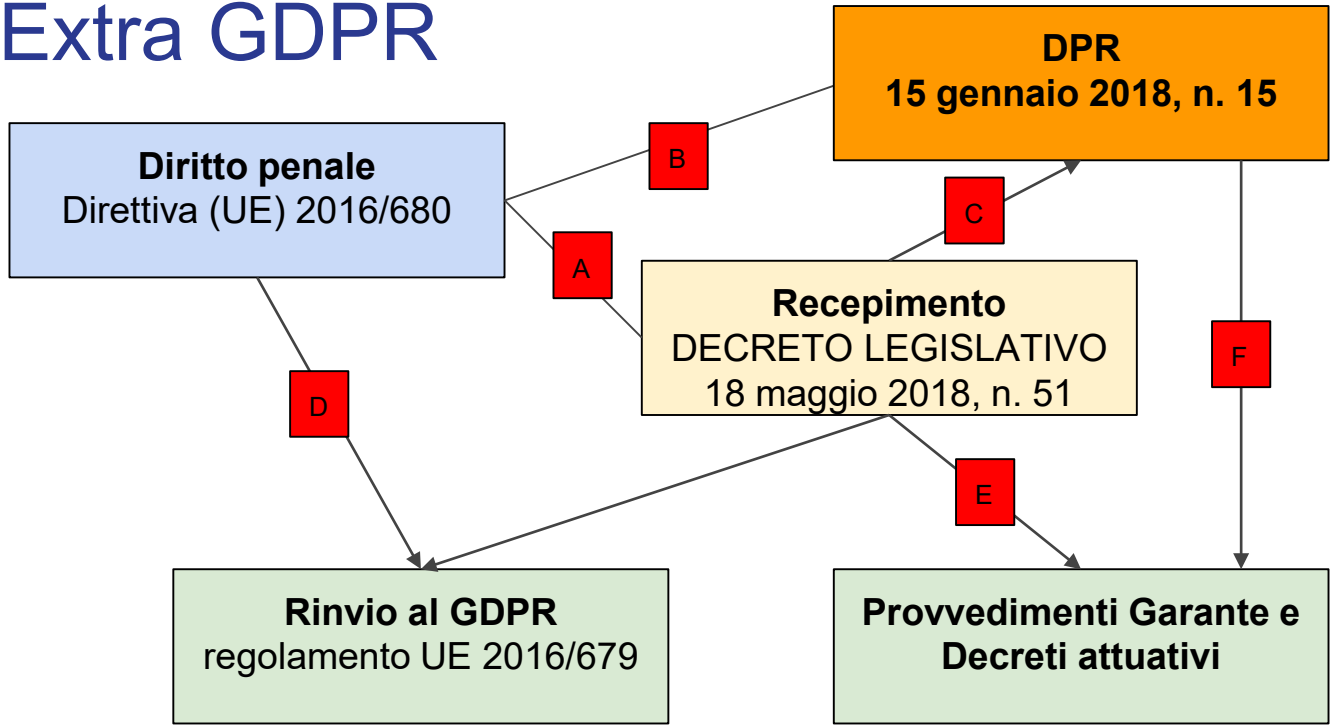
STORIA


Direttiva 95/46/CE
Direttiva 2002/58/CE
Direttiva 2009/136/CE
Regolamento 2016/679/UE
Direttiva 2016/680/UE
Legge 675/1996
Dlgs 196/2003
Dlgs 101/2018

Fonti del Diritto



Extra GDPR


DPR
15 gennaio 2018, n. 15
Diritto penale
Direttiva (UE) 2016/680
B
C
A
Recepimento
DECRETO LEGISLATIVO
18 maggio 2018, n. 51
F
D
E
Rinvio al GDPR
regolamento UE 2016/679
Provvedimenti Garante e
Decreti attuativi

DECRETO LEGISLATIVO 10 agosto 2018, n. 101

Disposizioni per l'**adeguamento** della normativa nazionale alle disposizioni del **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, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

(GU Serie Generale n.205 del 04-09-2018)

note: Entrata in vigore del provvedimento: **19/09/2018**

Cosa contiene il Dlgs 101/2018

Modifiche Dlgs 196/2003

Molti articoli del Codice della Privacy (Dlgs 196/2003) vengono corretti per adattarli alla nuova terminologia del GDPR

Abrogazioni Dlgs 196/2003

L'intervento più significativo riguarda le abrogazioni sia al Dlgs 196/2003 (le più importanti) che ad altre disposizioni

Nuove disposizioni

Gli articoli 17 e seguenti del Dlgs 101/2018 sono "norme nuove" e come tali non si ritrovano nel Dlgs 196/2003

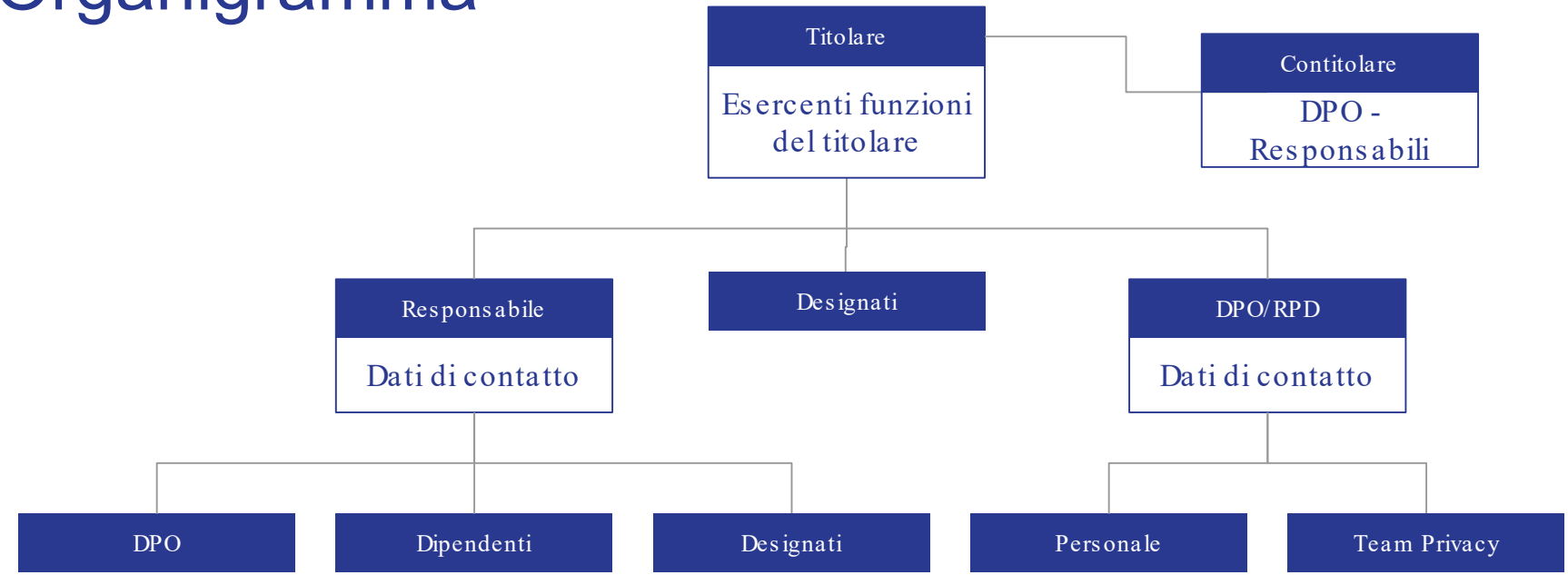
Cosa NON contiene il Dlgs 101/2018

Disposizioni sui soggetti	Disposizioni su adempimenti	Altro
La normativa nazionale non disciplina più titolare, contitolare, responsabile, dpo ecc… tranne qualche disposizione secondaria e la novità dei “designati”	Nessuna norma su Registri, DPIA (valutazione d’impatto) e rinvio completo sugli altri adempimenti (salvo qualche disposizione su reclamo)	Manca una disciplina specifica sulle sanzioni (minimo-massimo) per cui si rinvia al GDPR mentre ci sono disposizioni sulle procedure di applicazione

Ruoli e responsabilità nel sistema GDPR

Titolare, contitolare, DPO, Responsabili, autorizzati ecc.….

Organigramma



TITOLARE

CONTITOLARE

Titolare

Art. 4 (definizione)

la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali

Accountability

Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di **comprovarlo** («responsabilizzazione»)

Esercente funzioni

D.P.C.M. 25 maggio 2018 "i soggetti individuati per l'esercizio delle funzioni di titolare del trattamenti dei dati personali, ciascuno nel rispettivo ambito di competenza, sono: …."

Contitolare

Art. 26

Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento

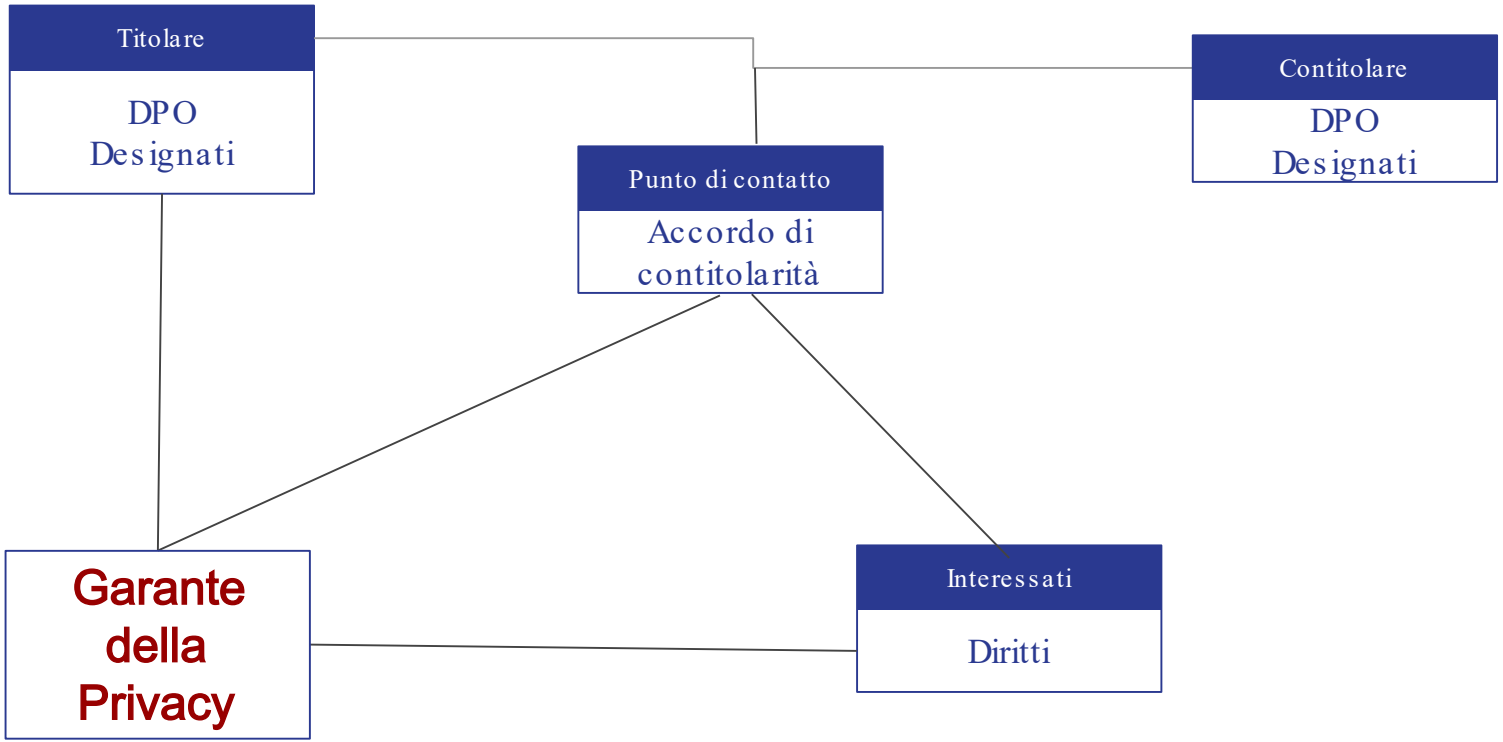
Accordo

Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità … Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

Diritti disgiunti

l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento.

Titolare e contitolare



DPO-RPD
(responsabile protezione dati)

Responsabile della protezione dei dati DPO/RPD

DPO obbligatorio	DPO obbligatorio	DPO obbligatorio
il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;	le attività principali consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala	le attività principali consistono nel trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e a reati

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

Esempio di comunicazione dati DPO

Si comunica inoltre che ai fini dell'applicazione del regolamento UE 679/2016 è stato designato con atto XXXXXX quale **Responsabile della Protezione dei dati RPD dell'Ente/Istituto/Comune il dott. XYZ.**

DATI DI CONTATTO Responsabile della Protezione dei dati [RPD]

- **Telefono** - 1111111111
- **Cellulare** - 33333333333
- **e mail -** email@del.dpo
- **pec** – email.del.dpo@pec.it

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)	Titolare-Responsabile	Sub-responsabile
la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali **per conto del titolare** del trattamento	ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate ...	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

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.

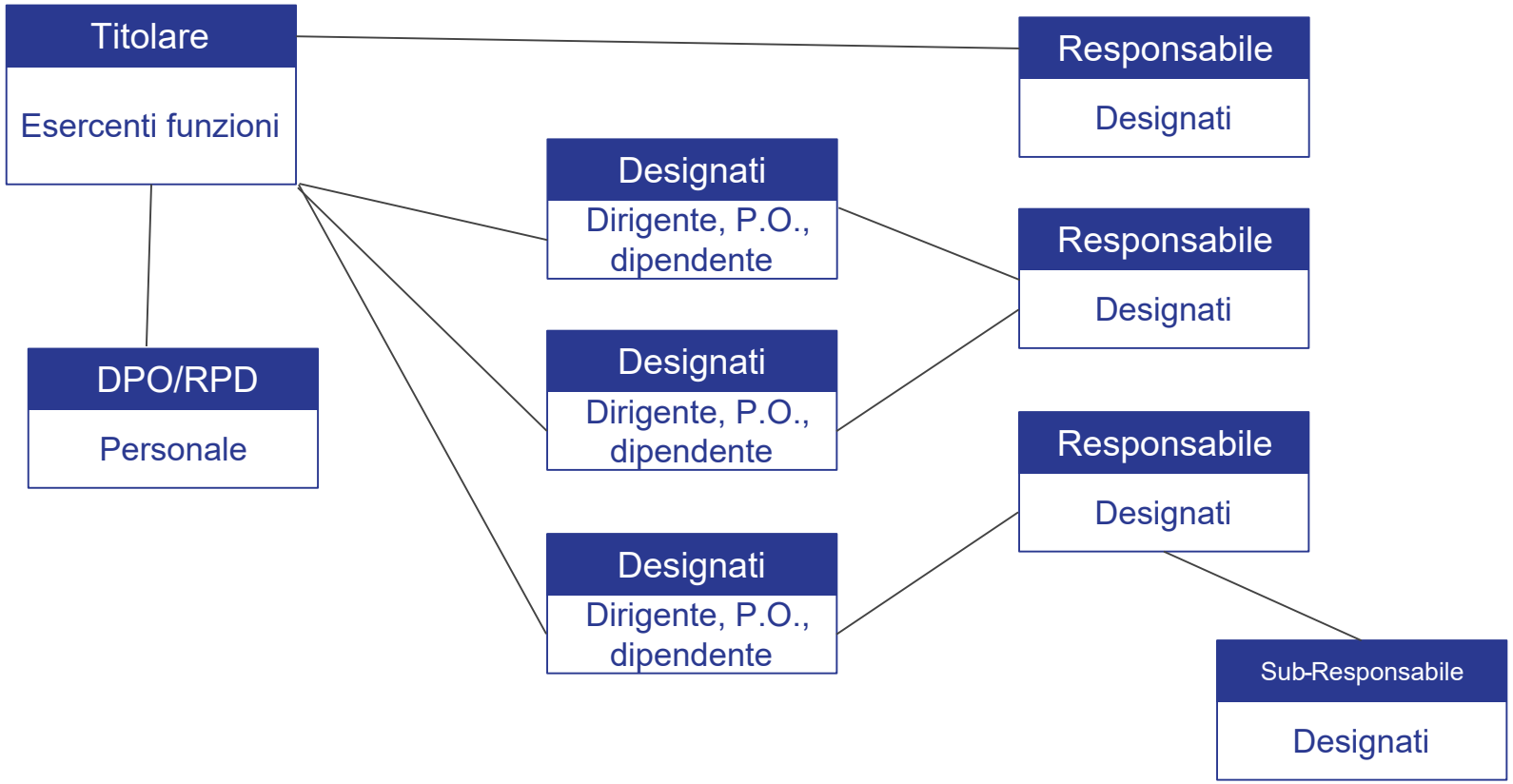
Responsabile

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.

Titolare - Responsabile - Designati



DESIGNATI
(interni)

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

Chi sono	Cosa fanno	Come designarli
Il **titolare** **o** il **responsabile** del trattamento **possono** prevedere … **persone fisiche**, **espressamente** designate, che operano sotto la loro **autorità**	**specifici compiti e funzioni** connessi al trattamento di dati personali	Il titolare o il responsabile del trattamento individuano le **modalita' piu' opportune**

PRINCIPI

(GDPR)

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

«liceità, correttezza e trasparenza»	«limitazione della finalità»	«minimizzazione dei dati»
Liceità Correttezza Trasparenza	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	adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati

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

«Esattezza»	«limitazione della conservazione»	«integrità e riservatezza»
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	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; 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	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.

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 comprovarlo («responsabilizzazione»).

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

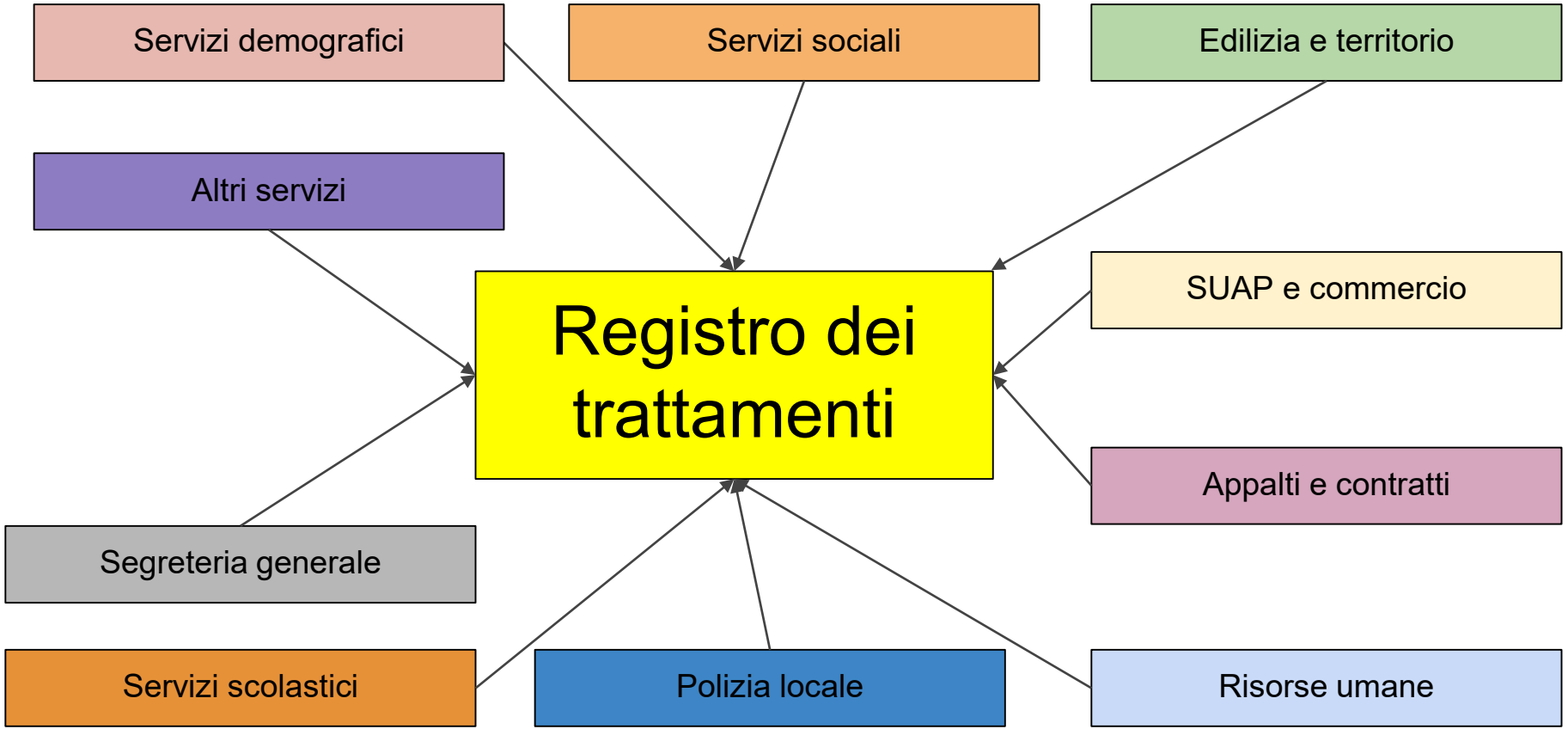
a disposizione dell'autorità di controllo

GDPR (art. 30)

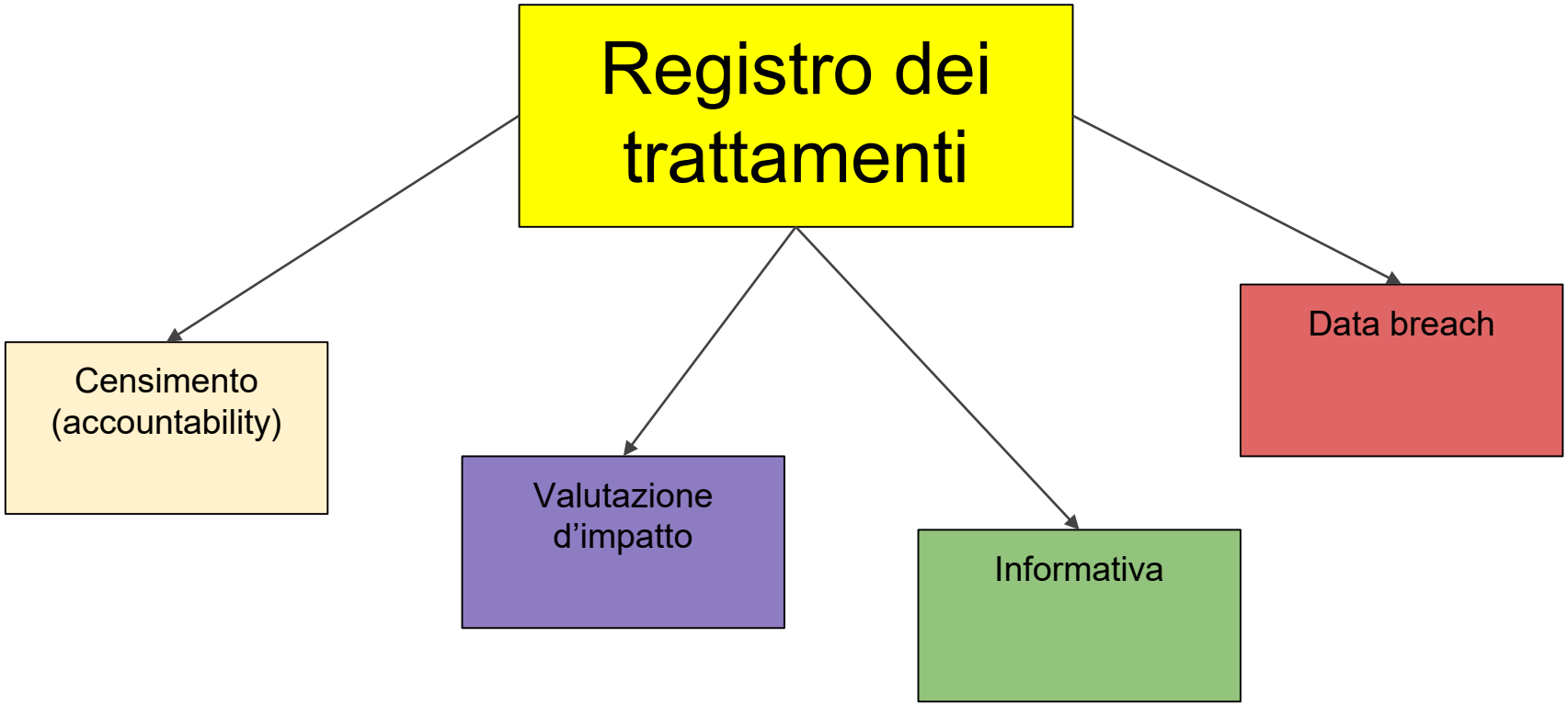
+ di 250 dipendenti,

- **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+-+FAQ+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).

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 nonchè, 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 nonchè 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

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

LICEITA' DEL TRATTAMENTO

Liceità del trattamento

Art. 6
regolamento UE 2016/679

- 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;

Liceità del trattamento

Art. 6
regolamento UE 2016/679

- 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;
- il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
- il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

Liceità del trattamento

Art. 6
regolamento UE 2016/679

- 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;
- 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.

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*) ogniqualvolta 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.

Valutazione d'impatto

Esempi

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

DIRITTI

Diritti dell’interessato (art. 12)

GDPR (art. 12)	1 mese	“Rompiscatole”
Il titolare del trattamento agevola l'esercizio dei diritti dell'interessato	Il titolare del trattamento fornisce all'interessato le informazioni relative all'azione intrapresa **senza ingiustificato ritardo** e, comunque, al più tardi entro **un mese** dal ricevimento della richiesta stessa	Se le richieste dell'interessato sono **manifestamente infondate, eccessive, ripetitive** : a) addebita un contributo b) rifiuta di soddisfare la richiesta

Diritti dell'interessato

regolamento UE 2016/679

- 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)

Diritti dell'interessato

regolamento UE 2016/679

- 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-undecies (Limitazioni ai diritti dell'interessato)

Diritti (artt. 15-22)	Dati	Forma
Diritto di accesso Diritto di rettifica Diritto alla cancellazione («diritto all'oblio») Diritto di limitazione di trattamento Diritto alla portabilità Diritto di opposizione	con **richiesta** al titolare del trattamento ovvero con **reclamo**	... puo', in ogni caso, essere ritardato, limitato o escluso con comunicazione motivata e resa senza ritardo In tali casi, i diritti dell'interessato possono essere esercitati anche tramite il Garante

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

Diritti (artt. 15-22)	Dati - soggetti	Blocco
Diritto di accesso Diritto di rettifica Diritto alla cancellazione («diritto all'oblio») Diritto di limitazione di trattamento Diritto alla portabilità Diritto di opposizione	dati personali concernenti persone decedute da chi ha un **interesse proprio**, o agisce **a tutela** dell'interessato, in qualita' di suo **mandatario**, o per ragioni **familiari** meritevoli di protezione.	nei **casi previsti dalla legge** … o (servizi web) l'interessato lo ha **espressamente vietato** con dichiarazione scritta presentata al titolare del trattamento o a quest'ultimo comunicata

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 **specifica** , **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.

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

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)