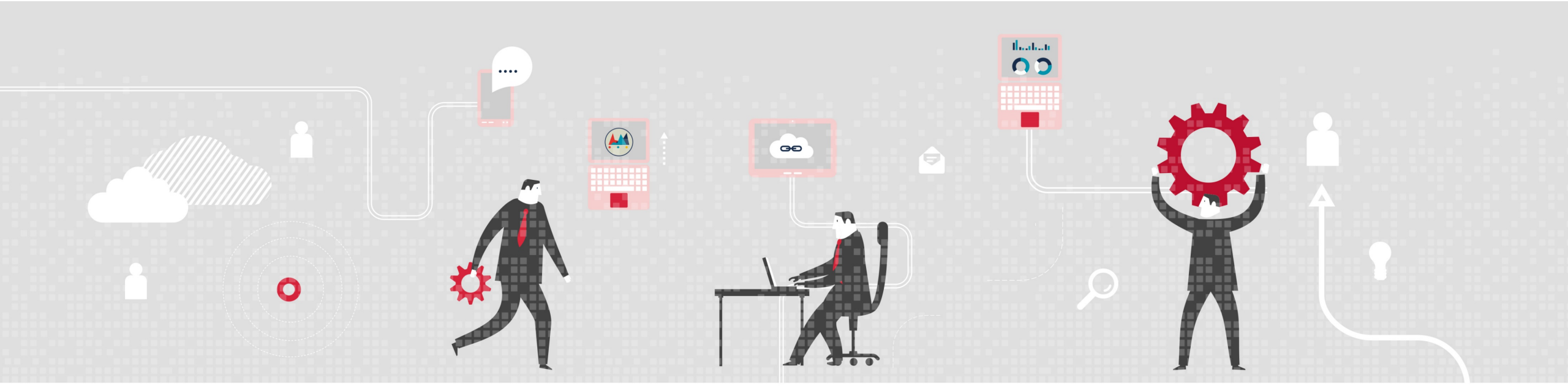
P4I

PARTNERS4INNOVATION



D.LGS. 10 AGOSTO 2018, N.101 IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

16 ottobre 2018

AGENDA

- Chi siamo
- Sicurezza Informatica & Privacy: lo scenario italiano
- Inquadramento del Decreto
- Approfondimento aspetti rilevanti del Decreto
- Impatti del Decreto sulle aziende: cosa succede adesso
- Domande e risposte

Sicurezza Informatica & Privacy: lo scenario italiano

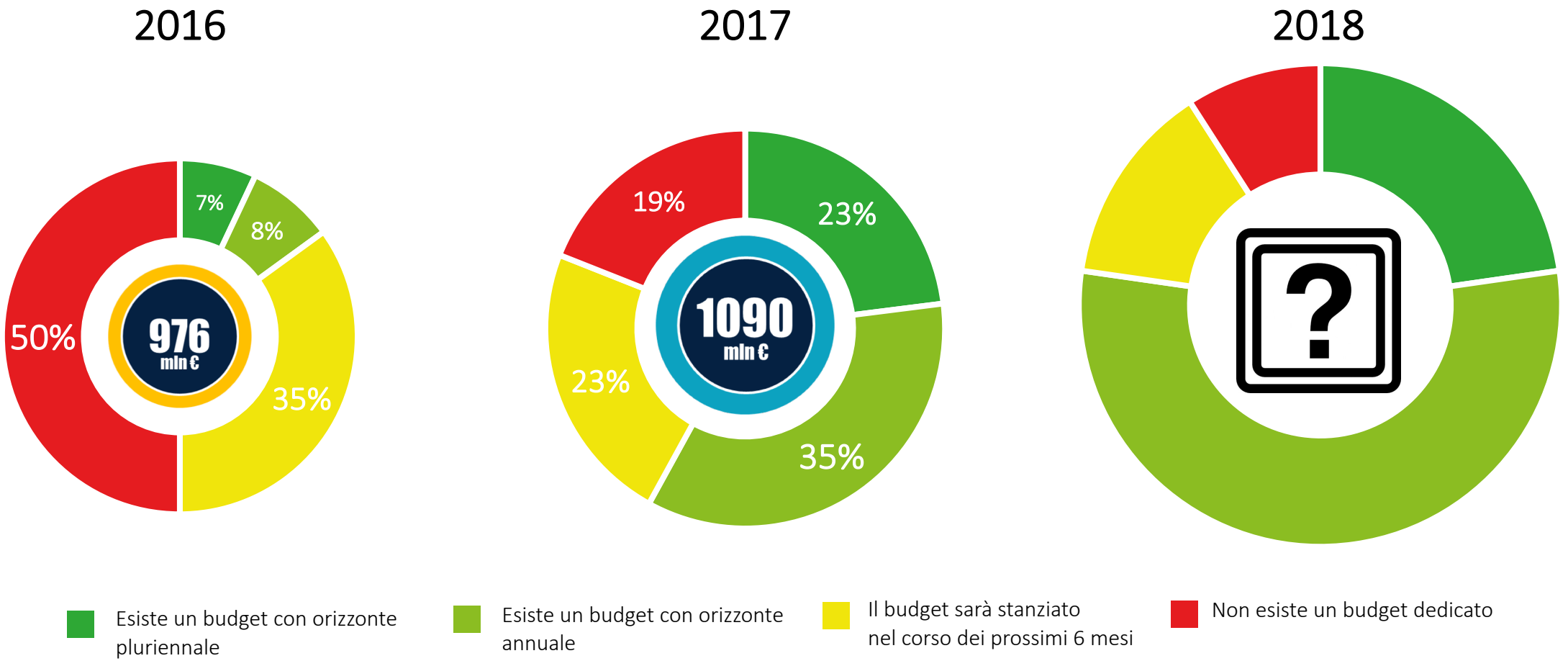
Cosa è successo nel 2017…

Sicurezza informatica & Privacy: lo scenario italiano

…e nel 2018

Cambridge Analytica

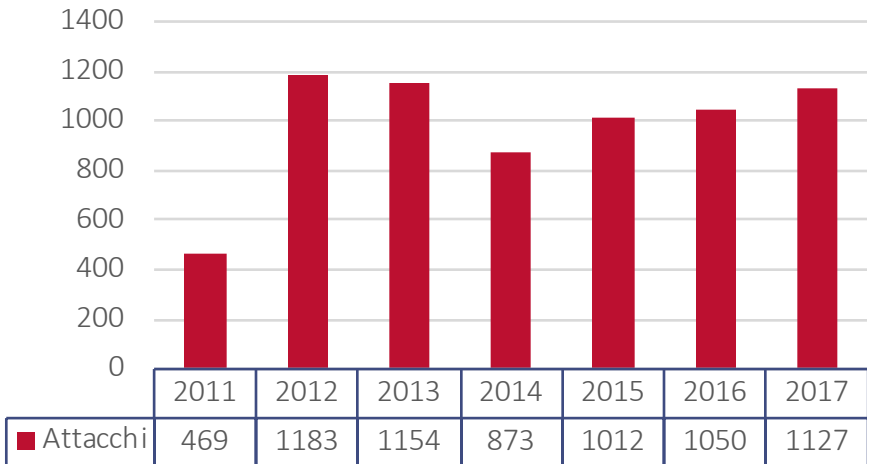
La crescita del budget in Information Security



Campione: 160 grandi imprese

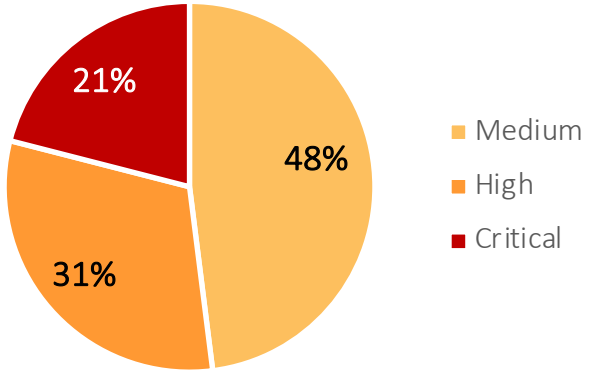
Sicurezza informatica & Privacy: lo scenario italiano

La crescita degli attacchi di dominio pubblico



6.865 attacchi dal 01/2011 al 12/2017

83 attacchi medi mensili (94/mese nel 2017)



21% degli attacchi aventi impatto critico

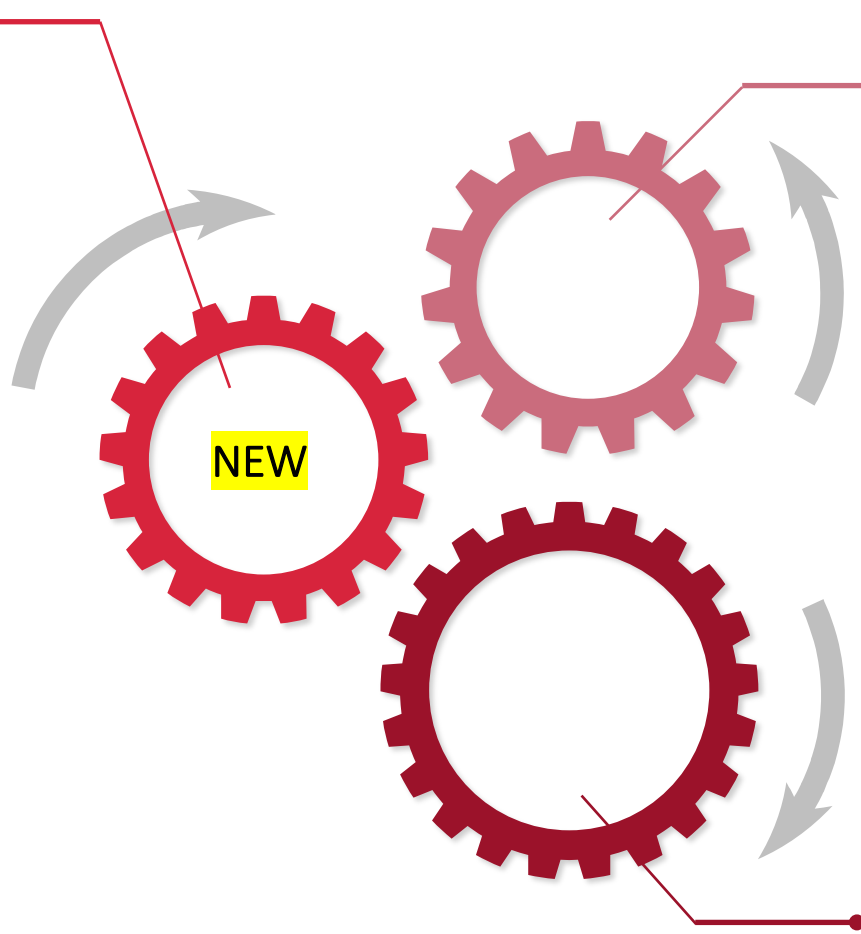
Inquadramento del decreto

D.lgs. 10 agosto 2018, n.101 in materia di protezione dei dati personali

Cos'è?

Decreto legislativo 10 agosto 2018, n.101

- Il decreto legislativo è finalizzato ad adeguare il quadro normativa nazionale alle disposizioni del GDPR 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
- In relazione all'elaborazione di questo testo è stata istituita una commissione di studio con decreto del Ministro del 14 dicembre 2017, che ha potuto incominciare i lavori il 4 gennaio 2018. Com'è noto, il GDPR è direttamente applicabile dal 25 maggio 2018. L'adeguamento dell'ordinamento italiano deve essere coerente temporalmente con tale data e dunque la commissione ha potuto operare in un tempo limitato
- La legge di delegazione europea n. 163 del 2017 ha quindi stabilito all'art. 13 comma 3, i criteri della delega



Regolamento (UE) 2016/679 (GDPR)

Decreto legislativo 196/2003 (Codice Privacy)

D.lgs. 10 agosto 2018, n.101 in materia di protezione dei dati personali

Come è nato?

24 maggio 2016
Entrata in vigore del Regolamento n. 679/2016

21 novembre 2017
Entrata in vigore Legge di delegazione Europea 2016-2017

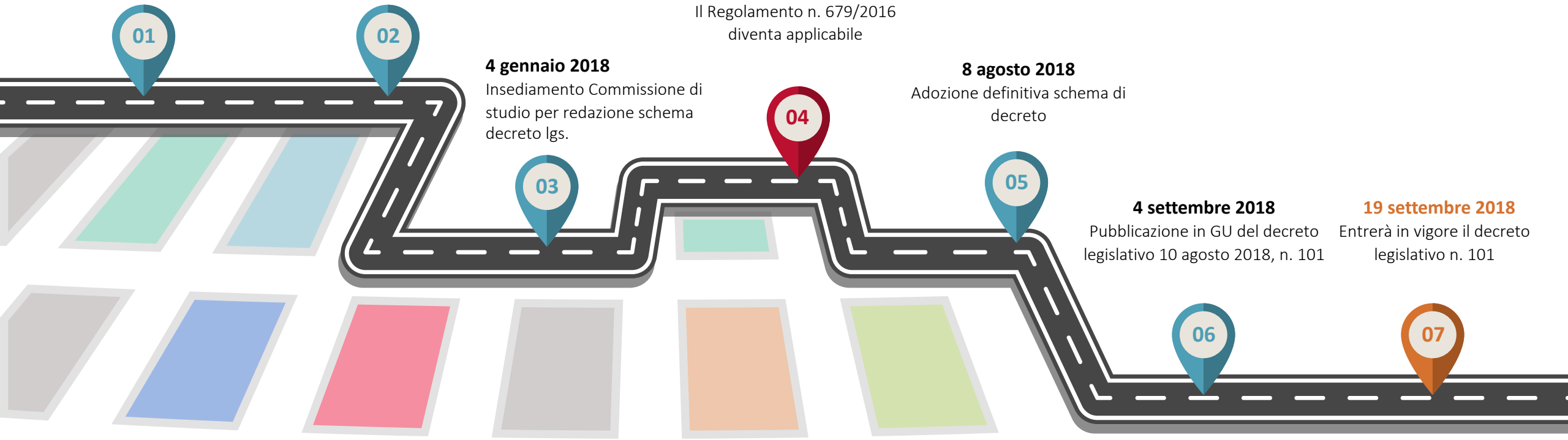
25 maggio 2018
Il Regolamento n. 679/2016 diventa applicabile

4 gennaio 2018
Insediamento Commissione di studio per redazione schema decreto lgs.

8 agosto 2018
Adozione definitiva schema di decreto

4 settembre 2018
Pubblicazione in GU del decreto legislativo 10 agosto 2018, n. 101

19 settembre 2018
Entrerà in vigore il decreto legislativo n. 101



D.lgs. 10 agosto 2018, n.101 in materia di protezione dei dati personali

Cosa ha fatto il Governo?

AZIONE 3

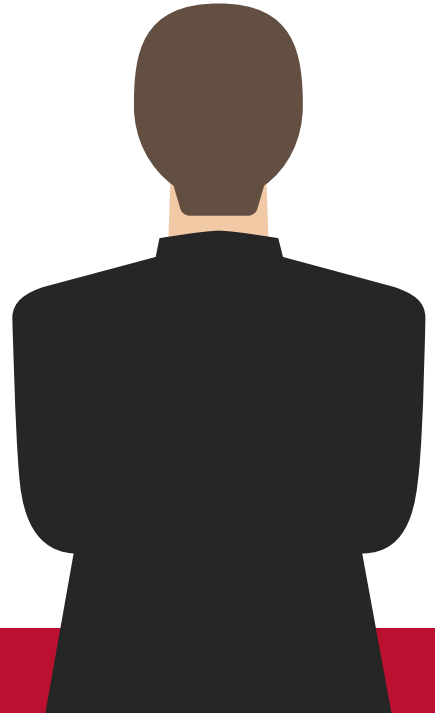
Coordinare le disposizioni vigenti in materia di protezione dei dati personali con le disposizioni recate dal GDPR

AZIONE 2

Modificare il Codice limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel GDPR

AZIONE 4

Prevedere il ricorso a **specifici provvedimenti attuativi e integrativi** adottati dal Garante nell'ambito e per le finalità previsti dal GDPR



AZIONE 1

Abrogare espressamente le disposizioni del Codice Privacy (d.lgs. 196/2003 - «Codice») incompatibili con le disposizioni contenute nel GDPR

AZIONE 5

Adeguare il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del GDPR

Perché si è reso necessario?

Il GDPR

- è direttamente applicabile in tutti gli Stati membri
- non necessita di alcuna legge statale di recepimento
- prevede espressamente la possibilità, per ciascuno Stato Membro, di disciplinare autonomamente determinati ambiti

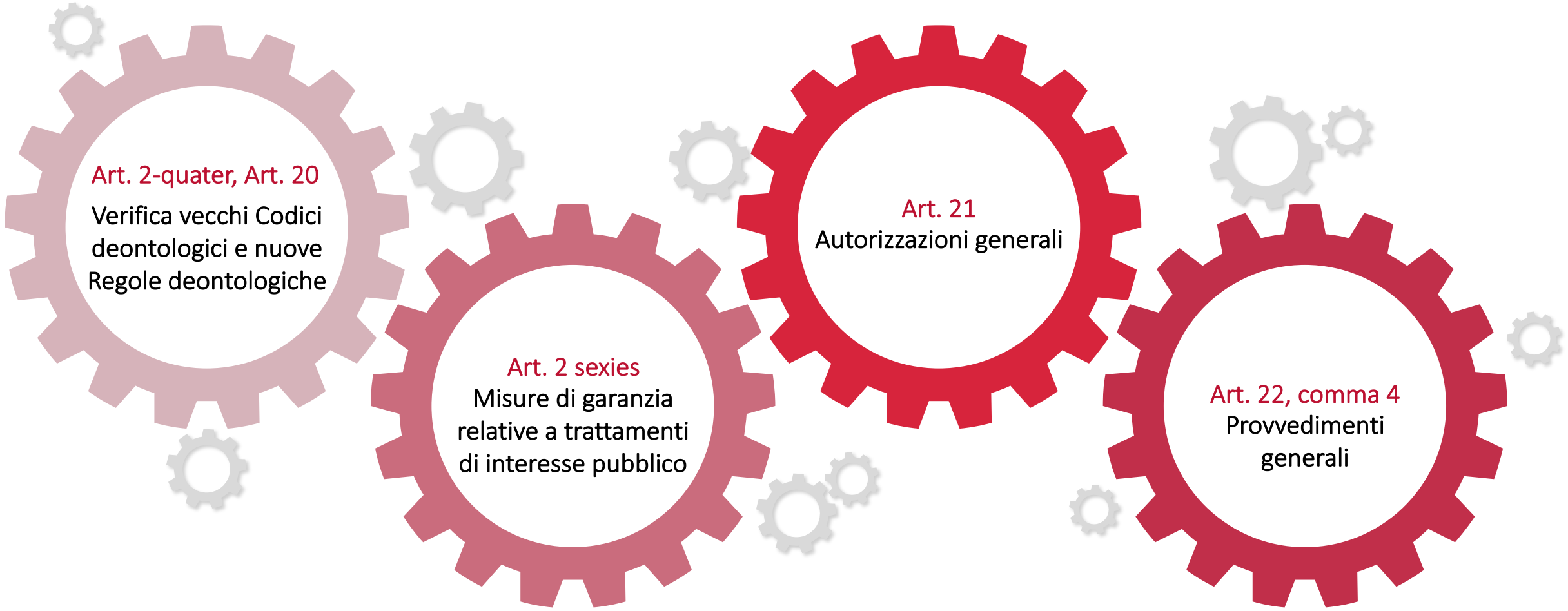
Il D.lgs. 10 agosto 2018, n.101

- va a disciplinare quegli ambiti che il Regolamento permette a ciascuno Stato di normare in autonomia (si è reso necessario perché il Regolamento ha concesso tale ulteriore adempimento)
- armonizzare le previsioni del Codice Privacy al GDPR

D.lgs. 10 agosto 2018, n.101 in materia di protezione dei dati personali

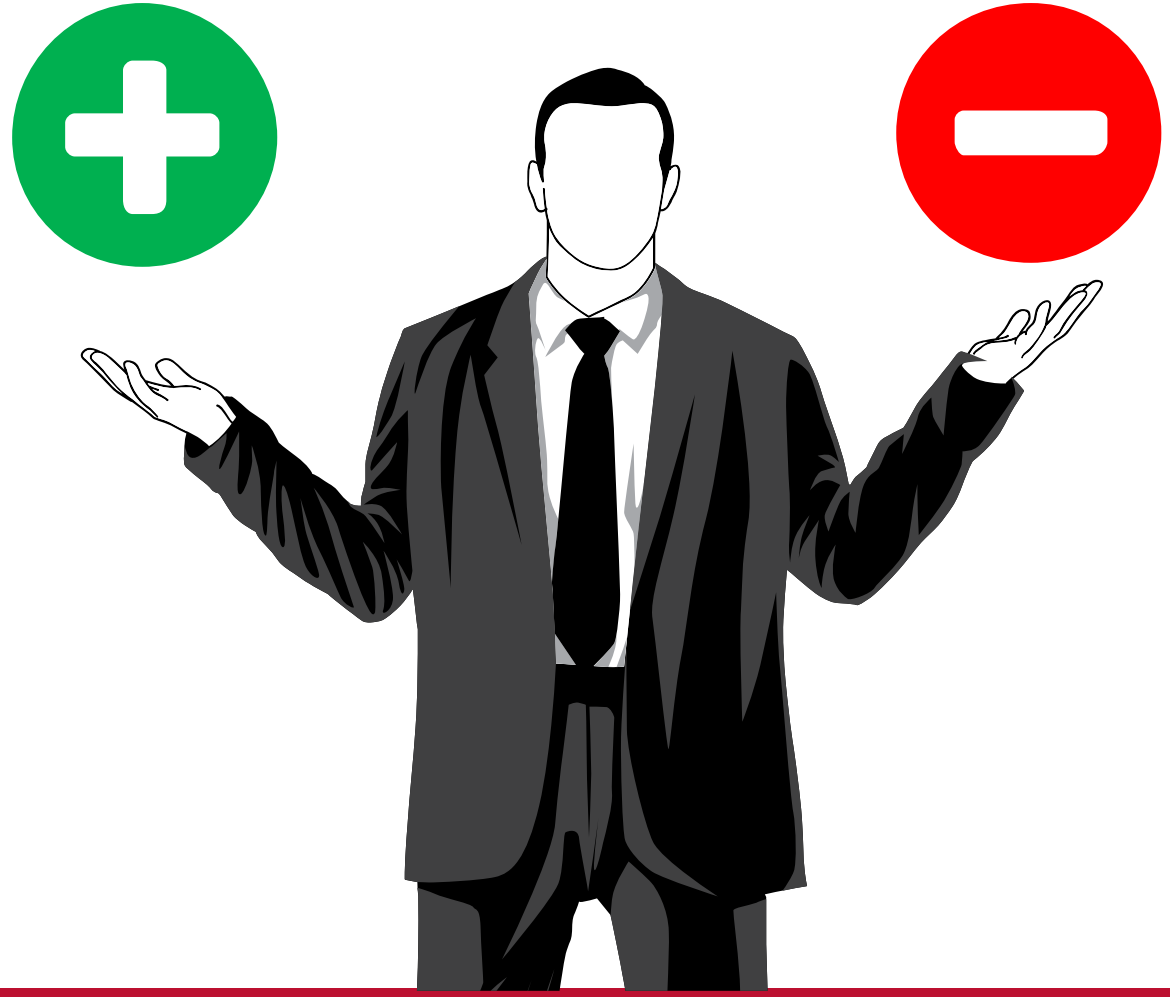
Quali sono gli ambiti in cui il GDPR consente spazi di manovra?

Quale ruolo ricoprirà il Garante per la protezione dei dati personali?



Quale ruolo ricoprirà il Garante per la protezione dei dati personali?

Al Garante vengono attribuiti ampi e significativi poteri di ***soft law*** che permetteranno di favorire una maggiore flessibilità nell'adeguamento della normativa alle reali esigenze concrete (ad es. per innovazioni tecnologiche)



Un'eventuale inadempienza porterebbe a situazioni poco chiare (ad es. sopravvivenza di norme del vecchio Codice espressamente abrogate)

D.lgs. 10 agosto 2018, n.101 in materia di protezione dei dati personali

Quali sono gli articoli abrogati?

a) alla parte I (Disposizioni Generali):
   1. gli articoli 3, 4, 5 e 6;
   2. il titolo II → Diritti dell'interessato
   3. il titolo III → Regole generali per il trattamento dei dati
   4. il titolo IV → Soggetti che effettuano il trattamento
   5. il titolo V → Sicurezza dei dati e dei sistemi
   6. il titolo VI
   7. il titolo VII

b) alla parte II:
   1. il capo I del titolo I (Profili generali dei trattamenti in ambito giudiziario)
   2. i capi III, IV e V del titolo IV (Trattamenti in ambito pubblico)
   3. gli articoli 76, 81, 83 e 84
   4. il capo III del titolo V (Trattamento di dati sanitari per finalità di rilevante interesse pubblico)
   5. gli articoli 87, 88 e 89 (Prescrizioni mediche)
   6. il capo V del titolo V (Dati Genetici)
   7. gli articoli 91, 94, 95, 98, 112, 117, 118 e 119
   8. i capi II e III del titolo X, il titolo XI e il titolo XIII (**Marketing Diretto**)

c) alla parte III:
   1. la sezione III del capo I del titolo I;
   2. gli articoli 161, 162, 162-bis, 162-ter, 163, 164, 164-bis,165 e 169
   3. gli articoli 173, 174, 175, commi 1 e 2, 176, 177, 178 e 179
   4. il capo II del titolo IV
   5. gli articoli 184 e 185

d) ALLEGATO B

e) allegato C

Viene espressamente abrogato tutto il titolo sulle misure di sicurezza, disciplinate unicamente dal GDPR

Non esistono più le misure minime di sicurezza elencate nell'allegato B del Codice

Anche gli articoli 53, 54, 55 e 56 del Codice sono stati abrogati recentemente dal decreto legislativo 18 maggio 2018, n. 51.

D.lgs. 10 agosto 2018, n.101 in materia di protezione dei dati personali

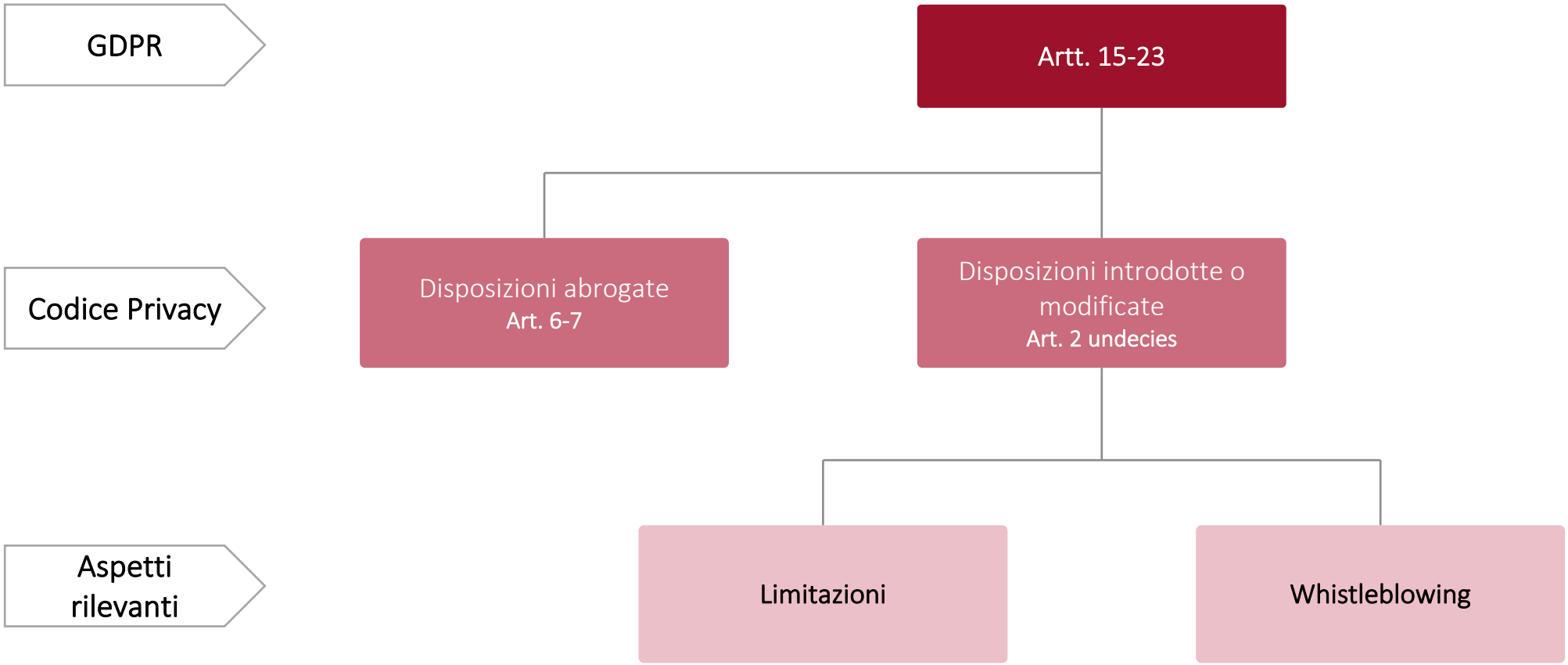
Quali sono gli aspetti più rilevanti per voi?

- **Diritti dell'interessato**
  - Limitazioni ai diritti
  - Whistleblowing
  - Diritti riguardanti persone decedute
- **Titolare e responsabile del trattamento**
  - Designati
  - Trattamento che presenta elevati rischi per l'esecuzione di un compito di interesse pubblico
- **Trattamenti nell'ambito del rapporto di lavoro**
  - Raccolta dei CV
  - Divieto di indagine e controllo a distanza dei lavoratori
  - Smart Working
- **Consenso del minore per servizi società dell'informazione**
  - Età minima per prestare consenso
  - Consenso dal Titolare della responsabilità genitoriale
  - Informativa chiara e semplice
- **Condizioni e misure di garanzia**
  - Dati biometrici
  - Dati genetici
  - Dati relativi allo stato di salute
- **Principi per trattamento dati relativi a condanne e reati**
  - Condizioni per il trattamento
  - Ambiti soggetti ad autorizzazione di legge o di Regolamento
- **Principi**
  - Trattamento per l'esecuzione di un compito di pubblico interesse o connesso all'Esercizio di pubblici poteri
  - "Comunicazione" e "Diffusione"
  - Regole deontologiche
  - Trattamento di categorie particolari di dati necessario per motivi di interesse pubblico rilevante
- **Tutela dell'interessato**
  - Tutela amministrativa e giurisdizionale
  - Tutela dinnanzi al Garante
  - Tutela giurisdizionale
  - Poteri e compiti del Garante
- **Sanzioni**
  - Sanzioni amministrative
  - Sanzioni penali
  - Sanzioni nei primi 8 mesi

Diritti dell’interessato (Parte 1, Titolo 1 Capo III)

Diritti dell'interessato (Parte 1, Titolo 1 Capo III, 2 undecies)

Quali sono gli aspetti più rilevanti per voi?



Limitazioni ai diritti (1/2)

Codice Privacy

Il D. Lgs. 196/2003 riconosceva all'interessato una serie di **diritti.**

- ACCESSO
- RETTIFICA
- OPPOSIZIONE
- CANCELLAZIONE

GDPR

Il GDPR amplia i diritti degli interessati (artt. da 15 a 22):

- ACCESSO
- RETTIFICA
- CANCELLAZIONE (OBLIO)
- OPPOSIZIONE
- LIMITAZIONE
- NON ESSERE SOTTOPOSTO A DECISIONI BASATE UNICAMENTE SUL TRATTAMENTO AUTOMATIZZATO
- PORTABILITÀ

Disposizioni introdotte da D.lgs 101/2018

- Il D. Lgs. 101/2018 recepisce i diritti riconosciuti all'interessato dal GDPR
- Non apporta modifiche ulteriori a tali diritti
- Introduce alcune novità con riferimento alle limitazioni all'esercizio degli stessi

Limitazioni ai diritti (2/2)

Codice Privacy

Il D. Lgs. 196/2003 prevede che i diritti riconosciuti all'interessato possono essere limitati qualora l'esercizio degli stessi comporti un **pregiudizio effettivo e concreto ad altri interessi normativamente tutelati**

GDPR

Il GDPR prevede che il diritto dell'Unione o dello Stato membro possa limitare, mediante misure legislative, la portata degli obblighi e dei diritti dell'interessato

Tale limitazione deve:

- rispettare l'essenza dei diritti e delle libertà fondamentali degli interessati
- essere una misura necessaria e proporzionata per salvaguardare una serie di interessi meritevoli di tutela
- essere attuata con disposizioni specifiche (es. finalità del trattamento)

Disposizioni introdotte da D.lgs 101/2018

Il D. Lgs. 101/2018 introduce un ulteriore interesse normativamente meritevole di tutela: garantire la riservatezza dell'identità del dipendente che segnala, ai sensi della legge 30 novembre 2017, n. 179 (legge sul whistleblowing), l'illecito aziendale di cui sia venuto a conoscenza in ragione del proprio ufficio

Limitazioni ai diritti - Whistleblowing

Interessi meritevoli di tutela ai sensi dell'art. 2-undecies

a. ANTIRICILAGGIO

b. SOSTEGNO A VITTIME DI RICHIESTE ESTORSIVE

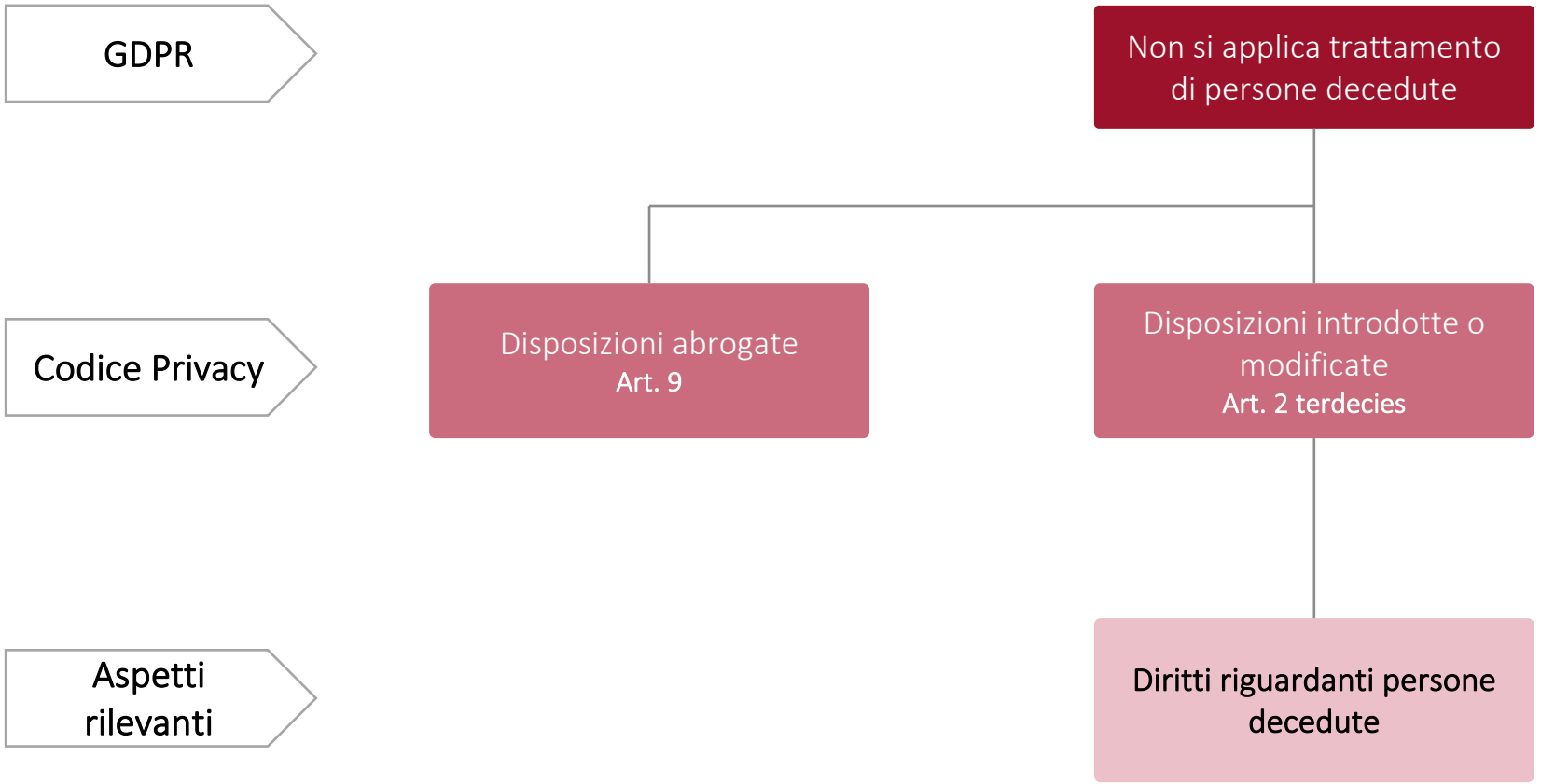
c. ATTIVITÀ SVOLTA DA COMMISSIONI PARLAMENTARI DI INCHIESTA

d. POLITICA MONETARIA E VALUTARIA, PAGAMENTI, CONTROLLO DEGLI INTERMEDIARI E MERCATI CREDITIZI E FINANZIARI

e. TUTELA DEL WHISTLEBLOWER

Diritti dell'interessato (Parte 1, Titolo 1 Capo III, 2 terdecies)

Quali sono gli aspetti più rilevanti per voi?



Esercizio di diritti riguardanti persone decedute (1/2)

Codice Privacy	Disposizioni introdotte da D.lgs 101/2018
Il D. Lgs. 196/2003 stabiliva che tali diritti avrebbero potuto essere esercitati «da chi ha un **interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione**»	Il D. Lgs. 101/2018: • **riprende la normativa previgente**, con riferimento ai **soggetti** che possono esercitare i diritti riguardanti dati personali di persone decedute, ovvero: - i prossimi congiunti che abbiano ragioni familiari meritevoli di protezione - gli esecutori testamentari - chiunque dimostri di avere un interesse proprio a difesa dei diritti patrimoniali • **introduce una novità**, prevedendo che l'**esercizio** di tali diritti possa essere **vietato o limitato** dall'interessato, relativamente **all'offerta diretta di servizi della società dell'informazione**

Esercizio di diritti riguardanti persone decedute (2/2)

Codice Privacy	Disposizioni introdotte da D.lgs 101/2018
Il D. Lgs. 196/2003 stabiliva che tali diritti avrebbero potuto essere esercitati «da chi ha un **interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione**»	• Il divieto o limitazione dell'esercizio di diritti riferibili a dati personali riguardanti una persona deceduta: o deve essere espresso attraverso dichiarazione scritta presentata o comunicata da parte dell'interessato al Titolare del trattamento o deve risultare in modo non equivoco ed essere frutto di una volontà specifica, libera e informata dell'interessato o può riguardare solo alcuni dei diritti di cui agli articoli da 15 a 22 del GDPR • La norma opera un bilanciamento di interessi tutelando: o il diritto dell'interessato a non vedere divulgati dopo il suo decesso dati personali (anche digitali) o i diritti di terzi per i quali il divieto o la limitazione all'esercizio di tali diritti potrebbe comportare una lesione dei diritti patrimoniali derivanti dalla morte dell'interessato o diritti di difesa in giudizio

Esercizio di diritti riguardanti persone decedute - Principali impatti

Il legislatore ha voluto riprendere la disciplina previgente, adeguandola al contesto e alle problematiche attuali quali, ad esempio, **questioni relative all'accesso ad account web, blog, portali, account di posta elettronica appartenenti ad una persona deceduta**

Dalla gestione del consenso alla governance del dato

Le recenti norme hanno introdotto la necessità di garantire i diritti degli interessati…

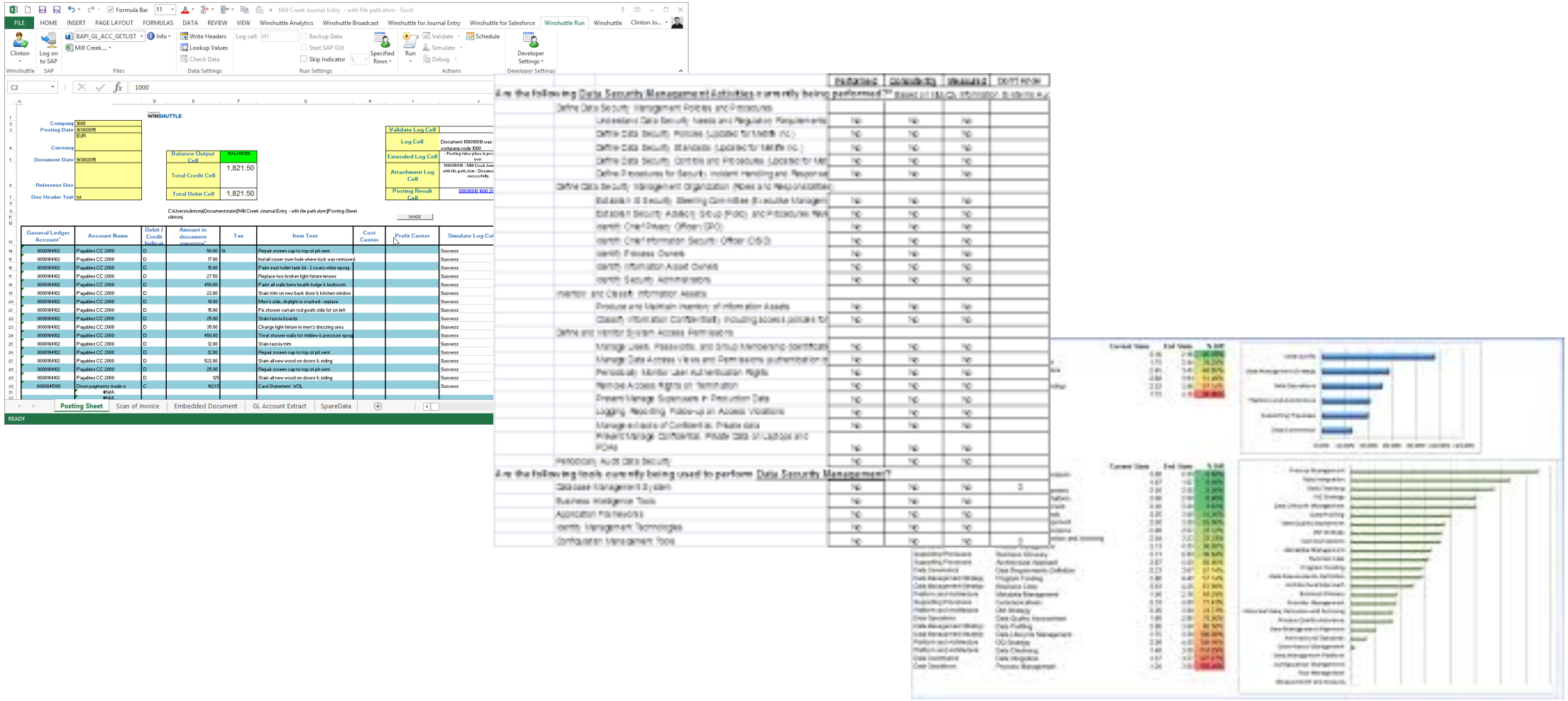
… concetto tanto semplice nella teoria quanto complesso nella pratica

Questo è vero se il nostro focus resta la gestione puntuale delle richieste di legge…

… se però spostiamo il focus sul dato e su una sua gestione sostenibile vediamo che ci sono software …

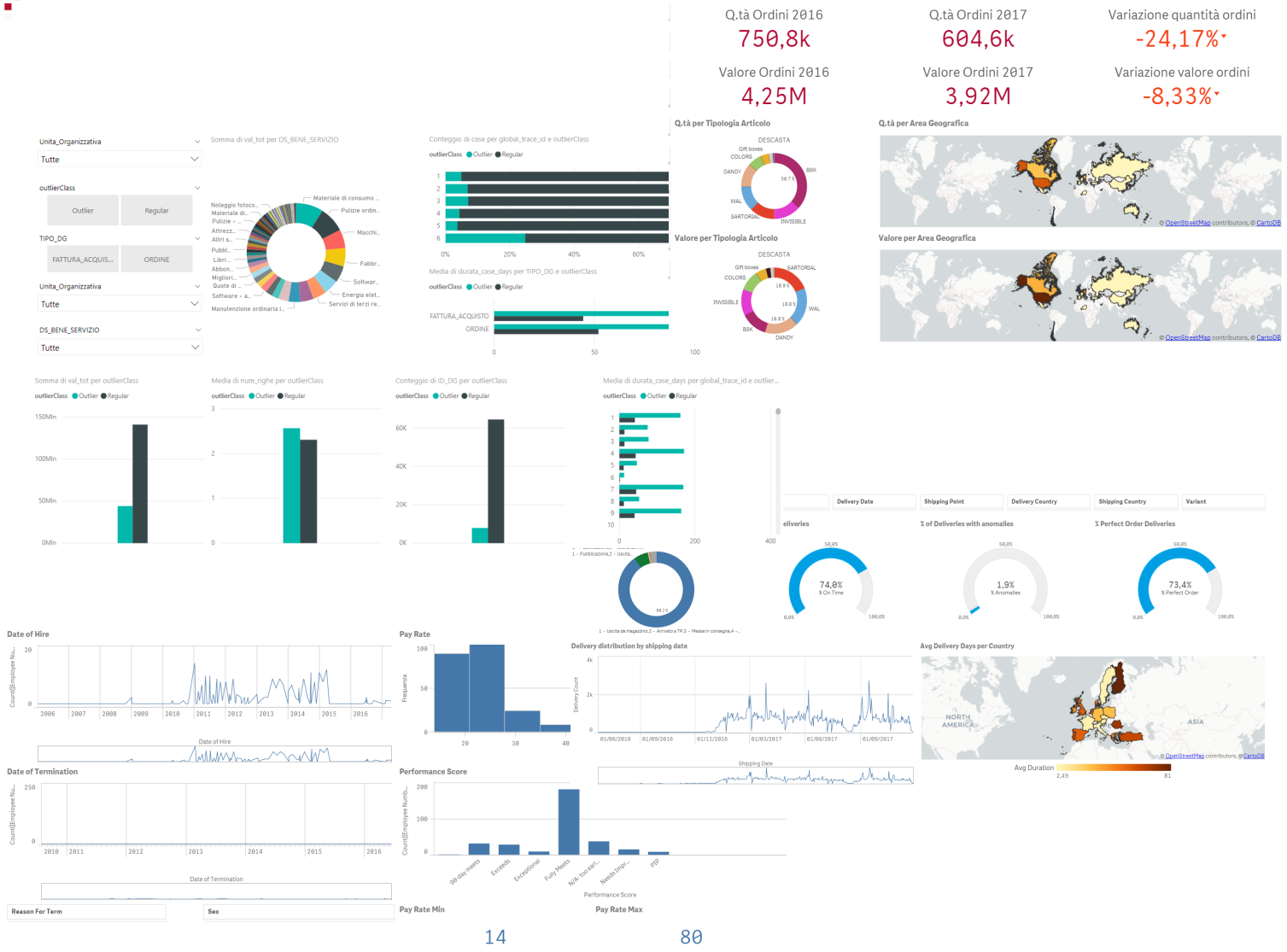
… metodologie …

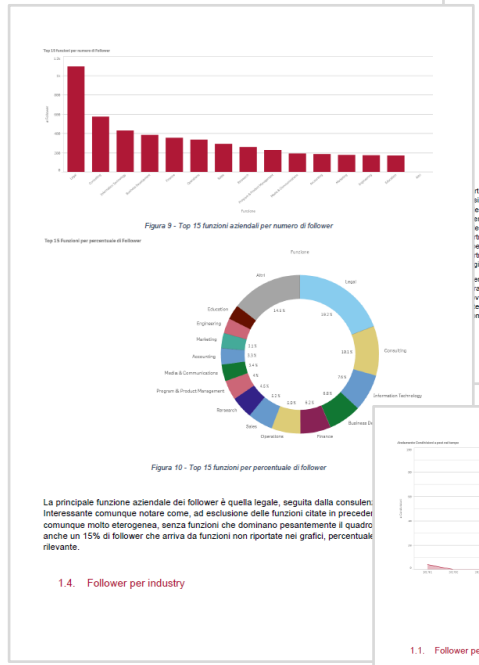
… e strumenti …

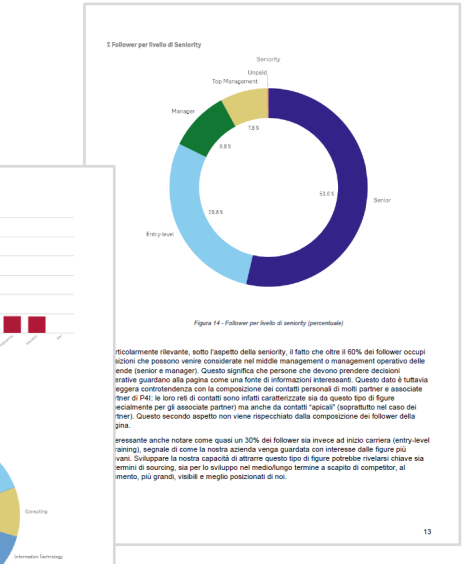


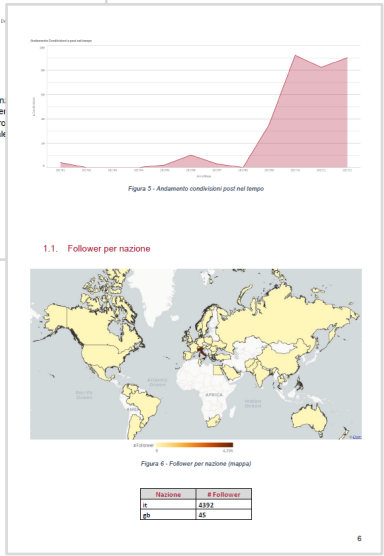
… che non solo ci garantiscono di adempiere agli obblighi normativi, ma anche di avere una maggior qualità dei dati …

… permettendoci di generare anche analytics che supportino più efficacemente le decisioni di business





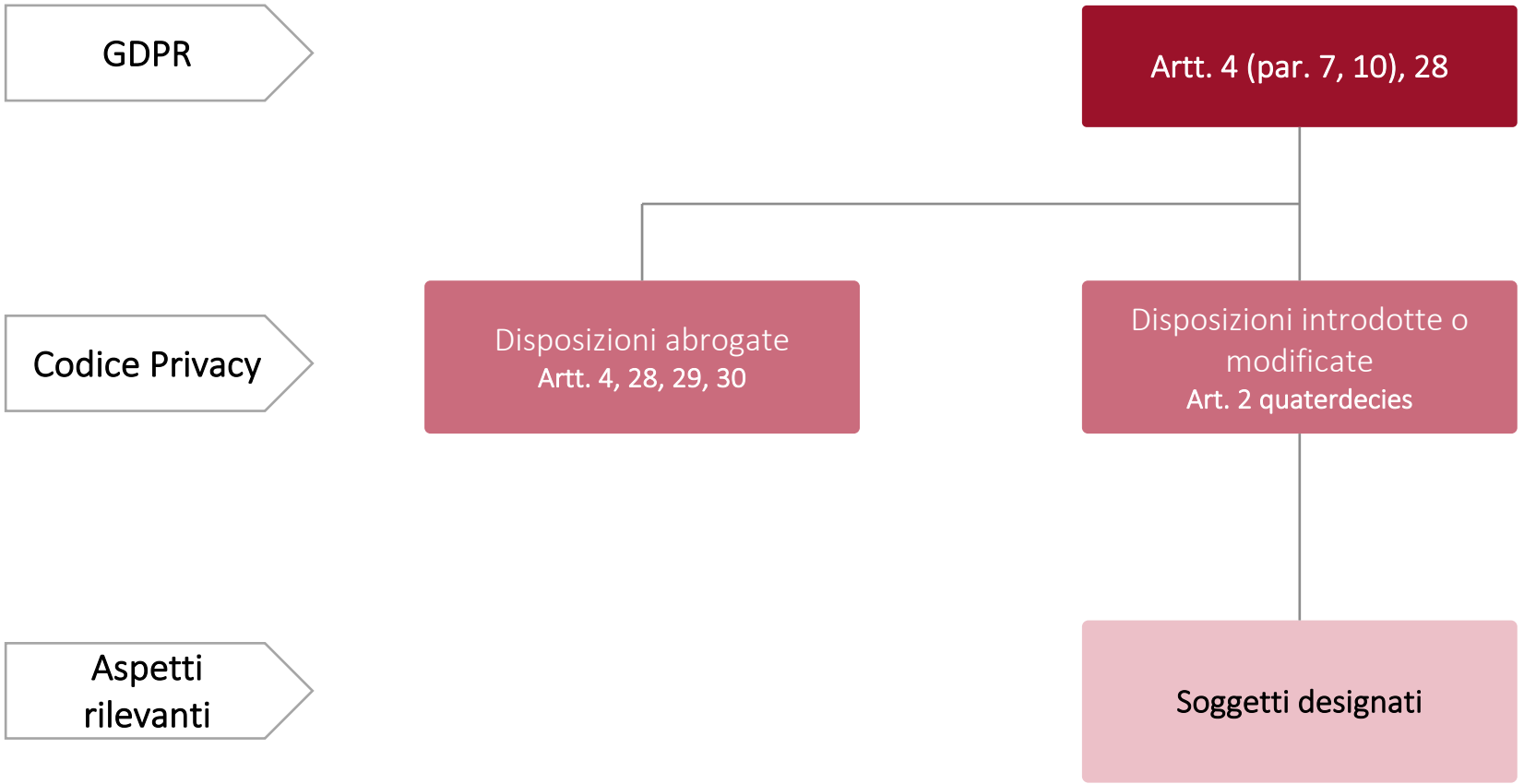




Titolare del trattamento e responsabile del trattamento (Parte 1, Titolo 1 Capo IV)

Titolare del trattamento e responsabile del trattamento (Parte 1, Titolo 1 Capo IV, 2 quaterdecies)

Quali sono gli aspetti più rilevanti per voi?



Titolare del trattamento e responsabile del trattamento (Parte 1, Titolo 1 Capo IV, 2 quaterdecies)

I ruoli nel Codice Privacy

- Il Titolare del trattamento è «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».

- Il Responsabile del trattamento è «la persona fisica, giuridica, l'autorità pubblica, il servizio o altro organismo che, tratta i dati personali per conto del titolare del trattamento».

- I soggetti «incaricati/autorizzati» sono figure (persone fisiche) che, sotto la responsabilità e nell'ambito dell'organizzazione del titolare del trattamento, svolgono specifici compiti e funzioni connessi al trattamento di dati personali

I nuovi ruoli Privacy - I soggetti designati

GDPR

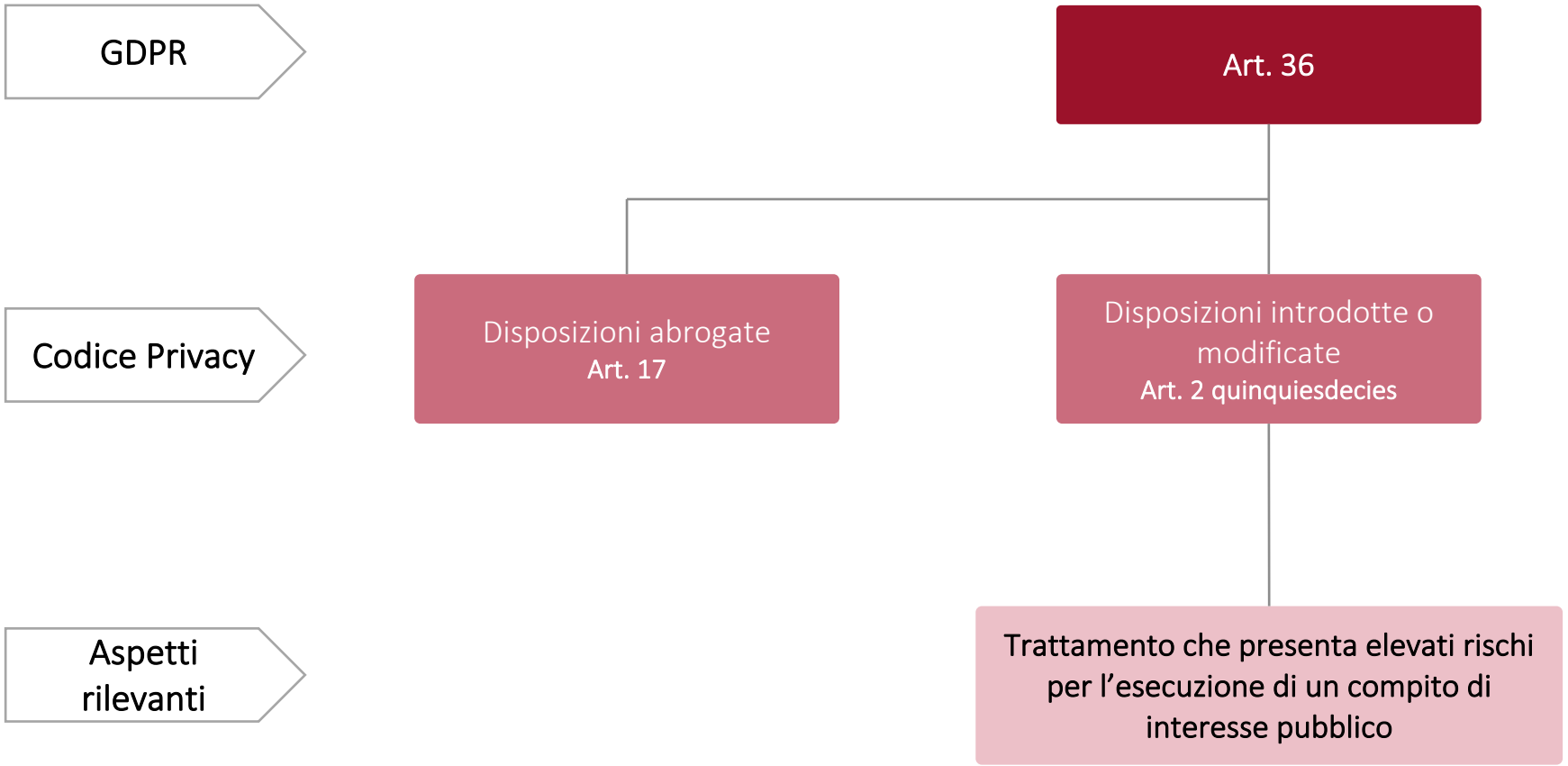
- La figura del responsabile del trattamento è esterna rispetto all'organizzazione aziendale.
- La figura autonoma dell'incaricato, introdotta dal D. Lgs. 196/2003, non è prevista nel GDPR e in nessun'altra delle legislazioni europee
- L'Autorità Garante della protezione dei dati, nella guida all'applicazione del Regolamento, considera la figura dell'incaricato non incompatibile con il regolamento

Disposizioni introdotte da D.lgs 101/2018

- La norma prevede il potere di titolare e responsabile di delegare compiti e funzioni a persone fisiche che operano sotto la loro autorità che dovranno essere espressamente **«designati»**
  - Come nel D. lgs. 196/2003, occorre un'indicazione analitica dei compiti e le funzioni assegnate a tali figure
  - Tali soggetti non devono essere chiamati «responsabili», che, ai sensi del GDPR, sono figure «esterne» rispetto al Titolare.
  - Spetta al titolare o al responsabile del trattamento individuare le modalità più opportune per l'autorizzazione del trattamento. È comunque consigliabile scegliere una modalità che consenta di dimostrare l'avvenuta autorizzazione

Titolare del trattamento e responsabile del trattamento (Parte 1, Titolo 1 Capo IV, 2 quinquiesdecies)

Quali sono gli aspetti più rilevanti per voi?



Diritti dell'interessato (Parte 1, Titolo 1 Capo III, 2 quinquiesdecies)

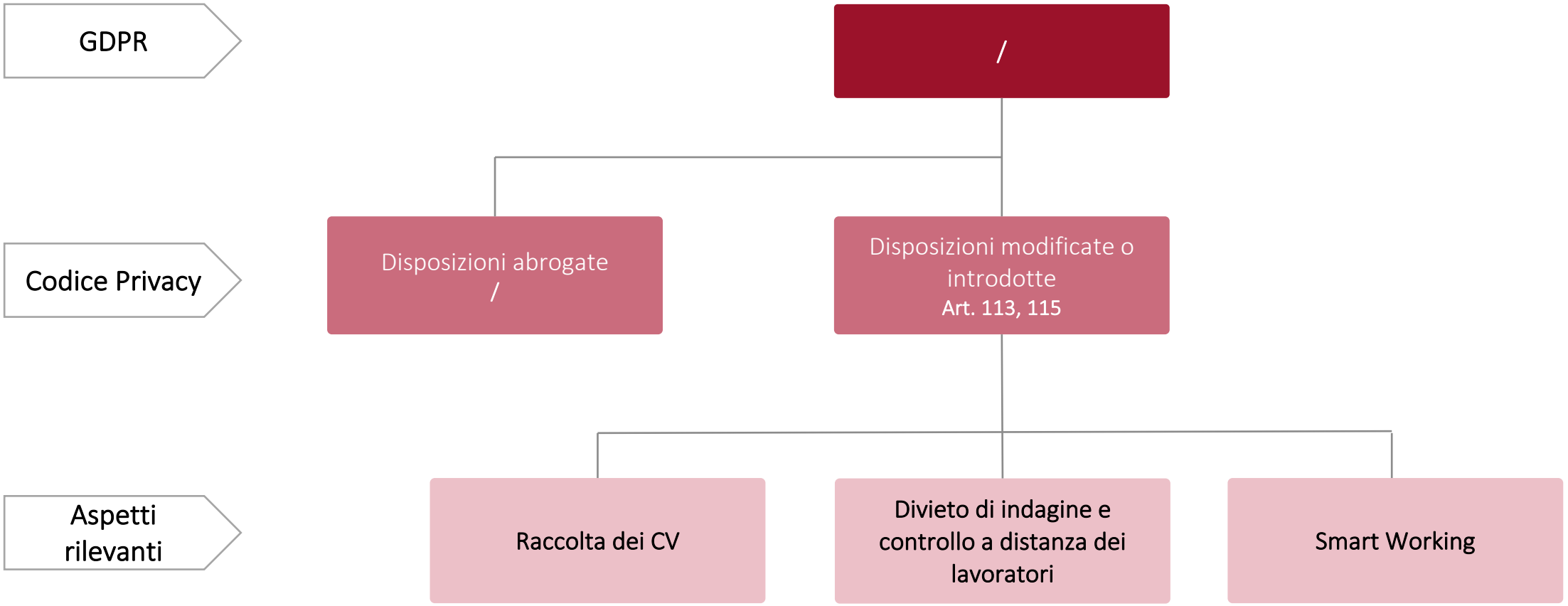
Trattamento che presenta elevati rischi per l'esecuzione di un compito di interesse pubblico

Codice Privacy	GDPR	Disposizioni introdotte da D.lgs 101/2018
Il D. Lgs. 196/2003 richiedeva un'istanza e una verifica preliminare dell'Autorità di controllo in presenza di trattamenti che presentavano rischi specifici per i diritti e per le libertà fondamentali, nonché per la dignità dell'interessato	Il GDPR prevede che: • il Titolare del trattamento può **consultare l'Autorità** qualora la **DPIA** indichi che il trattamento presenta un **rischio elevato** in assenza di misure adottate dal Titolare per attenuare il rischio • determina il **contenuto specifico** della comunicazione • lascia agli Stati membri la **possibilità di prescrivere che i Titolari consultino l'Autorità e ne ottengano l'autorizzazione preliminare**, in relazione al trattamento connesso all'esecuzione di un compito di interesse pubblico	Il D.Lgs. 101/2018 prevede che i trattamenti svolti per l'esecuzione di un compito di interesse pubblico, e che presentano rischi elevati, debbano ottenere **un'autorizzazione preventiva** da parte del **Garante** ai fini della loro legittimità.

Trattamenti nell’ambito del rapporto di lavoro (Parte 2, Titolo VIII)

Trattamenti nell'ambito del rapporto di lavoro (Parte 2, Titolo VIII)

Quali sono gli aspetti più rilevanti per voi?



Trattamenti nell'ambito del rapporto di lavoro (Parte 2, Titolo VIII)

Il quadro non cambia: raccolta dei CV

ART. 111-BIS

Le informazioni di cui all'articolo 13 del Regolamento (**INFORMATIVE**), nel caso di ricezione dei curricula spontaneamente trasmessi dagli interessati al fine della instaurazione di un rapporto di lavoro, vengono fornite **al momento del primo contatto utile, successivo all'invio del curriculum medesimo**.

Nei limiti delle finalità di cui all'articolo 6, paragrafo 1, lettera b) del Regolamento, **il consenso** al trattamento dei dati personali presenti nei curricula **non è dovuto**.

Trattamenti nell'ambito del rapporto di lavoro (Parte 2, Titolo VIII)

Il quadro non cambia: divieto di indagine sui lavoratori

ART. 113

Resta fermo quanto disposto **dall'articolo 8 della legge 20 maggio 1970, n. 300** nonché dall'**articolo 10 del decreto legislativo 10 settembre 2003, n. 276**.

ART. 8 - Statuto dei lavoratori

Divieto di indagini sulle opinioni.

È fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore.

ART. 10 Dlgs 276/2003

Divieto di indagini sulle opinioni e trattamenti discriminatori.

1. **E' fatto divieto** alle agenzie per il lavoro e agli altri soggetti pubblici e privati autorizzati o accreditati **di effettuare qualsivoglia indagine o comunque trattamento di dati ovvero di preselezione di lavoratori, anche con il loro consenso, in base alle convinzioni personali, alla affiliazione sindacale o politica, al credo religioso, al sesso, all'orientamento sessuale, allo stato matrimoniale o di famiglia o di gravidanza, alla eta', all'handicap, alla razza, all'origine etnica, al colore, alla ascendenza, all'origine nazionale, al gruppo linguistico, allo stato di salute nonche' ad eventuali controversie con i precedenti datori di lavoro**, a meno che non si tratti di caratteristiche che incidono sulle modalita' di svolgimento della attivita' lavorativa o che costituiscono un requisito essenziale e determinante ai fini dello svolgimento dell'attivita' lavorativa. **E' altresi' fatto divieto di trattare dati personali dei lavoratori che non siano strettamente attinenti alle loro attitudini professionali e al loro inserimento lavorativo.**
2. Le disposizioni di cui al comma 1 non possono in ogni caso impedire ai soggetti di cui al medesimo comma 1 di fornire specifici servizi o azioni mirate per assistere le categorie di lavoratori svantaggiati nella ricerca di una occupazione.

Il quadro non cambia: controllo a distanza dei lavoratori

ART. 114

Resta fermo quanto disposto **dall'articolo 4 della legge 20 maggio 1970, n. 300.**

ART. 4 - Statuto dei lavoratori

Impianti audiovisivi.

1. **Gli impianti audiovisivi** e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori **possono essere impiegati esclusivamente per esigenze organizzative e produttive**, per la **sicurezza del lavoro** e per la **tutela del patrimonio aziendale** e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione delle sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi. ([2])

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

3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore **adeguata informazione** delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196.

Lo Smart Working entra nella normativa

ART. 115

Telelavoro, lavoro agile e lavoro domestico.

Nell'ambito del rapporto di lavoro domestico, del telelavoro e del lavoro agile il datore di lavoro è tenuto a garantire al lavoratore **il rispetto della sua personalità e della sua libertà morale**.

Il lavoratore domestico è tenuto a mantenere la **necessaria riservatezza** per tutto quanto si riferisce alla **vita familiare**.

Il consenso del minore in relazione ai servizi della società dell'informazione (Parte 1, Titolo 1 Capo II)

Servizi della società dell'informazione

Concetto di matrice europea, che viene delineato a livello europeo dalla Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, richiamata dall'art. 4 n. 25 del GDPR

«*Qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi*»

Definizione ampia, i cui contorni sono delineati:

- dall'**ALLEGATO I della Direttiva stessa**, che prevede un "Elenco indicativo dei servizi non contemplati".
- dal **considerando 18 della Direttiva 2000/31**: secondo cui: «I servizi della società dell'informazione abbracciano una vasta gamma di attività economiche svolte in linea (on line). (...) Non sempre si tratta di servizi che portano a stipulare contratti in linea ma anche di servizi non remunerati dal loro destinatario, nella misura in cui costituiscono un'attività economica, come l'offerta di informazioni o comunicazioni commerciali in linea o la fornitura di strumenti per la ricerca, l'accesso e il reperimento di dati. I servizi della società dell'informazione comprendono anche (...) la fornitura di accesso a una rete di comunicazione»
- dalle **Linee guida sul consenso WP29**, che puntualizzano come l'art. 8 del Gdpr faccia riferimento solo ai casi di **offerta diretta ai minori** di servizi della società dell'informazione, escludendo dall'ambito dell'art. 8 quei servizi online che si rivolgono esclusivamente a persone di 18 anni, purché ciò non sia contraddetto da altri elementi (come il contenuto del sito).
- dalla **relazione illustrativa al D.lgs 101/2018**, che porta come esempio di trattamento effettuato nell'ambito dei servizi della società dell'informazione trattamenti dei dati conseguenti all'iscrizione a social network o a servizi di messaggistica

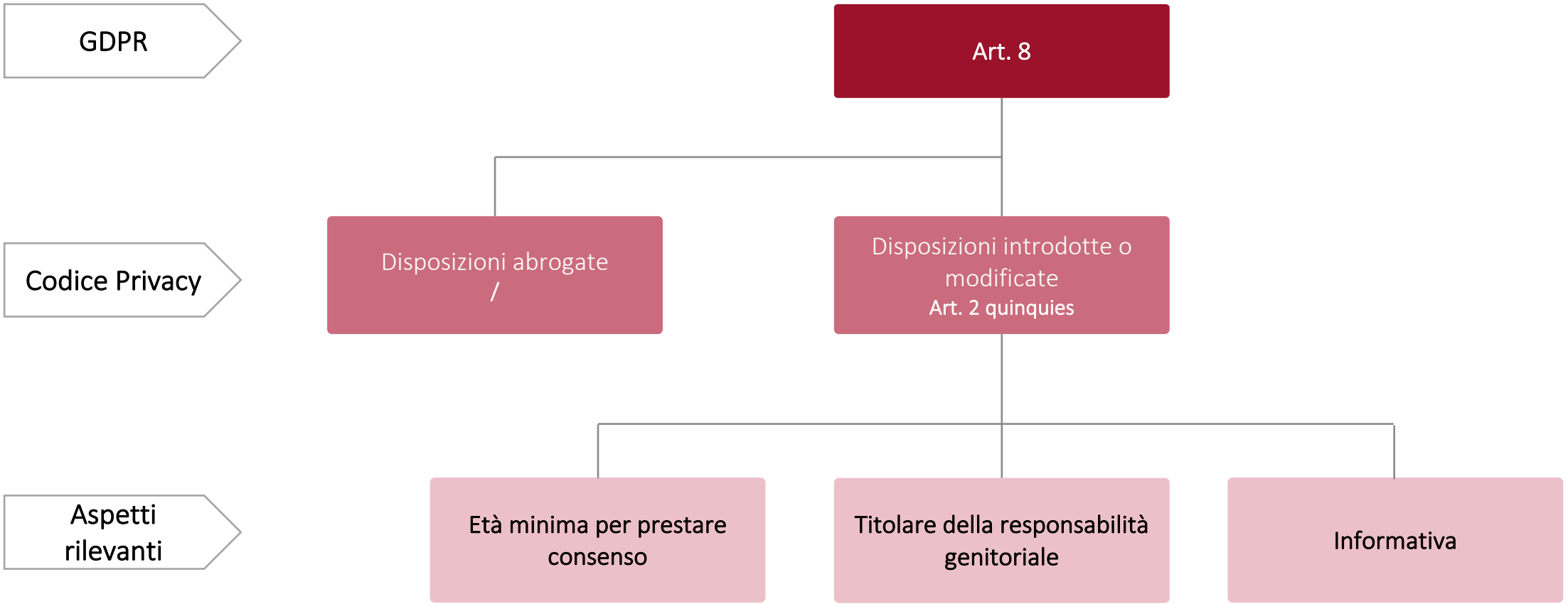
Minore età e Consenso

- Secondo la legge italiana **il minore di 18 anni è incapace di agire, cioè a porre in essere atti che producono effetti sulla sua sfera giuridica**:
    - CONSENSO DEL MINORE NEL DIRITTO CIVILE - Il contratto stipulato dal minore è annullabile, in quanto il suo consenso non può costituire una valida manifestazione di volontà ai fini contrattuali
    - CONSENSO DEL MINORE AL TRATTAMENTO PRIVACY NEI SERVIZI ONLINE - Altra cosa è il consenso al trattamento dei propri dati personali. Con il GDPR si riconosce al minore che abbia compiuto 16 anni la facoltà di disporre validamente dei propri dati personali, acconsentendo validamente al loro trattamento nell'ambito dei servizi della società dell'informazione.

- Lo stesso GDPR interviene a sottolineare la differenza tra i due campi. L'art. 8 del GDPR non intacca le regole nazionali relative alla capacità di agire: *«il paragrafo 1 non pregiudica le disposizioni generali del diritto dei contratti degli Stati membri, quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto ad un minore»*

Consenso del minore per servizi della società dell'informazione (Parte 1, Titolo 1 Capo II, 2 quinquies)

Quali sono gli aspetti più rilevanti per voi?



Consenso del minore per servizi della società dell'informazione (Parte 1, Titolo 1 Capo II, 2 quinquies)

Evoluzione normativa (1/2)

Codice Privacy	GDPR
Il D. Lgs. 196/2003 non affrontava la tematica del consenso del minore in relazione ai servizi della società dell'informazione.	• Il GDPR introduce in maniera molto innovativa la facoltà per il minore di prestare il consenso al trattamento dei propri dati, in presenza di tre condizioni cumulative: o **i trattamenti con base giuridica consenso** → no altre basi giuridiche diverse ex art. 6 par. 1 (contratti) o **il consenso deve essere prestato solo in relazione all'offerta diretta dei servizi della società dell'informazione** → no offline (slide n. 2); o Il minore ha **età superiore a 16 anni** • Se l'interessato ha **età inferiore agli anni 16**, il trattamento è illecito, salvo che il consenso sia stato **PRESTATO o AUTORIZZATO dal titolare della responsabilità genitoriale** • Il Titolare, inoltre, deve adoperare per **verificare**, nei limiti dello sforzo ragionevole (diligenza ordinaria), **se il genitore ha prestato/autorizzato il consenso** al trattamento dei dati del minore di 16 anni

Consenso del minore per servizi della società dell'informazione (Parte 1, Titolo 1 Capo II, 2 quinquies)

Evoluzione normativa (2/2)

Codice Privacy	Disposizioni introdotte da D.lgs 101/2018
Il D. Lgs. 196/2003 non affrontava la tematica del consenso del minore in relazione ai servizi della società dell'informazione.	Il D.Lgs. 101/2018 conferma l'impianto introdotto dal GDPR, con alcune precisazioni: • in attuazione dell'articolo 8, paragrafo 1,il legislatore nazionale riduce l'età minima per prestare validamente il consenso ai servizi della società dell'informazione, fissandola a 14 anni • l'esercente la responsabilità genitoriale è tenuto a prestare il consenso per il trattamento dei dati del minore se di età inferiore di 14 anni • il titolare del trattamento deve redigere le informative e ogni comunicazione con linguaggio particolarmente chiaro e semplice, conciso ed esaustivo, facilmente accessibile e comprensibile

Età minima per prestare consenso

Art. 2 quinquies, comma 1

«In attuazione dell'art. 8, paragrafo 1, del Regolamento, il minore che ha compiuto i quattordici anni, può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione.

- Il Legislatore nazionale, nel rispetto degli spazi di intervento riconosciuti dal GDPR (che nell'art. 8 par. 1 aveva fissato come limite minimo i 13 anni), riduce ulteriormente l'età minima per esprimere il consenso ai fini dell'art. 8, portandola a 14 anni

- Si tratta di una scelta:
  - in linea con ordinamenti di altri Paesi europei
  - idonea a coordinare l'età del consenso ad altre normative interne che riconoscono una capacità di agire attenuata in campi specifici (adozioni – cyberbullismo – consenso agli atti sessuali)

Titolare della responsabilità genitoriale

Art. 2 quinquies, comma 1

«Con riguardo a tali servizi, il trattamento dei dati personali del minore di età inferiore a quattordici anni, fondato sull'art. 6, paragrafo 1, lettera a) del Regolamento, è lecito a condizione che sia prestato da chi esercita la responsabilità genitoriale»

- Il Legislatore nazionale impone, inoltre, che se il minore ha un'età inferiore ai 14 anni, il consenso deve essere PRESTATO da chi esercita la responsabilità genitoriale (viene quindi eliminata l'alternativa posta dal GDPR tra «PRESTATO O AUTORIZZATO»)

- Si tratta di una scelta che potrebbe tradire la volontà del legislatore di approntare una tutela rafforzata nei confronti dei minori di 14 anni, non essendo più sufficiente una mera autorizzazione, ma richiedendosi il materiale coinvolgimento diretto dell'esercente la responsabilità genitoriale, il quale potrebbe essere chiamato a prestare personalmente il consenso per conto del minore di 14 anni

Informativa

Art. 2 quinquies, comma 2

«In relazione all'offerta diretta ai minori di servizi di cui al comma 1, il titolare del trattamento redige con linguaggio particolarmente chiaro e semplice, conciso ed esaustivo, facilmente accessibile e comprensibile al minore al fine di rendere significativo il consenso restato da quest'ultimo, le informazioni e le comunicazione relative al trattamento che lo riguardi»

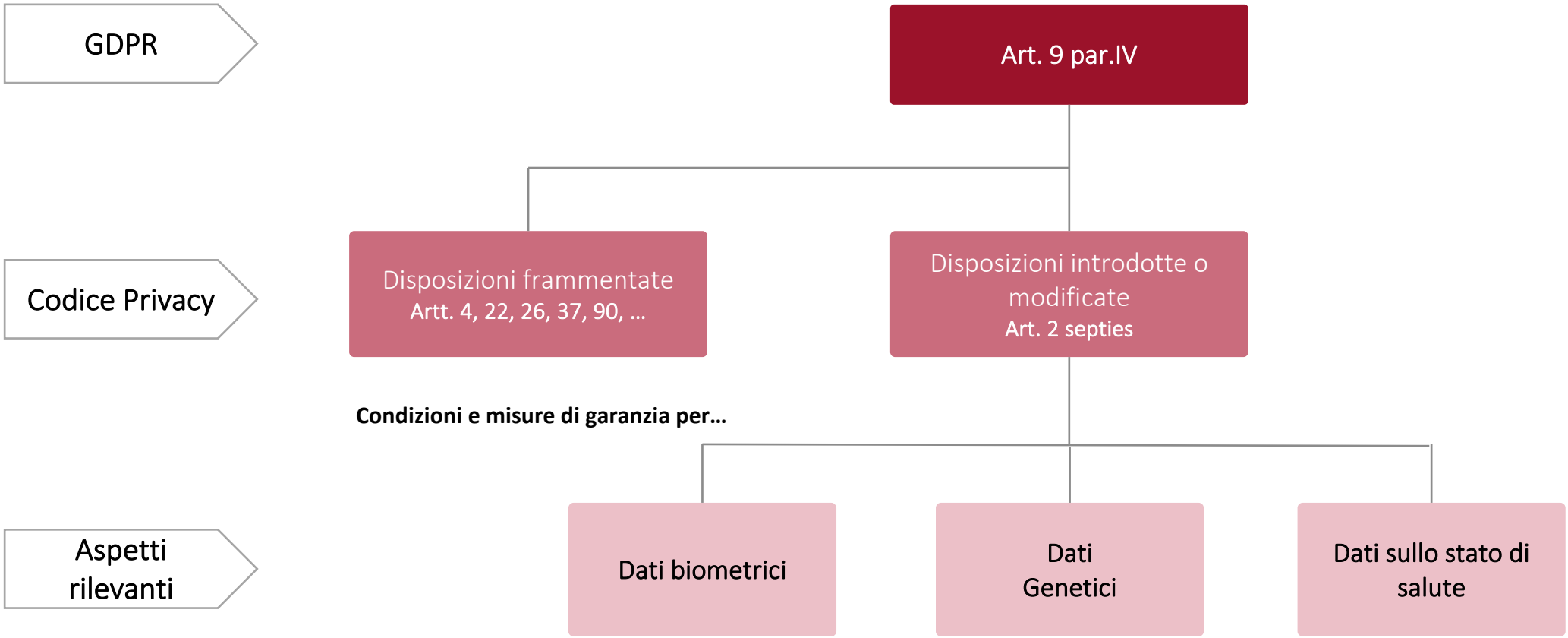
Si tratta di una disposizione recettiva delle regole dettate dal GDPR:

- Art 7 « Condizioni per il consenso»: «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, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro»
- Art. 12: «Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato»: il Titolare del trattamento adotta le misure appropriate per fornire all'interessato le informative e le comunicazioni sull'esercizio dei diritti «*in forma concisa, trasparente, intellegibile e facilmente accessibile con linguaggio semplice e chiaro, in particolare in caso di informazioni destinate specificamente ai minori»*

Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi allo stato di salute (Parte 1, Titolo 1 Capo II)

Trattamento di dati genetici, biometrici e relativi allo stato di salute (Parte 1, Titolo 1 Capo II, 2 septies)

Quali sono gli aspetti più rilevanti per voi?



Trattamento di dati genetici, biometrici e relativi allo stato di salute (Parte 1, Titolo 1 Capo II, 2 septies)

Condizioni per il trattamento e misure di garanzia

- Nel rispetto degli spazi di intervento riservati dal GDPR agli Stati membri (art. 9 par. 4), il Dlgs 101/18 ha introdotto l'art. 2 septies

- L'art. 2 septies comma 1 detta regole peculiari con riguardo al trattamento dei dati genetici, biometrici e relativi allo stato di salute, che rientrano nella definizione di «categorie particolari di dati personali» ex art. 9 par. 1 Gdpr.

Art. 2 septies comma 1

In attuazione di quanto previsto dall'articolo 9, paragrafo 4, del Regolamento, i dati genetici, biometrici e relativi alla salute, possono essere oggetto di trattamento in presenza di una delle condizioni di cui al paragrafo 2 del medesimo articolo ed in conformità alle misure di garanzia disposte dal Garante, nel rispetto di quanto previsto dal presente articolo.

Oltre alle condizioni dettate dall'art. 9 par. 2 lett. a) – j), l'art. 2 septies del Codice Privacy post Dlgs 101/2018 richiede che il trattamento avvenga in conformità con le misure di garanzia che verranno elaborate dal Garante Nazionale.

Resta fermo il rispetto delle disposizioni contenute nelle regole deontologiche, quale condizione essenziale per la liceità e la correttezza del trattamento (ove previste per tali categorie di dati personali).

Trattamento di dati genetici, biometrici e relativi allo stato di salute (Parte 1, Titolo 1 Capo II, 2 septies)

Misure di garanzia

COSA SONO?

Si tratta di misure di carattere tecnico ed organizzativo che verranno elaborate dal Garante Privacy tenendo conto di **tre fondamentali componenti**:

- Innanzitutto le linee guida ed i pareri del Gruppo 29 (divenuto Comitato europeo per la protezione dei dati)- le migliori prassi in materia di trattamento (→ che verranno individuate alla luce dei provvedimenti emanati dal Garante)
- l'evoluzione scientifica e tecnologica
- interesse alla libera circolazione dei dati personali in UE

DA CHI SONO EMANATE?

Le misure di garanzia saranno emanate dal Garante con provvedimento a cadenza almeno biennale, il cui schema sarà previamente sottoposto a consultazione pubblica. In particolare per alcuni particolari trattamenti dei dati genetici e dati relativi allo stato di salute, l'art. 2 septies comma 6 delinea un particolare iter di approvazione, che coinvolge il Ministero della Salute, acquisito il parere del Consiglio Superiore di Sanità.

QUALE SARA' IL CONTENUTO?

Il comma 5 dell'art. 2 septies chiarisce che le misure di garanzie individueranno:

- Le misure di sicurezza, ivi comprese quelle tecniche di cifratura, pseudonomizzazione e minimizzazione
- le specifiche modalità di accesso selettivo ai dati e per rendere le informazioni agli interessati e le altre eventuali misure necessarie a garantire i diritti.
- Il comma 4 individua, a titolo esemplificativo, **quattro specifici settori** in cui interverranno le misure di garanzia […]
- Secondo la Relazione illustrativa, "*le misure di garanzia dovrebbero presentare soprattutto un contenuto tecnico ed organizzativo, e dettare misure di sicurezza*".

Misure di sicurezza - Cosa NON cambia e le novità

Cosa NON cambia

- Si conferma l'impostazione «risk based» del Regolamento, orientato all'individuazione delle misure «adeguate» tenuto conto di criteri di proporzionalità

- le c.d. «Misure Minime» ex. Allegato B al Codice, già superate dal punto di vista sostanziale dall'obbligo di definire misure «adeguate» rispetto a quanto previsto nel lontano 2003, sono formalmente abrogate con l'eliminazione del Titolo V «Sicurezza dei dati e dei sistemi», artt. 31, 32, 33, 34, 35 e 36

Le novità

- Servizi di comunicazione elettronica: sono confermate le disposizioni ed i Provvedimenti in vigore ai sensi dell'art.132
- A questi si aggiungono:
  - il richiamo all'art.32 del Regolamento, imponendone l'applicazione anche laddove il fornitore di servizi di comunicazione elettronica si avvalga di altri fornitori (sostanzialmente non introduce niente di nuovo al combinato disposto degli artt.32 e 29 del Regolamento), con particolare riferimento ai dati di traffico e relativi all'ubicazione
  - L'obbligo imposto ai fornitori di servizi di comunicazione elettronica e al fornitore della rete pubblica di comunicazioni di definire congiuntamente le misure di sicurezza della rete
  - L'obbligo di informare gli abbonati e gli utenti in modo chiaro riguardo ai rischi di violazione della rete, ai possibili rimedi ed ai relativi (presumibili) costi di attuazione, quando tali rischi sono al di fuori dell'ambito di competenza del fornitore stesso. Tali informazioni (in forma naturalmente diversa), sono rese anche al Garante e all'Autorità per le Garanzie nelle Comunicazioni

Trattamento di dati genetici, biometrici e relativi allo stato di salute (Parte 1, Titolo 1 Capo II, 2 septies)

Misure di sicurezza - Cosa dobbiamo attenderci in futuro

Dati genetici, biometrici e relativi alla salute (art.2 septies)

- Le misure di garanzia emesse dal Garante, aggiornate ogni due anni, «individuano le misure di sicurezza, ivi comprese quelle tecniche di cifratura e di pseudonomizzazione, le misure di minimizzazione, le specifiche modalità per l'accesso selettivo ai dati e per rendere le informazioni agli interessati, nonché le eventuali altre misure necessarie a garantire i diritti degli interessati»
- È autorizzato l'uso di dati biometrici nell'ambito delle «**procedure di accesso fisico e logico ai dati da parte di soggetti autorizzati**», posto il rispetto delle garanzie che dovranno essere definite nel suddetto Provvedimento

Dati relativi a condanne penali o reati (art.2-octies)

- Art. 2-octies: il Ministro della Giustizia può, sentito il Garante, identificare mediante decreto ulteriori trattamenti consentiti (e relative garanzie, incluse le misure di sicurezza) rispetto a quanto già previsto dalle normative vigenti (GDPR e D.L.51/2018)

Certificazione della protezione dei dati

- (art. 42 GDPR): Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano, … l'istituzione di meccanismi di certificazione della protezione dei dati… allo scopo di dimostrare la conformità al presente regolamento …. Sono tenute in considerazione le esigenze specifiche delle micro, piccole e medie imprese
- (art. 2-septiesdecies) E' designata Accredia (Ente Unico Nazionale di Accreditamento) per l'accreditamento degli Organismi Di Certificazione

Dati biometrici

Definizioni

- art. 4 n. 14 GDPR: «*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****»*

- Linee Guida in tema di biometria: «*proprietà biologiche, aspetti comportamentali, caratteristiche fisiologiche, tratti biologici o azioni ripetibili laddove tali caratteristiche o azioni sono tanto proprie di un certo individuo quanto misurabili, anche se i metodi usati nella pratica per misurarli tecnicamente comportano un certo grado di probabilità"*

Condizioni di liceità

- GDPR - Rispetto di una delle condizioni previste dall'art. 9 par. 2 lett. a) – j)

- Dlgs. 101/2018 - Per il trattamento dei dati biometrici sarà necessario il rispetto di due requisiti:
  - La sussistenza di una delle condizioni previste dall'art. 9 par. 2 del GDPR
  - l'osservanza delle misure di garanzia che verranno emanate dal Garante

Dati biometrici – Utilizzo per accesso fisico e logico

Evoluzione storica

- Codice Privacy - il trattamento dei dati genetici e biometrici era soggetto alla procedura della verifica preliminare, di cui all'art. 17 e della notifica preventiva, di cui all'art 37
- Provvedimento prescrittivo in materia di biometria - ammetteva il trattamento del dato biometrico sulla base del legittimo interesse per finalità di accesso fisico
- Provvedimento 22 febbraio 2018 - negava il trattamento del dato biometrico sulla base del legittimo interesse
- GDPR - non contempla il legittimo interesse del titolare tra le condizioni che possono legittimare il trattamento dei dati biometrici, dettate dall'art. 9 par. 2 in generale per le categorie particolari di dati

Novità

- Art. 2 septies introdotto dal D.lgs. 101/2018 - *«Ai fini del rispetto dei principi in materia di protezione dei dati personali, con riferimento, agli obblighi di cui all'articolo 32 del Regolamento, è ammesso l'utilizzo dei dati biometrici con riguardo alle procedure di accesso fisico e logico ai dati da parte dei soggetti autorizzati, nel rispetto delle misure di garanzia di cui al presente articolo»*
- Attraverso tale norma si intende così autorizzare il trattamento di dati biometrici quando le esigenze di **sicurezza e integrità dei sistemi o delle aree** (ad esempio, dei locali ove sono custoditi dati e informazioni di particolare delicatezza) richiedono un **maggior grado di certezza dell'identità del soggetto legittimato all'utilizzo di sistemi o all'accesso alle aree indicate**, anche al fine di scongiurare il rischio di cessione illegittima o di furto di credenziali

Dati genetici

Definizioni

- *art 4 n. 13 GDPR: 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.*

- *Considerando 34 GDPR: fa riferimento, in particolare, ai dati personali relativi alle caratteristiche genetiche, ereditarie o acquisite, di una persona fisica, che risultino dall'analisi di un campione biologico della persona fisica in questione, in particolare dall'analisi dei cromosomi, del DNA o del RNA ovvero dall'analisi di un altro elemento che consenta di ottenere informazioni equivalenti.*

Condizioni di liceità

- Codice Privacy - I dati genetici erano ricompresi all'interno della definizione di dati sensibili e sottoposti ad una disciplina particolarmente rigorosa per il loro trattamento, dettata da:
  - Art. 37 Notificazione del trattamento
  - Art 41: Necessità di autorizzazione
  - Capo V della Parte II: Art. 90

- GDPR - i dati genetici acquisiscono autonomia e vengono formalmente distinti dai dati relativi allo stato di salute:
  - l'art. 9 par. 2 del GDPR impone, per il loro trattamento, il rispetto di una delle condizioni dettate alle lett. a)-j)
  - L'art. 9 par. 4 del GDPR autorizza il Legislatore Nazionale a prevedere ulteriori cautele per il loro trattamento

Dati genetici – Peculiarità del D.lgs 101/2018

Il D.lgs 101/2018 detta anche per i dati genetici la **medesima disciplina stabilita per il trattamento dei dati biometrici e sullo stato di salute**. Per svolgere un trattamento lecito è quindi necessario contestualmente:

- rispettare una delle **condizioni previste dall'art. 9 par. 2 GDPR lett. a) – j)**
- conformarsi alle **misure di garanzia che verranno dettate dal Garante** con apposito provvedimento

PRIMA PECULIARITA'

Si prevede un particolare Iter procedimentale per l'approvazione delle misure di garanzia relative al trattamento dei dati genetici

«le misure di garanzie che riguardano i dati genetici […] sono adottate sentito il Ministro della salute che, a tali misure di garanzia che riguardano i dati genetici e il fine, acquisisce il parere del Consiglio superiore di sanità»

Iter che **ricalca il vecchio articolo 90 del Codice Privacy**, il quale però prevedeva questo procedimento per il rilascio delle singole autorizzazioni al trattamento del titolare.

SECONDA PECULIARITA'

Attribuisce al Garante la facoltà di stabilire, in un'ottica di rafforzamento delle garanzie in favore degli interessati, il consenso dell'interessato o altre misure specifiche come ulteriore misura di protezione adottabile in caso di elevato rischio. Questo requisito si andrebbe a sommare alle già fissate condizioni di liceità del trattamento.

«*Limitatamente ai dati genetici, le misure di garanzia possono individuare, in caso di particolare ed elevato livello di rischio, il consenso come ulteriore misura di protezione dei diritti dell'interessato, a norma dell'articolo 9, paragrafo 4, del Regolamento, o altre cautele specifiche»*

Dati relativi allo stato di salute

Definizioni

- art. 4 n. 15 GDPR: *«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»*

- Considerando 35: *«Nei dati personali relativi alla salute dovrebbero rientrare tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso. Questi comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria o della relativa prestazione di cui alla direttiva 2011/24/UE del Parlamento europeo e del Consiglio […].»*

Condizioni di liceità

- Codice Privacy - Rispetto dei requisiti previsti dall'art. 26 Codice Privacy: Consenso scritto dell'interessato; Previa autorizzazione del Garante (art. 40-41). Salvo disposizioni più specifiche.

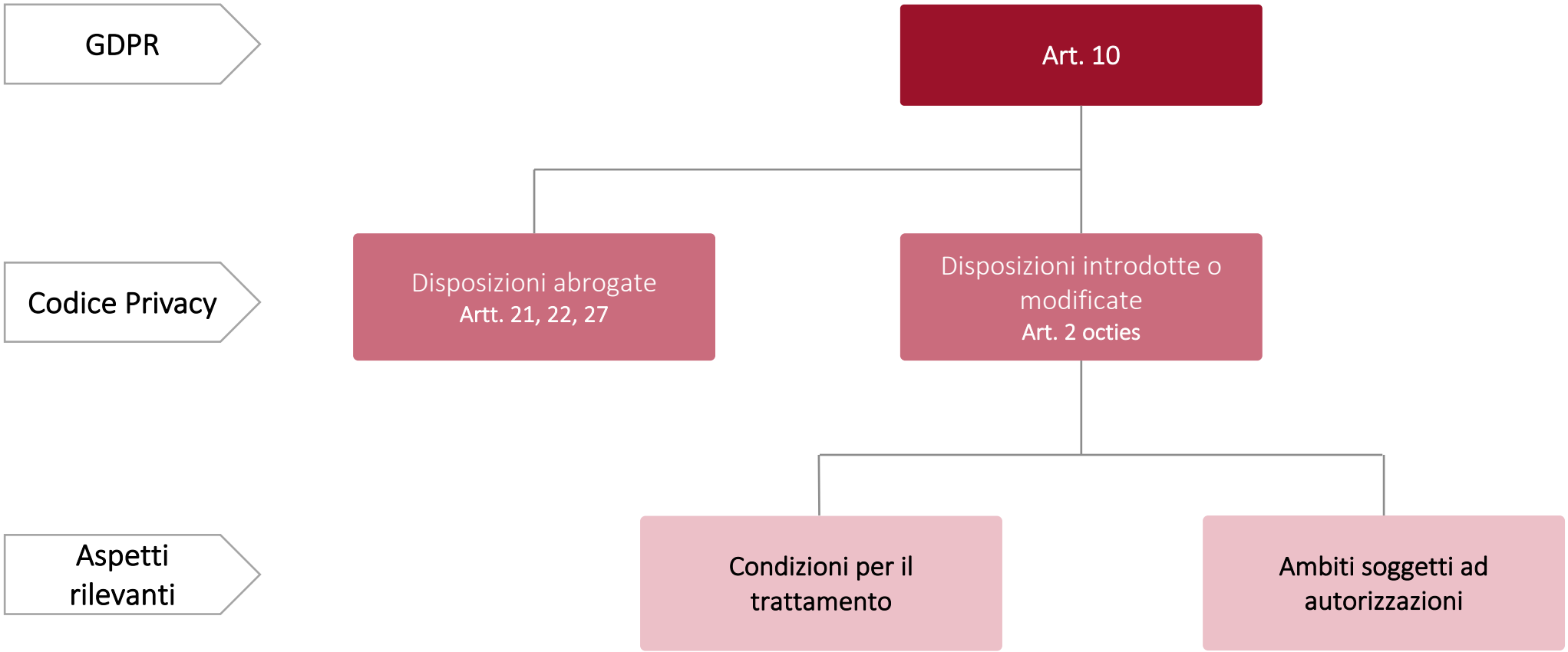
- GDPR - Rispetto di una delle condizioni previste dall'art. 9 par. 2 lett. a) – j)

- Dlgs. 101/2018 - Art. 2 septies riprende l'impianto delineato dal GDPR, introducendo un ulteriore requisito di liceità. Per il trattamento dei dati relativi allo stato di salute sarà necessario il rispetto di due requisiti:
  - La sussistenza di una delle condizioni previste dall'art. 9 par. 2 del GDPR
  - l'osservanza delle misure di garanzia che verranno emanate dal Garante

Principi relativi al trattamento di dati relativi a condanne e reati (Parte 1, Titolo 1 Capo II)

Principi relativi al trattamento di dati relativi a condanne e reati (Parte 1, Titolo 1 Capo II, 2 octies)

Quali sono gli aspetti più rilevanti per voi?



Principi relativi al trattamento di dati relativi a condanne e reati (Parte 1, Titolo 1 Capo II, 2 octies)

Definizione

Codice Privacy

art. 4 c. 1 lett. e) → dati giudiziari:

«Dati personali idonei a rivelare provvedimenti di cui all'art. 3 comma 1, lettere da a) a o) e da r) ad u) del Dpr 12 novembre 2002 n. 313 in materia di casellario giudiziale, anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti o la qualità di imputato o indagato ai sensi degli articoli 60 e 61 del codice di procedura penale»

GDPR

- abbandona la denominazione "dati giudiziari" in favore di "dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza»
- non fornisce una definizione precisa dell'espressione

Si cambia quindi approccio, accogliendo una definizione più generica e meno legata all'emanazione di provvedimenti formali.

All'interno dell'espressione potranno pertanto farsi rientrare ogni informazione che riveli:

- l'esistenza di una condanna penale a carico dell'interessato
- l'attribuibilità di un reato (a partire quindi dalla notizia di reato e l'acquisizione della qualità di indagato e poi di imputato)
- l'irrogazione di misure di sicurezza di carattere penale previste dagli art. 200 e ss. c.p., che sono comunque rivolte a coloro che hanno commesso un reato e vengono ritenuti socialmente pericolosi

Principi relativi al trattamento di dati relativi a condanne e reati (Parte 1, Titolo 1 Capo II, 2 octies)

Condizioni per il trattamento

Codice Privacy

Secondo l'art. 27 "*Garanzie per i dati giudiziari*", il trattamento di dati giudiziari da parte di privati [...] era consentito soltanto se:

- autorizzato da espressa disposizione di legge
- autorizzato da provvedimento del Garante (generale o particolare)

I quali specifichino le rilevanti finalità di interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili.

GDPR

Il trattamento dei dati relativi a condanne e reati o connesso a misure di sicurezza è ammesso in presenza di alcune **condizioni**:

1. un primo presupposto: la sussistenza di una base giuridica ex art. 6 par. 1.
2. un secondo presupposto, alternativo:
   - il controllo dell'Autorità pubblica, che è l'unico Ente che può tenere il registro completo delle condanne penali
   - oppure in presenza di un'autorizzazione del diritto dell'UE o degli Stati membri la quale preveda garanzie appropriate per i diritti e le libertà.

Disposizioni introdotte da D.lgs 101/2018

Il D.Lgs. 101/2018 mantiene l'impianto introdotto dal GDPR, provvedendo tuttavia a **specificarlo nel dettaglio**:

1. l'esistenza di una base giuridica ex art. 6 par. 1
2. come secondo presupposto, alternativo:
   - il controllo dell'Autorità Pubblica sul trattamento
   - l'autorizzazione al trattamento da parte di una norma di legge o, nei casi previsti dalla legge, di un regolamento che prevedano garanzie adeguate per i diritti e le libertà dell'interessato
   - in assenza delle norme di legge o regolamento, i trattamenti e le garanzie sono individuati da decreto del Ministero della Giustizia, sentito il Garante

Condizioni per il trattamento - Fonti autorizzative

- Nell'art. 10 del GDPR si parlava, quindi genericamente di "Diritto", senza specificare quale fonte del diritto fosse legittimata ad autorizzare il trattamento dei dati relativi a condanne penali e reato o a connesse misure di sicurezza.

- Il D.lgs 101/2018 restringe il campo a:
  - Norme di legge (fonti primarie del diritto: Legge, D.lgs, D.l., D.p.r.)
  - Regolamenti, nei casi previsti dalla legge (Principio di riserva di legge)
  - Decreti Ministero della Giustizia, sentito il Garante

- Si tratta di un rafforzamento della protezione del dato:
  - NO qualsiasi fonte del diritto → esclusivamente quelle previste dall'art. 2 octies
  - NO più autorizzazioni generali → potranno ancora esse tenute in considerazione (ove ritenute compatibili dal Garante)
  - NO contratti collettivi → possono al più individuare modalità e limiti del trattamento già autorizzato da legge e regolamenti

Relazione illustrativa: "*la **Ratio** di tale disposizione è da rinvenire nella volontà di tutelare l'interessato da trattamenti particolarmente invasivi della propria privacy, considerate le finalità del trattamento e la tipologia dei dati. Una tutela effettiva può essere garantita solo dal vaglio di un'autorità pubblica, in grado di bilanciare gli interessi nazionali con quelli di riservatezza del singolo ovvero da un'espressa disposizione normativa contenente garanzie ulteriori, rispetto a quelle normalmente adottate, per la riservatezza dell'interessato*»

Principi relativi al trattamento di dati relativi a condanne e reati (Parte 1, Titolo 1 Capo II, 2 octies)

Principali ambiti soggetti ad autorizzazione (1/3)

Art. 2 octies comma 3 effettua, a titolo esemplificativo, un lungo elenco di **11 "aree"** nell'ambito delle quali le Leggi, i Regolamenti ed i Decreti del Min. Giust. possono **autorizzare il trattamento dei dati relativi a condanne penali e reati o connesse misure di sicurezza**

1. L'adempimento di obblighi e l'esercizio di diritti in materia di diritto del lavoro, nei limiti stabiliti da leggi, regolamenti e contratti collettivi, secondo quanto previsto dall'art. 9 par. 2 lett. b) e 88 del GDPR

   → Fa riferimento al campo del diritto del lavoro (disciplina contenuta, tra gli altri, nel Dlgs 81/2008). In tale ambito: La **fonte autorizzativa** del trattamento deve essere sempre legge o regolamento. I contratti collettivi possono contribuire specificando le **modalità ed i limiti** del trattamento dei dati «giudiziari»

2. L'adempimento di obblighi previsti da legge o regolamento in materia di mediazione finalizzata alla conciliazione nell'ambito del contenzioso civile e commerciale

   → Il riferimento è agli strumenti deflattivi del contenzioso civile e commerciale, le cosiddette ADR (alternative dispute resolution)

3. La verifica dei requisiti di onorabilità, requisiti soggettivi e presupposti interdittivi nei casi previsti da leggi o dai regolamenti Es. art. 76 dlgs 209/2005 per le assicurazioni

   → D.M. n. 220/2011: «Regolamento recante determinazione dei requisiti di professionalità, onorabilità e indipendenza degli esponenti aziendali, nonché dei requisiti di onorabilità dei titolari di partecipazioni, ai sensi degli artt. 76 e 77 C.Ass.Pr. di cui al Dlgs. n. 209/2005»

Principi relativi al trattamento di dati relativi a condanne e reati (Parte 1, Titolo 1 Capo II, 2 octies)

Principali ambiti soggetti ad autorizzazione (2/3)

Art. 2 octies comma 3 effettua, a titolo esemplificativo, un lungo elenco di **11 "aree"** nell'ambito delle quali le Leggi, i Regolamenti ed i Decreti del Min. Giust. possono **autorizzare il trattamento dei dati relativi a condanne penali e reati o connesse misure di sicurezza**

4. l'accertamento di responsabilità in relazione a sinistri o eventi attinenti alla vita umana, nonché la prevenzione, l'accertamento e il contrasto di frodi o situazioni di concreto rischio per il corretto esercizio dell'attività assicurativa, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia

   → Art. 30 della legge 27/2012 per quanto concerne la comunicazione della relazione annuale ad ISVAP

5. l'adempimento di obblighi previsti da disposizioni di legge in materia di comunicazioni e informazioni antimafia o in materia di prevenzione della delinquenza di tipo mafioso e di altre gravi forme di pericolosità sociale, nei casi previsti da leggi o da regolamenti, o per la produzione della documentazione prescritta dalla legge per partecipare a gare d'appalto

   → D.lgs. 6 settembre 2011, n. 159 Codice delle leggi antimafia e delle misure di prevenzione, nonché nuove disposizioni in materia di documentazione antimafia

6. l'accertamento del requisito di idoneità morale di coloro che intendono partecipare a gare d'appalto, in adempimento di quanto previsto dalle vigenti normative in materia di appalti

   → D.lgs. 50/2016 Codice Appalti Pubblici, art. 80, ad esempio, che enuncia i motivi di esclusione dalla gara pubblica.

Principi relativi al trattamento di dati relativi a condanne e reati (Parte 1, Titolo 1 Capo II, 2 octies)

Principali ambiti soggetti ad autorizzazione (3/3)

Art. 2 octies comma 3 effettua, a titolo esemplificativo, un lungo elenco di **11 "aree"** nell'ambito delle quali le Leggi, i Regolamenti ed i Decreti del Min. Giust. possono **autorizzare il trattamento dei dati relativi a condanne penali e reati o connesse misure di sicurezza**

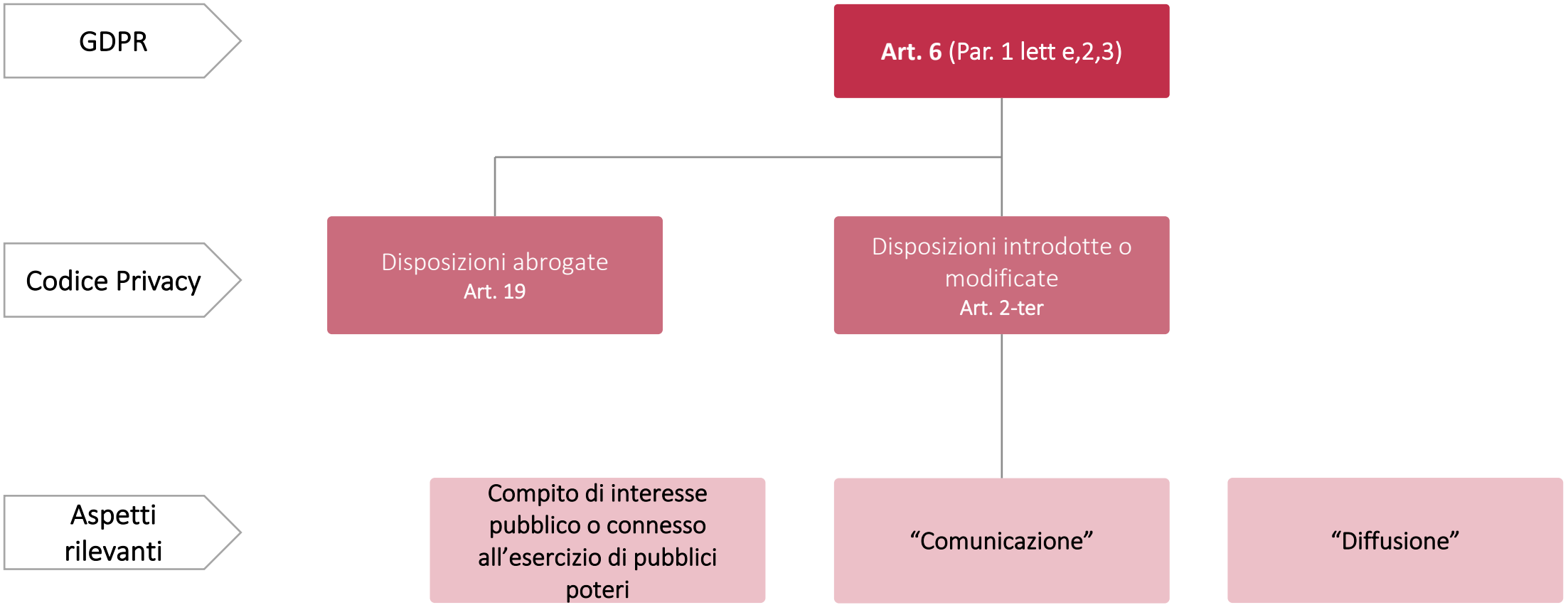
7. l'adempimento degli obblighi previsti dalle normative vigenti in materia di prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo

D.lgs 231/2007 in materia di «prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attivita' criminose e di finanziamento del terrorismo»

Trattamento per esecuzione di un compito di interesse pubblico; regole deontologiche; trattamento di categorie particolari di dati per motivi di interesse pubblico rilevante (Parte 1, Titolo 1, Capo II)

Trattamento per esecuzione di un compito di interesse pubblico (Parte 1, Titolo 1, Capo II, 2 ter)

Quali sono gli aspetti più rilevanti per voi?



Trattamento per esecuzione di un compito di interesse pubblico (Parte 1, Titolo 1, Capo II, 2 ter)

Rapporti con la normativa previgente

- L'articolo 2 ter si presenta come una riformulazione dell'articolo 19 del previgente Codice, che viene integralmente abrogato. L'ambito di applicazione soggettivo viene esteso al fine di adeguarsi all'impostazione adottata dal GDPR.

Il focus è sulla natura dell'attività che genera il trattamento

- Nel GDPR scompare la distinzione basata sulla natura ·pubblica o privata dei soggetti che trattano i dati, **rilevando unicamente la finalità del trattamento perseguita, pertanto se la finalità concerne un interesse pubblico o privato.**

- L'articolo quindi deve intendersi applicabile ai soggetti che trattano i dati personali per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, **a prescindere dalla loro natura soggettiva** (Cfr. Relazione illustrativa p. 6).

Compito di interesse pubblico o connesso all'esercizio di pubblici poteri

Basi giuridiche

L'articolo 6 del GDPR richiede che i dati personali possano essere trattati solo se una delle seguenti sei condizioni di legittimità è presente:

ART. 6, par. 1 del GDPR

- Consenso
- Esecuzione contratto o misure precontrattuali
- Obbligo legale
- Salvaguardia interessi vitali
- Interesse legittimo del Titolare o di un terzo
- **Esecuzione compito di interesse pubblico**

Nell'impianto del GDPR, le basi giuridiche hanno valenza equipollente

ART. 6, par. 1, lett. 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*»

Compito di interesse pubblico o connesso all'esercizio di pubblici poteri

ART. 6, par. 3, del GDPR

«La base su cui si fonda il trattamento dei dati di cui al paragrafo 1, lettere c) ed e), deve essere stabilita:

a) dal diritto dell'Unione; o

b) dal diritto dello Stato membro cui è soggetto il titolare del trattamento. La finalità del trattamento è determinata in tale base giuridica o, per quanto riguarda il trattamento di cui al paragrafo 1, lettera e), è necessaria per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Tale base giuridica potrebbe contenere disposizioni specifiche per adeguare l'applicazione delle norme del presente regolamento, tra cui: le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto, quali quelle per altre specifiche situazioni di trattamento di cui al capo IX. Il diritto dell'Unione o degli Stati membri persegue un obiettivo di interesse pubblico ed è proporzionato all'obiettivo legittimo perseguito».

L'articolo 2 ter del Codice emendato, in particolare, specifica la base giuridica individuata ai sensi dell'articolo 6, paragrafo 3, lettera b) del GDPR nel "diritto dello Stato membro", precisando che a livello nazionale tale base è costituita esclusivamente da una norma di legge o di regolamento. La norma si colloca nel Capo II «Principi»

ART. 6, par. 2, del GDPR *«Gli Stati membri possono mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione delle norme del presente regolamento con riguardo al trattamento, in conformità del paragrafo 1, lettere c) ed e), determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto anche per le altre specifiche situazioni di trattamento di cui al capo IX»*

Compito di interesse pubblico o connesso all'esercizio di pubblici poteri

Scelte del legislatore nazionale nell'impianto del previgente Codice

Già la Direttiva 95/46/CE del Parlamento Europeo e del Consiglio del 24 ottobre 1995 (di seguito, «Direttiva»), all'art. 7 lett. e) prevedeva, tra i fondamenti giuridici, la necessità del trattamento «*per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento o il terzo a cui vengono comunicati i dati".*

Da notare che la Direttiva non operava alcuna distinzione in base alla natura ·pubblica o privata dei soggetti che trattano i dati. La scelta di dare rilievo all'elemento soggettivo era stata operata dal legislatore italiano in sede di recepimento nell'ordinamento nazionale.

Il Gruppo dei Garanti europei nel «Parere 6/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE» («**WP 217**») dedica talune riflessioni al fondamento di liceità di cui all'art. 7 lett. e) della Direttiva che possono essere qui utilizzate in quanto l'attuale art. 6 par. 1 lett. e) del GDPR riprende la medesima formulazione, con qualche piccola differenza.

Compito di interesse pubblico o connesso all'esercizio di pubblici poteri

Il Parere dei Garanti europei WP 217

Come si legge nel **WP 217:**

- **l'espressione «pubblici poteri»** si riferisce **a un mandato conferito dall'Unione europea o da uno Stato membro**. In altre parole, i compiti eseguiti nell'interesse pubblico di **un paese terzo** o connessi all'esercizio di pubblici poteri conferiti in virtù del diritto estero **non rientrano nel campo di applicazione di questa disposizione**.
- «*l'articolo 7, lettera e), contempla due situazioni ed è pertinente sia per il settore pubblico che per quello privato.* Innanzitutto, riguarda le situazioni in cui il titolare del trattamento stesso è investito di pubblici poteri o svolge un compito di interesse pubblico (ma non è necessariamente soggetto anche all'adempimento di un obbligo legale per il trattamento dei dati) e il trattamento è necessario all'esercizio di tali poteri o all'esecuzione di quel compito.

Alcuni esempi:

- un'autorità tributaria può raccogliere e trattare i dati relativi alla dichiarazione dei redditi di una persona al fine di stabilire e verificare l'importo da versare a titolo di imposta.
- un'associazione professionale come un ordine forense o un ordine di professionisti del settore medico investiti di pubblici poteri per agire in tal senso possono avviare procedimenti disciplinari nei confronti di alcuni dei loro membri.
- un ente pubblico locale quale un'amministrazione comunale cui sia stato affidato il compito di gestire un servizio di biblioteca, una scuola o una piscina comunale.

Trattamento per esecuzione di un compito di interesse pubblico (Parte 1, Titolo 1, Capo II, 2 ter)

«Comunicazione» e «Diffusione»

Definizione

ART. 2-ter, comma 4, lett. a) e b) del Decreto

"Comunicazione", *il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione*

"Diffusione", *il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione*

L'art. 2 ter, comma 4, **INTRODUCE** specifiche definizioni di "comunicazione" e "diffusione", riprendendo quelle presenti nel Codice previgente, adeguate alle modifiche normative del nuovo testo.

Il GDPR non fornisce alcuna definizione

Trattamento per esecuzione di un compito di interesse pubblico (Parte 1, Titolo 1 Capo II, 2 ter)

«Comunicazione»

Condizioni di legittimità della comunicazione

La comunicazione **fra titolari che effettuano trattamenti di dati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri** è ammessa solo per il trattamento di dati comuni:

1. ai sensi del comma 1, nei casi previsti dalla legge o, nei casi previsti dalla legge, di regolamento;
2. **anche in assenza di previsione legislativa o regolamentare**, qualora la stessa sia necessaria allo svolgimento delle finalità istituzionali, previa comunicazione al Garante (e *«può essere iniziata se è decorso il termine di quarantacinque giorni dalla relativa comunicazione al Garante, senza che lo stesso abbia adottato una diversa determinazione delle misure da adottarsi a garanzia degli interessati»*)

Tale eccezione vale solo per la comunicazione e **MAI** per la diffusione

La norma riprende il disposto dell'art. 39 del vecchio Codice nella nuova impostazione basata sulla finalità del trattamento.

«Diffusione»

Condizioni di legittimità della diffusione

La diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalità è invece ammessa unicamente **nei casi previsti dalla legge o, nei casi previsti dalla legge, di regolamento.**

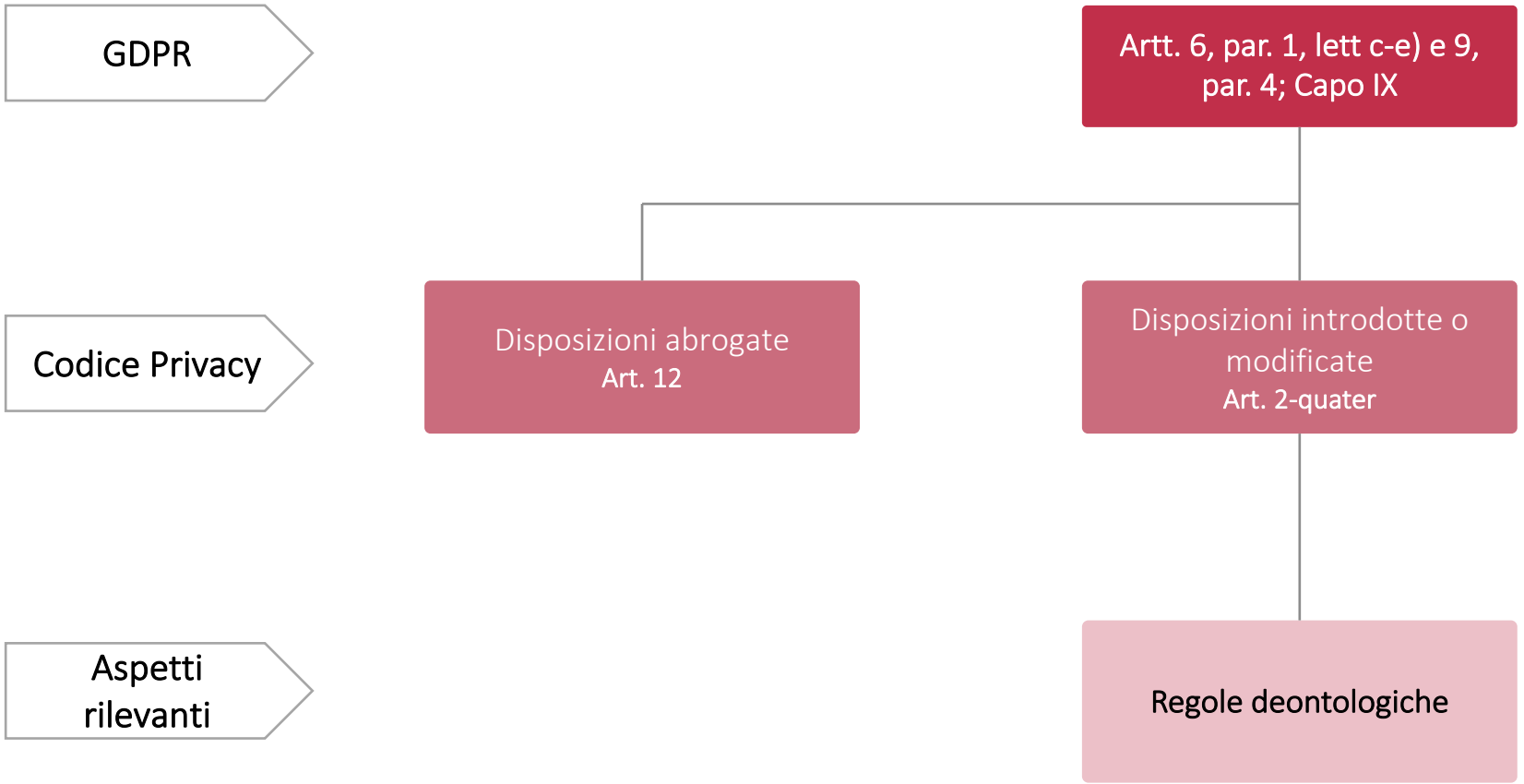
Diritto di opposizione dell'interessato

I trattamenti basati sulla base giuridica ex art. 6 lett. e) GDPR sono potenzialmente quelli a maggiore incidenza sugli interessati considerati lo squilibrio e la contrapposizione tra potere pubblico e vita privata

→ Quale contrappeso, all'interessato è infatti riconosciuta la facoltà di opporsi al trattamento ai sensi dell'art. 21, par. 1, del GDPR

Regole deontologiche (Parte 1, Titolo 1, Capo II, 2 quater)

Quali sono gli aspetti più rilevanti per voi?



Regole deontologiche (Parte 1, Titolo 1, Capo II, 2 quater)

Cosa prevede

- L'articolo affida al Garante l'attività di promozione della sottoscrizione di "Regole deontologiche" negli ambiti in cui il GDPR riserva la materia agli Stati membri.
- In particolare, il GDPR prevede che il legislatore nazionale possa individuare disposizioni più specifiche, nonché determinare requisiti ad hoc relativamente a:
  a) trattamenti necessari per adempiere un obbligo legale;
  b) trattamenti necessari per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri;
  c) trattamento di dati genetici, biometrici o relativi alla salute;
  d) talune specifiche situazioni di trattamento, come ad esempio il trattamento a scopi giornalistici o di espressione accademica, artistica o letteraria, il trattamento nell'ambito dei rapporti di lavoro e il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

Regole Deontologiche (Artt. GDPR)

Artt. 6, par. 1, lettere c) ed e) GDPR:

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento

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;

Art. 9, par. 4 GDPR:

Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute

Capo IX «Disposizioni relative a specifiche situazioni di trattamento» GDPR:

- Articolo 85 Trattamento e libertà d'espressione e di informazione
- Articolo 86 Trattamento e accesso del pubblico ai documenti ufficiali
- Articolo 87 Trattamento del numero di identificazione nazionale
- Articolo 88 Trattamento dei dati nell'ambito dei rapporti di lavoro
- Articolo 89 Garanzie e deroghe relative al trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici
- Articolo 90 Obblighi di segretezza
- Articolo 91 Norme di protezione dei dati vigenti presso chiese e associazioni religiose

Il Garante

- ***promuove**, nell'osservanza del **principio di rappresentatività** e tenendo conto delle raccomandazioni del Consiglio d'Europa sul trattamento dei dati personali, **l'adozione di regole deontologiche** per i trattamenti previsti dalle disposizioni di cui agli articoli 6, paragrafo 1, lettere c) ed e), 9, paragrafo 4, e al Capo IX del Regolamento*
- ***ne verifica la conformità alle disposizioni vigenti** anche attraverso l'esame di osservazioni di soggetti interessati, e contribuisce a garantirne la diffusione e il rispetto*

Regole Deontologiche e Ratio dell'intervento legislativo

La disposizione

ART. 2-quater

«2. Lo schema di regole deontologiche è sottoposto a ***consultazione pubblica*** *per almeno sessanta giorni.*

3. Conclusa la fase delle consultazioni, le regole deontologiche ***sono approvate dal Garante ai sensi dell'articolo 154-bis,*** *comma 1, lettera b),* ***pubblicate nella Gazzetta Ufficiale*** *della Repubblica italiana e, con decreto del Ministro della giustizia, sono riportate nell'allegato A del presente codice.*

4. Il rispetto delle disposizioni contenute nelle regole deontologiche di cui al comma 1 costituisce condizione essenziale per la liceità e la correttezza del trattamento dei dati personali».

Tale disposizione trova in parte la propria ratio nella scelta di conservare le regole stabilite nei "Codici di deontologia e di buona condotta", previsti all'articolo 12 del previgente Codice, che sino ad oggi hanno costituito una rilevante fonte di riferimento per i settori a cui sono diretti.

Come si legge nella Relazione illustrativa (p. 7), sebbene si sia preferito far sopravvivere tali corpus settoriali, non si è optato per una loro integrale trasposizione nel nuovo testo normativo, ritenendo piuttosto necessario un loro aggiornamento ed adeguamento alla luce del nuovo impianto normativo e dei progressi tecnico-scientifici. Per tale motivo, l'articolo in esame prevede che lo schema di regole deontologiche sia sottoposto ad una previa consultazione pubblica.

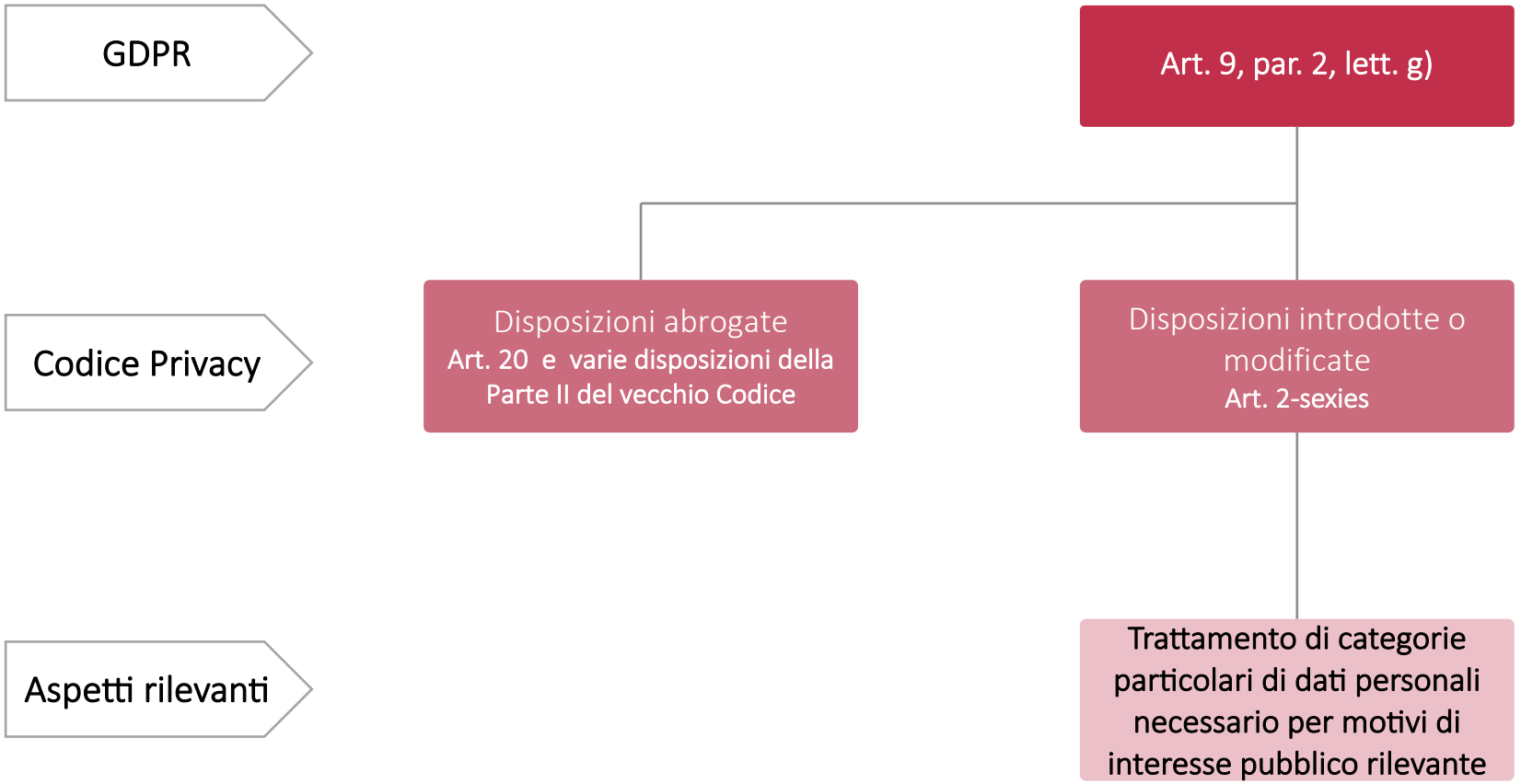
Il dialogo con le parti, gli stakeholders e i settori direttamente interessati è essenziale al fine di elaborare regole condivisibili e stabilire modalità di attuazione che non risultino eccessivamente onerose ovvero inefficaci agli occhi degli operatori.

Regime transitorio - Art. 20 decreto 101

Restano provvisoriamente vigenti e applicabili anche i codici di deontologia e buona condotta (gli Allegati da A.1 e A4 e A.7 al Codice della privacy); ciò **fino al controllo della loro compatibilità con il GDPR** che il Garante dovrà effettuare entro 90 giorni dalla data di entrata in vigore del decreto (il 19 Settembre prossimo) **o** – per quanto riguarda i soli codici A.5, sulle centrali rischi private; A.6 per i trattamenti di dati personali effettuati per svolgere investigazioni difensive e A.7 per il trattamento dei dati personali effettuato a fini di informazione commerciale - **fino alla definizione delle nuove procedure di adozione di codici di condotta (ridefiniti dall'art. 16 "Regole deontologiche") ai sensi dell'art. 40 del GDPR**

Trattamento categorie particolari di dati per motivi di interesse pubblico rilevante (Parte 1, Titolo 1, Capo II, 2 sexies)

Quali sono gli aspetti più rilevanti per voi?



Trattamento di «categorie particolari di dati personali» (Art. 9, par. 1 e 2 GDPR)

Il trattamento di categorie particolari dei dati è vietato (art. 9, co.1), a meno che ricorra una delle seguenti condizioni:

a) consenso esplicito dell'interessato

b) necessario all'assolvimento di obblighi o per l'esercizio di diritti specifici del titolare o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e della protezione sociale

c) salvaguardia di interessi vitali dell'interessato o di un terzo

d) enti senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali

e) dati resi manifestamente pubblici dall'interessato

f) esercizio di un diritto in sede giudiziaria

g) motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri

h) finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali

i) motivi di interesse pubblico nel settore della sanità pubblica

j) archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici

Trattamento categorie particolari di dati per motivi di interesse pubblico rilevante (Parte 1, Titolo 1, Capo II, 2 sexies)

Cosa prevede

- L'articolo 2-sexies specifica quanto previsto dall'articolo 9, paragrafo 1, lettera g) del GDPR, ai sensi del quale il trattamento di categorie particolari di dati è ammesso quando è «*necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato*».

- Il suddetto trattamento è pertanto ammesso solo se previsto dal diritto dell'Unione europea o dal diritto nazionale.

- In quest'ultimo caso, la base giuridica è costituita esclusivamente da una disposizione di legge o di regolamento, che, oltre ad assicurare le condizioni di proporzionalità del trattamento, di salvaguardia del diritto alla protezione dei dati e la previsione di misure di salvaguardia appropriate per gli interessati, deve ulteriormente specificare i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante.

- Come si legge nella Relazione illustrativa (p. 8), a fini di razionalizzazione e semplificazione, l'articolo riunisce in un elenco, non esaustivo, i trattamenti che possono ritenersi effettuati per motivi di rilevante interesse pubblico, in precedenza disseminati in molteplici disposizioni del previgente Codice.

- La norma riguarda solo le «categorie particolari di dati».

- Infine, con riferimento al trattamento di dati genetici, biometrici e relativi alla salute, l'articolo opera un rinvio alle misure di garanzia di cui al successivo art. 2-septies.

La casistica di cui al secondo comma dell'art. 2 sexies (1/3)

*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:*

a) accesso a documenti amministrativi e accesso civico;

b) tenuta degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia e dei cittadini italiani residenti all'estero, e delle liste elettorali, nonché rilascio di documenti di riconoscimento o di viaggio o cambiamento delle generalità;

c) tenuta di registri pubblici relativi a beni immobili o mobili;

d) tenuta dell'anagrafe nazionale degli abilitati alla guida e dell'archivio nazionale dei veicoli;

e) cittadinanza, immigrazione, asilo, condizione dello straniero e del profugo, stato di rifugiato;

f) elettorato attivo e passivo ed esercizio di altri diritti politici, protezione diplomatica e consolare, nonché documentazione delle attività istituzionali di organi pubblici, con particolare riguardo alla redazione di verbali e resoconti dell'attività di assemblee rappresentative, commissioni e di altri organi collegiali o assembleari;

g) esercizio del mandato degli organi rappresentativi, ivi compresa la loro sospensione o il loro scioglimento, nonché l'accertamento delle cause di ineleggibilità, incompatibilità o di decadenza, ovvero di rimozione o sospensione da cariche pubbliche;

h) svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalità direttamente connesse all'espletamento di un mandato elettivo;

La casistica di cui al secondo comma dell'art. 2 sexies (2/3)

i) attività dei soggetti pubblici dirette all'applicazione, anche tramite i loro concessionari, delle disposizioni in materia tributaria e doganale;

l) attività di controllo e ispettive;

m) concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni;

n) conferimento di onorificenze e ricompense, riconoscimento della personalità giuridica di associazioni, fondazioni ed enti, anche di culto, accertamento dei requisiti di onorabilità e di professionalità per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonché rilascio e revoca di autorizzazioni o abilitazioni, concessione di patrocini, patronati e premi di rappresentanza, adesione a comitati d'onore e ammissione a cerimonie ed incontri istituzionali;

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

p) obiezione di coscienza;

q) attività sanzionatorie e di tutela in sede amministrativa o giudiziaria;

r) rapporti istituzionali con enti di culto, confessioni religiose e comunità religiose;

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

t) attività amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale, ivi incluse quelle correlate ai trapianti d'organo e di tessuti nonché alle trasfusioni di sangue umano;

La casistica di cui al secondo comma dell'art. 2 sexies (3/3)

u) compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica;

v) programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale;

z) vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio e all'importazione di medicinali e di altri prodotti di rilevanza sanitaria;

aa) tutela sociale della maternità ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili;

bb) istruzione e formazione in ambito scolastico, professionale, superiore o universitario;

cc) trattamenti effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante, per fini di ricerca scientifica, nonché per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale (Sistan);

dd) instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunità nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilità civile, disciplinare e contabile, attività ispettiva.

Art. 2 sexies e il previgente art. 20 del Codice

Il previgente art. 20. «Principi applicabili al trattamento di dati sensibili» Abrogato

1. *Il trattamento dei dati sensibili da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite.*
2. *Nei casi in cui una disposizione di legge specifica la finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi e nel rispetto dei principi di cui **all'articolo 22, con atto di natura regolamentare adottato in conformità al parere espresso dal Garante ai sensi dell'articolo 154, comma 1, lettera g), anche su schemi tipo.***
3. *Se il trattamento non è previsto espressamente da una disposizione di legge **i soggetti pubblici possono richiedere al Garante l'individuazione delle attività, tra quelle demandate ai medesimi soggetti dalla legge, che perseguono finalità di rilevante interesse pubblico e per le quali è conseguentemente autorizzato, ai sensi dell'articolo 26, comma 2, il trattamento dei dati sensibili.** Il trattamento è consentito solo se il soggetto pubblico provvede altresì a identificare e rendere pubblici i tipi di dati e di operazioni nei modi di cui al comma 2.*
4. *L'identificazione dei tipi di dati e di operazioni di cui ai commi 2 e 3 è aggiornata e integrata periodicamente.*

Tutela dell’interessato e sanzioni (Parte III)

Agenda

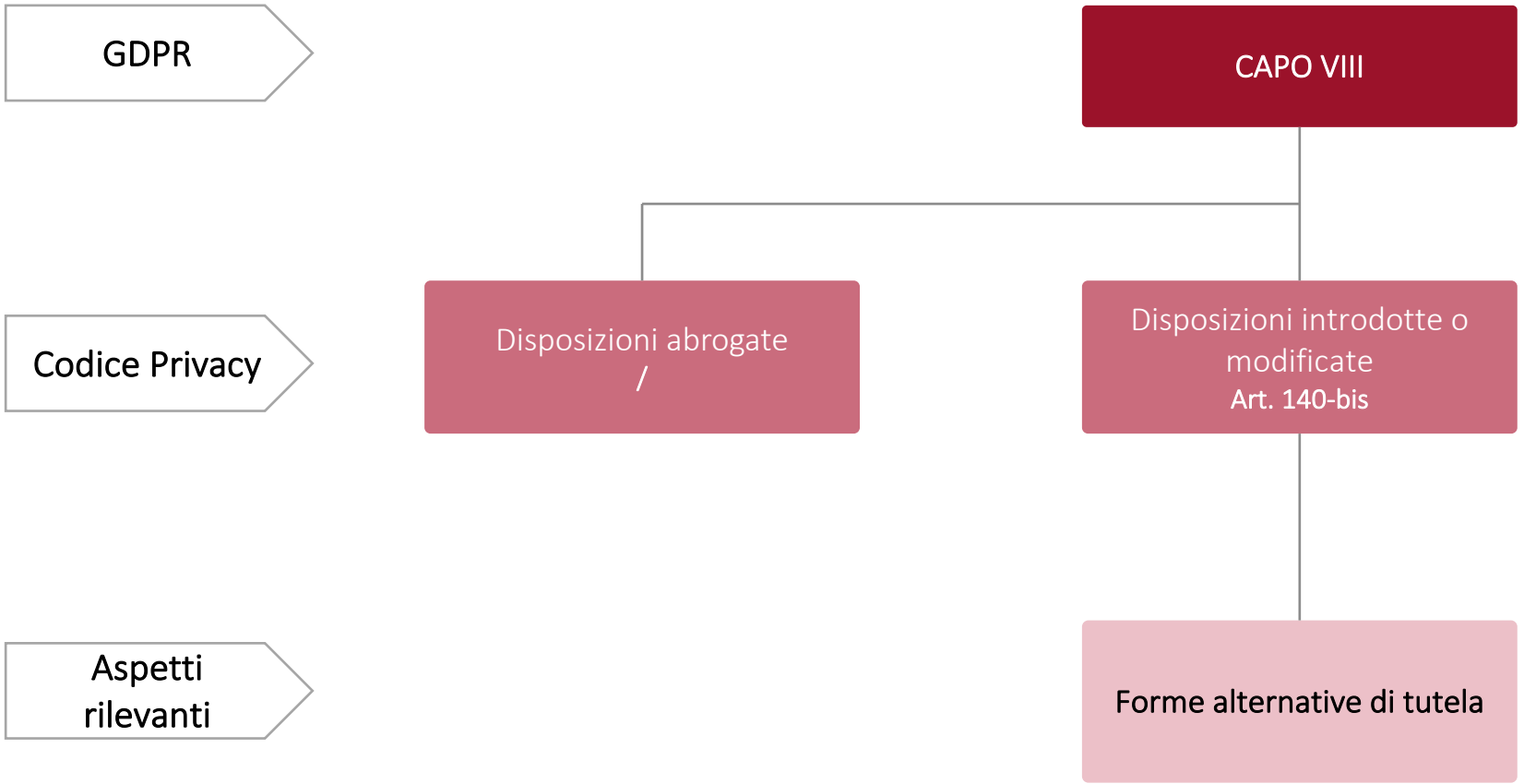
Tutela amministrativa e giurisdizionale (Titolo I)

- Tutela dinnanzi al Garante (Capo I)
- Tutela giurisdizionale (Capo II)

Autorità di controllo indipendente (Titolo II)

Sanzioni (Titolo III)

Quali sono gli aspetti più rilevanti per voi?



Articolo 140 bis

L'interessato se ritiene che siano stati violati i propri diritti può proporre:

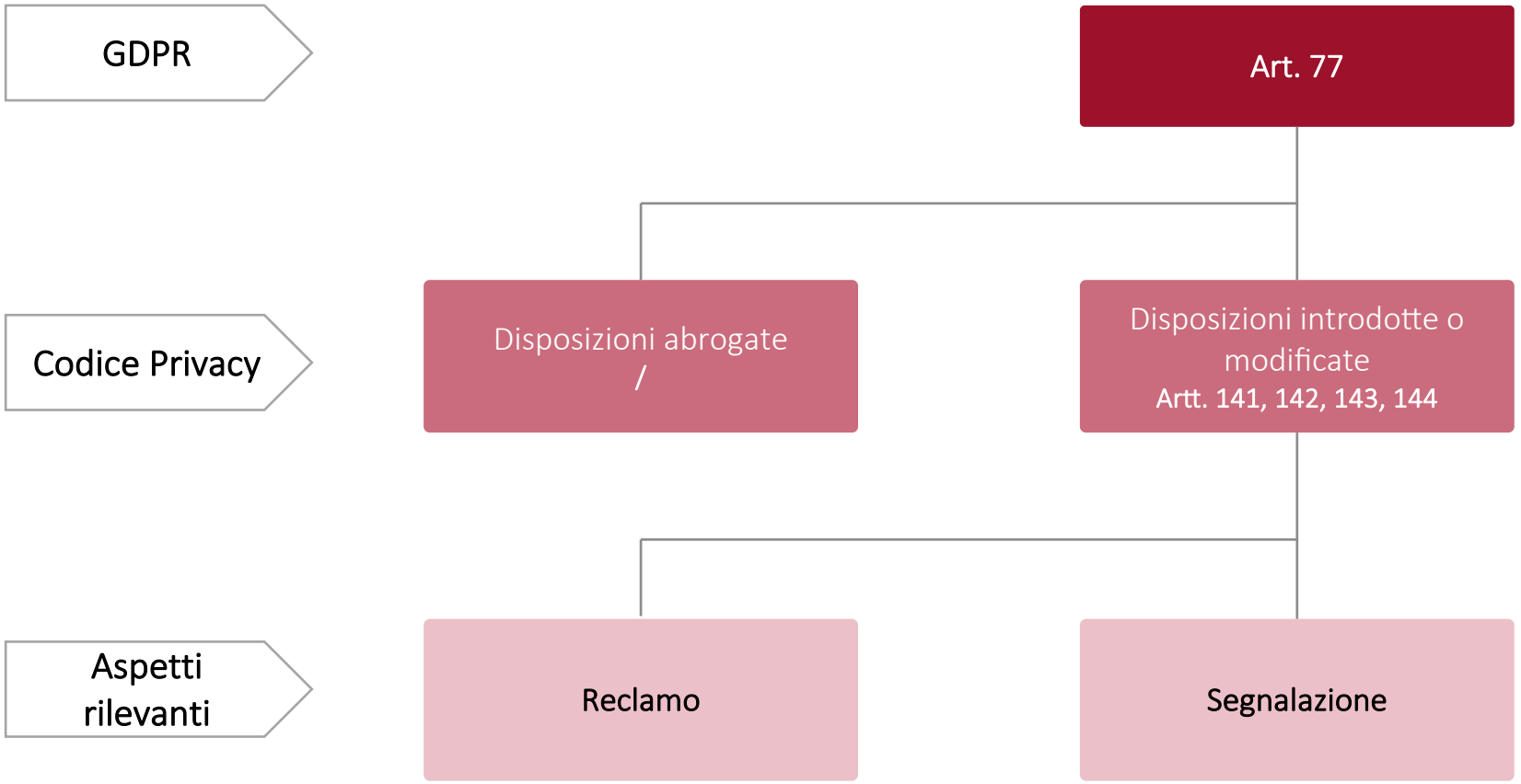
- **reclamo** al Garante
- **ricorso** all'Autorità Giudiziaria

Alternatività della tutela

Il reclamo non può essere proposto se, per lo stesso oggetto e fra le stesse parti, è stata già adita l'autorità giudiziaria

Analogamente la presentazione del reclamo al Garante rende improponibile la stessa domanda in sede giudiziaria

Quali sono gli aspetti più rilevanti per voi?



Reclamo e segnalazione al Garante (artt. 141, 142, 143, 144)

Reclamo

Può essere proposto solo dall'interessato

- **Deve contenere l'indicazione dei fatti e delle circostanze** su cui si fonda, delle disposizioni che si presumono violate e delle misure richieste
- **Va sottoscritto dall'interessato** o (previo mandato) da un «ente del terzo settore» (tra cui organizzazioni e associazioni no profit) → **una sorta di «class action»**
- **Il Garante decide il reclamo entro 9 mesi** dalla data di presentazione oppure, se presenti motivate esigenze istruttorie, entro 12 mesi…
- …ma nelle more, se il reclamo non appare manifestatamente infondato, può esercitare i **poteri correttivi e di indagine di cui all'art. 58 GDPR**
- avverso la decisione del Garante è ammesso **ricorso all'autorità giudiziaria**

Segnalazione

Può essere proposta da chiunque

(soggetti diversi dall'interessato)

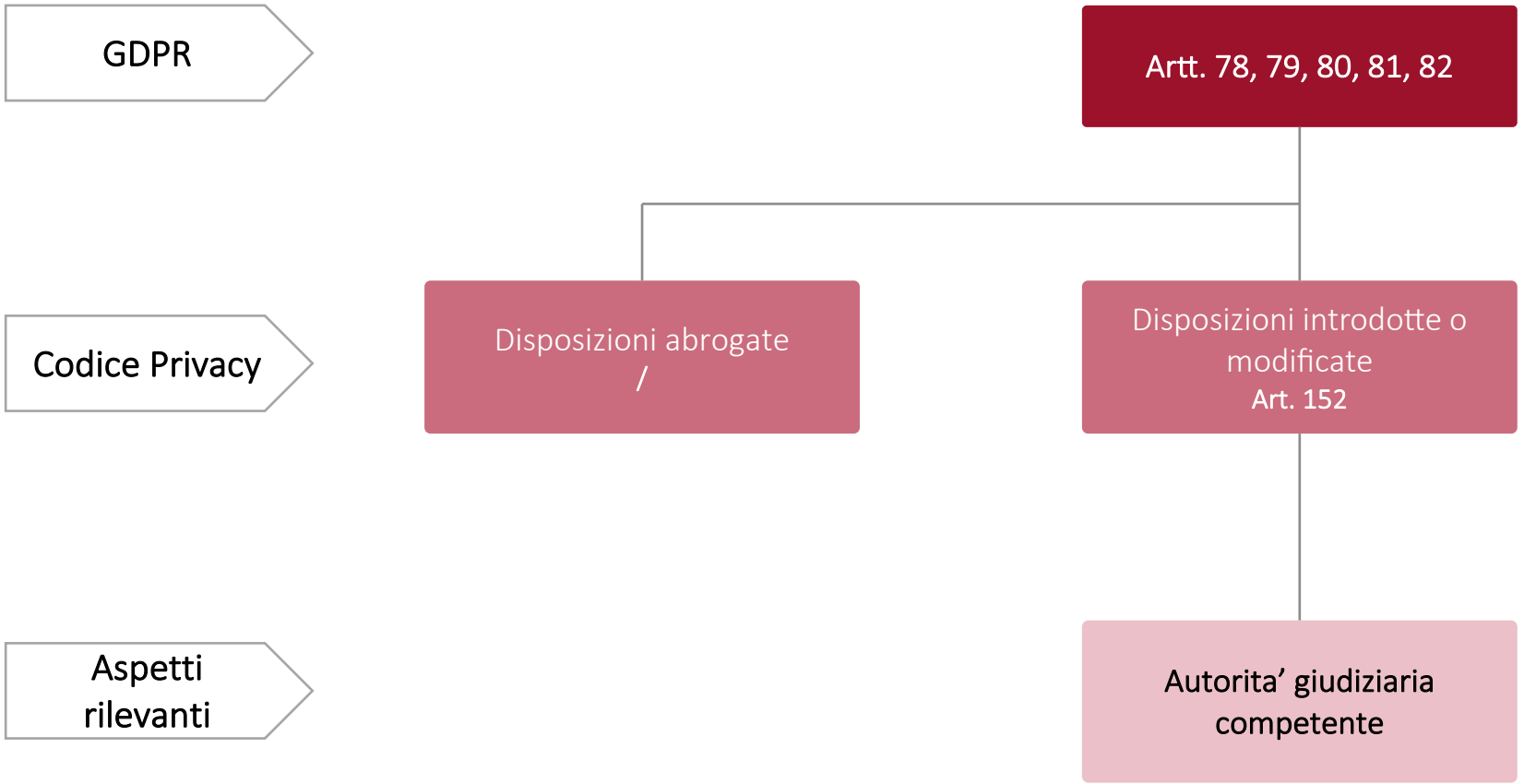
- **Serve a portare all'attenzione del Garante vicende anche a carattere collettivo e sociale** concernenti possibili violazioni della disciplina in materia di protezione dei dati personali, chiedendone l'intervento
- Sulla base della stessa il Garante può adottare **i provvedimenti di cui all'art. 58 GDPR**

Poteri dell'autorità di controllo (Art. 58, co. 2 GDPR)

Poteri correttivi e di indagine ai sensi del GDPR

- rivolgere avvertimenti
  sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni del presente regolamento
- rivolgere ammonimenti
  ove i trattamenti abbiano violato le disposizioni del GDPR
- ingiungere di soddisfare le richieste dell'interessato
  di esercitare i diritti loro derivanti dal GDPR
- ingiungere di conformare i trattamenti
  alle disposizioni del GDPR, se del caso, in una determinata maniera ed entro un determinato termine
- ingiungere di comunicare all'interessato una violazione dei dati personali
- imporre una limitazione provvisoria o definitiva al trattamento
  incluso il divieto di trattamento
- ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento
  a norma degli articoli 16, 17 e 18 e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali ai sensi dell'articolo 17, paragrafo 2, e dell'articolo 19;
- revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione
  rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti
- ordinare la sospensione dei flussi di dati extra UE

Quali sono gli aspetti più rilevanti per voi?



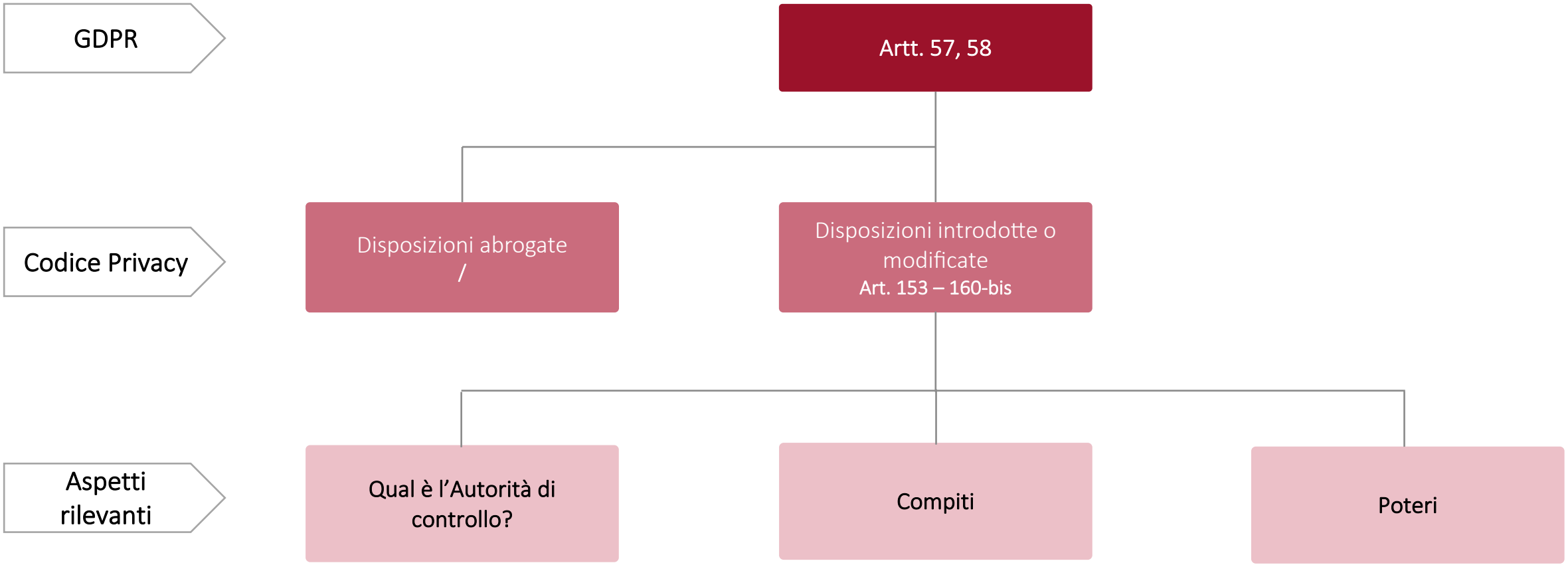
Autorità giudiziaria ordinaria (art. 152)

Alla **magistratura ordinaria** viene assegnata la **competenza** dell'**autorità giudiziaria** nelle materie di cui al GDPR (Rito del lavoro)

Controversie riguardanti:

- l'applicazione della normativa
  in materia di protezione dei dati personali;
- il diritto al risarcimento del danno
  causato da una violazione del Regolamento ai sensi dell'art. 82 GDPR
- le materie oggetto dei ricorsi giurisdizionali
  di cui agli artt. 78 e 79 del GDPR (sia nei confronti del Garante, sia nei confronti del titolare e del responsabile da parte dell'interessato direttamente che ritenga che i propri diritti siano stati violati)

Quali sono gli aspetti più rilevanti per voi?



GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Garante per la protezione dei dati personali (Artt. 2, 153, 154, 154 bis, 154 ter)

Il Garante è l'Autorità di controllo indipendente
a cui è affidato il compito di sorvegliare l'applicazione del GDPR
al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche ai sensi dell'art. 51 GDPR

I suoi **compiti** e **poteri** sono stati **rafforzati**

Compiti

Oltre a quanto previsto agli artt. 57 e 58 del GDPR:

- **Controllare** se i trattamenti vengono effettuati nel rispetto della disciplina applicabile
- **Trattare i reclami**
- **Promuovere l'adozione di «regole deontologiche»** di cui all'articolo 2-quater del Codice*
- **Denunciare i fatti**
  configurabili come reati perseguibili d'ufficio
- **Assicurare la tutela dei diritti e delle libertà** fondamentali degli individui

* *per i trattamenti per adempiere obblighi legali, per lo svolgimento di compiti di interesse pubblico e di dati genetici, biometrici o relativi alla salute e specifiche situazioni di trattamento)*

Poteri

Oltre a quanto previsto nella Sezione II del Capo IV del GDPR:

- **Agire in giudizio**
  nei confronti dei titolari o dei responsabili

Poteri a contenuto regolamentare:

- **Adottare linee guida di indirizzo**
  riguardanti le misure tecniche e organizzative anche per singoli settori e in applicazione dei principi di privacy by design/by default
- **Approvare le «regole deontologiche»**
  di cui all'articolo 2-quater del Codice

L'Autorità può promuovere, mediante linee guida, **modalità semplificate di adempimento** degli obblighi del titolare del trattamento per le micro, piccole e medie imprese

PMI

I poteri di accertamento del Garante (Artt. 157 e 158)

Richiesta di informazioni e di esibizione di documenti

- Il garante può chiedere al titolare, al responsabile, al loro eventuale rappresentante, all'interessato o anche a terzi di fornire informazioni e di esibire documenti anche con riferimento al contenuto di **banche di dati**

NEW

Accertamenti

- Il garante può disporre accessi a banche di dati, archivi o altre ispezioni e verifiche nei luoghi ove si svolge il trattamento o nei quali occorre effettuare rilevazioni utili al controllo del rispetto della disciplina in materia di trattamento dei dati personali
- Il garante si avvale, se necessario, della collaborazione di altri organi dello Stato per lo svolgimento dei suoi compiti istituzionali

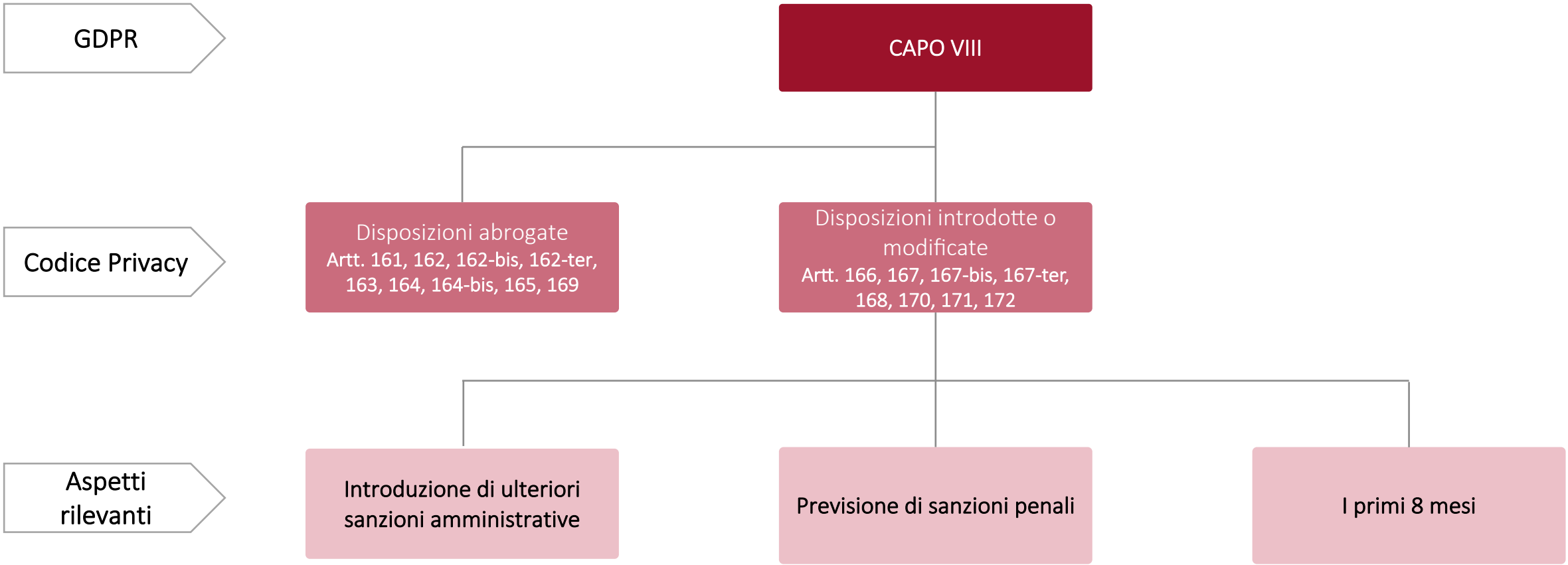
NEW

Ai controlli possono prendere parte, se del caso, componenti o personale di autorità di controllo di altri Stati membri dell'Unione Europea.

NEW

Gli accertamenti possono essere effettuati anche sulle reti di comunicazione accessibili al pubblico, potendosi procedere all'acquisizione di dati e informazioni on line.

Quali sono gli aspetti più rilevanti per voi?



Disciplina sanzionatoria

Dal combinato disposto del GDPR e del Codice emerge una articolata, oltre che pesante, disciplina sanzionatoria, che prevede:

- sanzioni amministrative
- sanzioni penali

Violazioni amministrative nel GDPR (Art. 83)

L'art. 83 del GDPR distingue
due gruppi di sanzioni amministrative

Sanzioni più alte

fino a € **20.000.000** o
al **4%** del fatturato globale annuo

- **violazione delle obbligazioni di titolare e responsabile** incluso gli obblighi di sicurezza e data breach notification (art. 83, par. 4 del GDPR)

Sanzioni più basse

fino a €. 10.000.000 o,
in caso di undertaking, al 2% del fatturato,
a seconda di quale risulti la sanzione più elevata

- **violazioni dei principi del trattamento**, incluse le condizioni per il consenso
- **violazione dei diritti degli interessati**
- **inosservanza delle norme in tema di trasferimento internazionale dei dati** (art. 83, par. 5 del GDPR)

La sanzioni non sono imposte in riferimento al fatturato della specifica società responsabile della violazione, ma alle revenue di un **"undertaking",** da intendersi, come chiarito dal WP29 n. 253, come gruppo di imprese

Violazioni amministrative introdotte dal decreto (Art. 166 Codice Privacy novellato)

Il GDPR consente agli Stati membri di prevedere ulteriori sanzioni, in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie di cui all'art. 83, a condizione che esse siano sempre «***effettive, proporzionate e dissuasive***» (art. 84).

In virtù di tale facoltà, il d.lgs. 101/2018 ha previsto sia **sanzioni penali**, che ulteriori fattispecie di illeciti soggetti alle sanzioni amministrative di cui all'art. 83 del GDPR.

Violazioni amministrative introdotte dal decreto (Art. 166, co. 1, Codice Privacy novellato)

FATTISPECIE CON SANZIONE PIÙ BASSA

- **violazione dell'obbligo di redigere un'informativa con linguaggio semplificato per i minori** (Art. 2, quinquies, co. 2)
- **violazione dei provvedimenti generali del Garante** con riguardo a **trattamenti per l'esecuzione di un compito di interesse pubblico che presentano rischi elevati** (Art. 2-quinquiesdecies)
- Violazioni relativi alle cartelle cliniche (**Art. 92, co. 1**) e a certifica certificati di assistenza al parto (**Art. 93, co. 1**)
- **Violazioni di norme relative ai servizi di comunicazione elettronica** (quali l'**Art. 123, co. 4** sull'informativa inerenti ai dati di traffico), l'**Art. 128 su**l trasferimento automatico delle chiamate , l'**Art. 129, co.2** sugli elenchi dei contraenti, l'**Art. 132-ter** sulla *a*lla sicurezza dei trattamenti effettuati da fornitori di servizi di comunicazione elettronica
- mancata effettuazione della valutazione di impatto di cui all'art. 110, co. 1, primo periodo per le **attività di ricerca medica, biomedica o epidemiologica** ovvero mancata sottoposizione del programma di ricerca a consultazione preventiva del Garante a norma del terzo periodo del predetto comma

10 milioni di euro

o

2% fatturato mondiale annuo

(art. 83, par. 4, GDPR)

Violazioni amministrative introdotte dal decreto (Art. 166, co. 2, Codice Privacy novellato)

FATTISPECIE CON SANZIONE PIÙ ALTA

- Violazione dell'*art. 2-ter* relativo alla base giuridica del trattamento effettuato per **l'esecuzione di un compito di interesse pubblico**
- Violazione dell'*art. 2-quinquies, co. 1* riguardante **il consenso del minore in relazione ai servizi della società dell'informazione**
- Violazioni *dell'Art. 2-sexies* relativo al trattamento di **categorie particolari di dati per motivi di interesse pubblico rilevante**
- Violazione delle misure di garanzia per il trattamento dei **dati biometrici** riguardo alle **procedure di accesso fisico e logico** da parte dei soggetti autorizzati (*art. 2-septies, co. 7)*
- Violazione dei principi relativi al trattamento di dati relativi a condanne penali e reati (*Art. 2-octies*)
- Violazione dei **diritti riguardanti le persone decedute** (*Art. 2-terdecies, co. 1, 2, 3 e 4*)
- Violazione della disciplina sulla **diffusione di provvedimenti giudiziari contenenti dati identificativi degli interessati** (*art. 52, co. 4 e 5*)
- Violazione degli adempimenti previsti per il **trattamento dei dati in ambito sanitario** (*Art. 75-78-79-80-82-92, co. 2- 93, co. 2 e 3)*
- Violazione della disciplina sul **trattamento dei dati relativi a studenti** (*Art. 96*)
- Violazione di disposizioni in materia di **trattamento dei dati a fini di archiviazione nel pubblico interesse, ricerca scientifica o storica o a fini statistici** (*Art. 99, 100, co. 1, 2 e 4, 101, 105, co. 1, 2 e 4, 110-bis, co. 2 e 3)*

20 milioni di euro

o

4% fatturato mondiale annuo

(art. 83, par. 5, GDPR)

Violazioni amministrative introdotte dal decreto (Art. 166, co. 2, Codice Privacy novellato)

FATTISPECIE CON SANZIONE PIÙ ALTA

- Violazione delle disposizioni riguardanti il trattamento nell'ambito del lavoro (a*rt. 111-111-bis -116, co. 1)*
- Violazione dell'Art.120, co.2 relativo alle assicurazioni (banca dati dei sinistri)
- Violazioni di quasi tutte le previsioni relativa ai servizi di comunicazioni elettroniche (*artt.-122, 123, co. 1, 2, 3 e 5, 124, 125, 126-130, co. 1, 2, 3, 4 e 5,131, 132, 132-bis, co. 2,132-quater)*
- Violazione della disposizione in materia di **richiesta di informazioni e di esibizione di documenti** da parte del **Garante** (*Art. 157*)
- Violazione delle **regole deontologiche** di cui all'*art. 2-quater* previste per i trattamenti necessari per adempiere un obbligo legale o per l'esecuzione di un compito di interesse pubblico (Art. 6, par. 1, lett. c) ed e) GDPR), per il trattamento di dati genetici e biometrici relativi alla salute (Art. 9, par. 4 GDPR) e delle disposizioni di cui al Capo IX del GPDR relative a specifiche situazioni di trattamento di cui il Garante promuove l'adozione;
- Violazione delle **misure di garanzia** disposte dal Garante per il trattamento di dati genetici e biometrici relativi alla salute di cui all'*art. 2-septies*

20 milioni di euro

o

4% fatturato mondiale annuo

(art. 83, par. 5, GDPR)

Esempi:

Omissione di un idoneo recapito per l'esercizio dei diritti all'interno di una mail promozionale (Art. 130, co. 5)

Mancato rilascio dell'informativa privacy all'interessato, in occasione del primo contatto, nel caso di CV ricevuti spontaneamente (Art. 111-bis)

Procedimento sanzionatorio (Art. 166, co. 3-10)

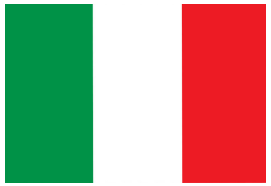
Organo competente ad irrogare le sanzioni è il Garante, il quale dovrà tener in debito conto le circostanze di cui all'art. 83, co. 2 GDPR, ossia:

- la natura, la gravità e la durata della violazione,
- il carattere doloso o colposo della stessa,
- le categorie di dati personali interessate dalla violazione,
- eventuali precedenti violazioni commesse ecc.

I proventi delle sanzioni, nella misura del **50%** del totale annuo, sono riassegnati al fondo destinato alle spese di funzionamento del Garante, per essere destinati alle specifiche attività di sensibilizzazione e di ispezione, nonché di attuazione del Regolamento.

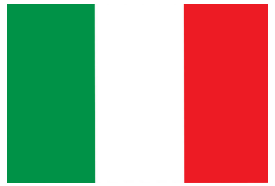
Illeciti penali: Introduzione

Il GDPR consente agli Stati Membri di stabilire «***altre sanzioni***» per le violazioni del GDPR, "*in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'articolo 83*" (art. 84 co.1 GDPR)



Una delle critiche rivolte al precedente schema di decreto era quella di aver non aver previsto sanzioni penali, **depenalizzando la fattispecie di «trattamento illecito dei dati»….**

Precedente schema:
Depenalizzazione



… invece la scelta da ultimo effettuata dal legislatore italiano è stata quella di avvalersi della facoltà, concessa dal GDPR, di prevedere **sanzioni penali** per alcune violazioni della normativa sulla privacy, sia modificando le fattispecie penalmente rilevanti già previste dal Codice Privacy che introducendo ulteriori violazioni.

Attuale versione:
Previsione di sanzioni penali

L'imposizione di sanzioni penali e di sanzioni amministrative «***non dovrebbe essere in contrasto con il principio*** *del* ***ne bis in idem*** *quale interpretato dalla Corte di giustizia*" (considerando 149), che ha censurato casi in cui gli ordinamenti nazionali avevano previsto per le medesime violazioni sia sanzioni **amministrative** che **penali**

Illeciti penali: prima e dopo

Vecchio codice	Nuovo codice
Trattamento illecito di dati (Art. 167)	Trattamento illecito di dati (Art. 167) RIFORMULATO
/	Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala (Art. 167-bis) NEW
/	Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala (Art. 167-ter) NEW
Falsità nelle dichiarazioni e notificazioni al Garante (Art. 168)	Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante (Art. 168)
Omissione delle misure minime di sicurezza (Art. 169)	ABROGATO
Inosservanza di provvedimenti del Garante (Art. 170)	Inosservanza di provvedimenti del Garante (Art. 170)
Altre fattispecie (art. 171)	Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori (Art. 171)

Illeciti penali: trattamento illecito di dati (Art. 167)

Chiunque,
al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato:

→ REATI A DOLO SPECIFICO

ARRECA NOCUMENTO ALL'INTERESSATO

Art. 167, co. 1

Servizi di comunicazioni elettroniche

Violando le norme relative ai **dati di traffico**, ai dati relativi all'ubicazione, all'invio delle comunicazioni indesiderate e il provvedimento del Garante in tema di elenchi cartacei elettronici a disposizioni del pubblico ***(condotte inalterate rispetto al previgente art. 167)***

è punito con → Reclusione **da 6 mesi a 1 anno**

Art. 167, co. 2

Categorie particolari di dati e dati «giudiziari»

Trattando **categorie particolari di dati** o **dati relativi a condanne penali e reati** in violazione dell'artt. 2-sexies e 2-octies o delle misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute (art. 2-septies) ovvero operando in violazione delle misure prescritte dal Garante per i trattamenti svolti per l'esecuzione di un compito di interesse pubblico che possono presentare rischi elevati (art. 2-quinquiesdecies)

Art. 167, co. 3

Trasferimento extra-UE

Procedendo al **trasferimento dei dati extra-UE** al di fuori dei casi consentiti dal Regolamento ***(condotta già espressamente sanzionata in via amm. dal GDPR all'art. 83, 5° co.)***

è punito con → Reclusione **da 1 a 3 anni**

Salvo che il fatto costituisca più grave reato

Illeciti penali: Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala (Art. 167-bis) e acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala (Art. 167-ter)

Chiunque,
al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato:

→ REATI A DOLO SPECIFICO

Art. 167-bis, co.

Comunica o diffonde un archivio automatizzato o una parte sostanziale di esso contenente dati personali trattati **su larga scala**

è punito con → Reclusione **da 1 a 6 anni**

Art. 167-bis co. 2

Comunica o diffonde, senza consenso (laddove questo sia richiesto) un archivio automatizzato o una parte sostanziale di esso contenente dati personali trattati **su larga scala**

è punito con → Reclusione **da 1 a 6 anni**

Art. 167-ter, co. 1

acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento **su larga scala**

è punito con → Reclusione **da 1 a 4 anni**

"LARGA SCALA"

Da notare che né il GPPR né il decreto contengono una definizione di "*larga scala*", tantomeno le linee guida del Working Party ex art. 29 chiariscono in modo certo e definitivo cosa debba intendersi con tale locuzione, offrendo criteri alternativi non fondati su elementi quantitativi, ma su indicazioni generiche suscettibili di diversa interpretazione.

Salvo che il fatto costituisca più grave reato

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

Art. 168, co. 1

Chiunque in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi

→ è punito con → Reclusione **da 6 mesi a 3 anni**

Art. 168, co. 2

Chiunque intenzionalmente cagiona una interruzione o turba la regolarità di un procedimento dinanzi al Garante o degli accertamento svolti da esso

→ è punito con → Reclusione **sino ad 1 anno**

Salvo che il fatto costituisca più grave reato

Illeciti penali: Inosservanza di provvedimenti del Garante (Art. 170) E Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori (Art. 171)

Art. 170

Chiunque , essendovi tenuto, non osserva il provvedimento con cui il Garante:

- impone una limitazione provvisoria o definitiva al trattamento incluso il divieto (**Art. 58, par. 2, lett. f**) del Regolamento)
- dispone le misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute (**Art. 2-septies, co. 1**)
- individua le prescrizioni contenute nelle proprie autorizzazioni generali già adottate compatibili con il GDPR e il Codice (**Art. 21, co.1, d.lgs. 101/2018**) e, eventualmente procede al loro aggiornamento

è punito con → Reclusione **da 3 mesi a 2 anni**

Art. 171

Le violazioni delle disposizioni di cui agli articoli 4, comma 1, e 8 della legge 20 maggio 1970, n. 300

è punito con → **Sanzioni ex. Art. 38 l. 300/1970**

Le sanzioni in sede di prima applicazione

Il decreto, recependo le richieste pervenute da più parti anche in sede di audizioni parlamentari, contiene all'art. 22, co 13, una norma "cuscinetto" riferita all'applicazione delle sanzioni:

Per i **primi otto mesi** dalla data di entrata in vigore del decreto, il Garante **terrà conto, ai fini dell'applicazione delle sanzioni amministrative e nei limiti in cui risulti compatibile con le disposizioni del GDPR, della fase di prima applicazione delle disposizioni sanzionatorie**.

La norma non appare di facile interpretazione, dato che non contiene alcun riferimento o limite preciso alla potestà sanzionatoria del Garante.

In ogni caso, **non si tratta di un rinvio di otto mesi** dell'applicazione della normativa da parte del Garante, come richiesto da Camera e Senato, **ma di un'opera di "*moral suasion*" del legislatore** nei confronti del Garante, una raccomandazione di non applicare in maniera severa, ma *soft* le sanzioni amministrative nella prima fase di applicazione del decreto, senza prevedere l'invalidità di eventuali provvedimenti adottati in contrasto alla previsione e facendo comunque salvo il limite della compatibilità alle previsioni del GDPR.

Ciò riguarda in ogni caso solo la potestà sanzionatoria del Garante. Rimane ferma, ovviamente, la facoltà degli interessati di adire l'Autorità giudiziaria per ottenere il risarcimento del danno, anche tramite «class action».

Conclusioni

Il quadro normativo della disciplina della protezione dei dati personali nel nostro paese: non è ancora completo ed esaustivo:

- Il decreto prevede (e rinvia a)
  - **regole deontologiche**,
  - **codici di condotta**,
  - **misure di garanzie**,
  - provvedimento sulle **autorizzazioni generali**
  - **altri provvedimenti del Garante**;
- Il futuro **Regolamento e-Privacy**, che dovrebbe vedere la luce per la fine del 2018 o agli inizi del 2019, comporterà ulteriori modifiche

Conclusioni

Difficoltà interpretative e possibili controversie attuative :

possibili ricorsi alla Corte Costituzionale o

ricorsi alla Corte di giustizia per non conformità della normativa italiana al GDPR o per violazione del principio del *ne bis in idem* o

Possibilità di disapplicazione della normativa interna non conforme da parte dei giudici nazionali

Da notare che intanto la normativa nazionale è legittima se:

- rientra nelle materie rimesse dal GDPR alla competenza del legislatore nazionale;
- Il suo contenuto è conforme al GDPR;
- è interpretata ed applicata in conformità con il GDPR.

→ il GDPR rappresenta il parametro di legittimità della normativa nazionale, oltre che la disciplina primaria della materia.

Conclusioni

Rischio di aumento dei contenziosi

- sia per la possibilità di ricorsi sia al Garante che all'AG da parte di enti del terzo settore per conto degli interessati («class action»),
- sia per la legittimazione del Garante ad agire in giudizio nei confronti del Titolare o del Responsabile

↓

problematiche interpretative sulle **misure** da attuare per ridurre il rischio sanzionatorio.

Impatti del D.Lgs 101/2018 sulle Aziende: cosa succede adesso

Il nostro Modello per la convergenza delle Compliance

Un Modello di Compliance consente di **mappare e classificare i requisiti di Normative e Standard in funzioni delle principali dimensioni aziendali**, facilitandone la comprensione e favorendo l'individuazione di azioni concrete da implementare

- Normative e Standard
- Organizzazione e Ruoli
- Persone, Cultura e Competenze
- Processi e Regole
- Documentazione
- Dati, Sistemi e Sicurezza
- Rischi e Controlli

L’impatto del D.lgs. 101/2018

- Attribuzione di funzioni e compiti a soggetti designati
- Adeguamento delle modalità di autorizzazione al trattamento
- Valutazione delle deleghe in relazione ai rischi di sanzioni penali connessi all’esercizio delle stesse

- Revisione dell’analisi del rischio di non conformità alla luce delle sanzioni penali introdotte
- Verifica della rispondenza del sistema dei controlli ai nuovi livelli di rischio

- Definizione di istruzioni per la corretta gestione del consenso dei minori e per la verifica dell’età dichiarata
- Definizione di istruzioni per la gestione dei dati personali relativi a persone decedute

- Applicazione delle misure di garanzia per il trattamento dei dati particolari di cui all’art. 9 (biometria, dati genetici e salute) da provvedimento del Garante (verificare impatto su registro, informative e nomine a responsabile esterno)

- Applicazione dei criteri di identificazione dei dati giudiziari e conseguente eventuale revisione del registro e delle informative
- Verifica dell’utilizzo dell’interesse pubblico come base legale per i trattamenti e conseguente eventuale revisione del registro e delle informative
- Informative rivolte ai minori

L’impatto del D.lgs. 101/2018 - La dimensione internazionale

- Verifica dei provvedimenti adottati a livello dei singoli stati membri negli ambiti delegati. Esempio:
  - Diverse età dei minori
  - Potenzialmente diverse misure di garanzia per il trattamento di particolari categorie di dati

P4.I

PARTNERS4.INNOVATION

DIGITAL 360 | Group