Privacy e Sicurezza Informatica nella scuola: il regolamento europeo in materia di protezione dei dati personali GDPR UE 679/2016 D.Lgs 101/2018 (modifiche al 196/2003)

Avv. Rita Di Carlo
Specializzata in Privacy e Data Protection Office

- Evoluzione normativa
- Entrata in vigore ed efficacia
- Le novità del GDPR 679/2016
- Ruoli e responsabilità nel sistema GDPR
- Privacy e scuola
- Diritti dell'interessato
- Sanzioni

Evoluzione normativa in Europa

1995 Directive 95/46/EC - Prima Direttiva europea su Data protection

Evoluzione normativa in Italia

1996: prima legge sulla protezione dei dati personali. Obbligo di adozione di misure «minime» di sicurezza e di misure «idonee». Per la prima volta i «dati personali» potevano essere trattati seguendo regole ben determinate.

-Pregio: grandissima valenza educativa

-Difetto: ampiezza e disomogeneità della normativa

- **2003**: **D.lgs 196/03** ha riaccorpato la normativa (è ancora la normativa in vigore). Le misure minime di sicurezza sono previste dall'Allegato B. Seguono numerosi provvedimenti che prevedono misure di sicurezza e condizioni per una serie di trattamenti e per settori di mercato
  - -Pregio: distinzione per settori di mercato
  - -Difetto: scarsa capacità della norma di adeguarsi alle evoluzioni tecnologiche

- **2018**: **Regolamento UE**. Il tema della sicurezza passa da una logica di «minimo» a una logica di «adeguato» in base ai rischi concreti. Ogni azienda o pubblica amministrazione deve analizzarsi e decidere come posizionarsi

La Fonte

DIRETTIVA (1995)

Per l'esecutività richiede un recepimento di atti normativi nazionali

REGOLAMENTO (2016)

Self Executing

Diretta applicabilità in tutti gli Stati membri

Garanzia di uniformità e coerenza

DIRETTIVA

REGOLAMENTO

DECRETO LEGISLATIVO 10 agosto 2018, n. 101

Disposizioni per l'**adeguamento** della normativa nazionale alle disposizioni del **regolamento (UE) 2016/679** del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

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

Entratato in vigore del provvedimento: **19/09/2018**

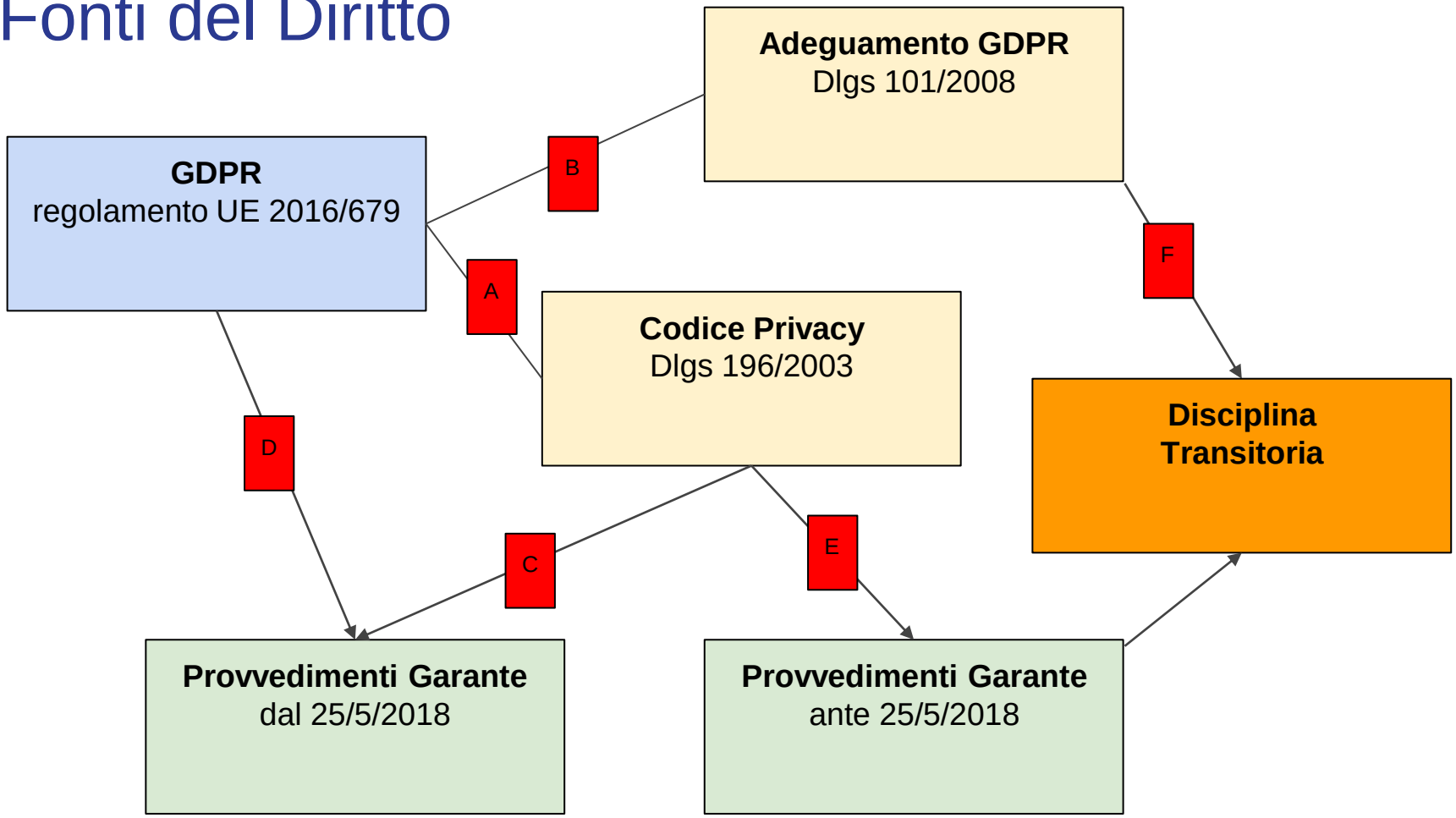
Cosa contiene il Dlgs 101/2018

Modifiche Dlgs 196/2003	Abrogazioni Dlgs 196/2003	Nuove disposizioni
Molti articoli del Codice della Privacy (Dlgs 196/2003) vengono corretti per adattarli alla nuova terminologia del GDPR	L'intervento più significativo riguarda le abrogazioni sia al Dlgs 196/2003 (le più importanti) che ad altre disposizioni	Gli articoli 17 e seguenti del Dlgs 101/2018 sono "norme nuove" e come tali non si ritrovano nel Dlgs 196/2003

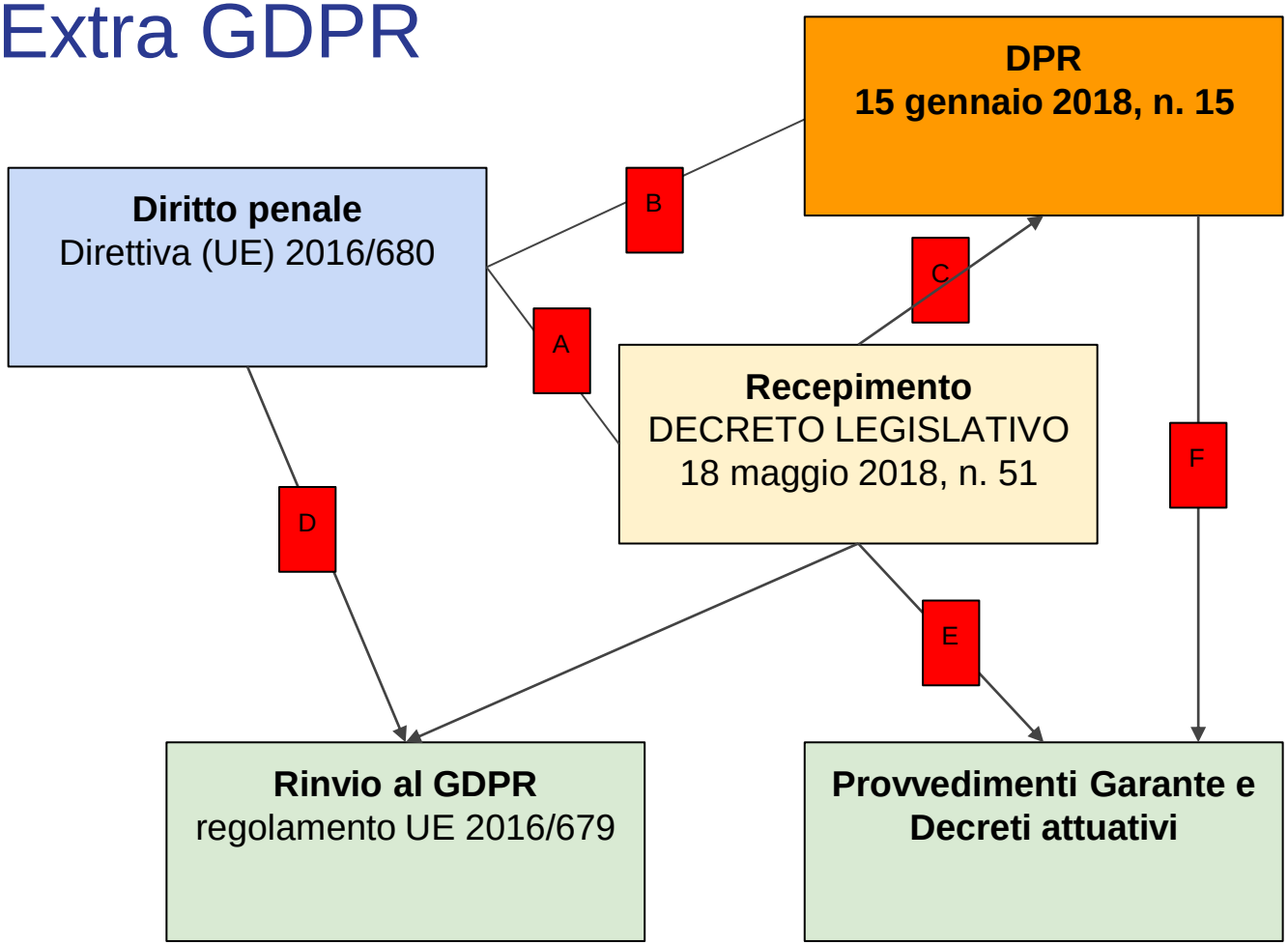
Cosa NON contiene il Dlgs 101/2018

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

Fonti del Diritto



Extra GDPR


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

Entrata in vigore ed Efficacia territoriale del Regolamento

La Struttura

- TESTO
- CONSIDERANDO
- N. 99
- N. 173

Disposizioni generali

Principi

Diritti dell'interessato

Titolare e Responsabile del trattamento

Trasferimenti di dati personali verso paesi

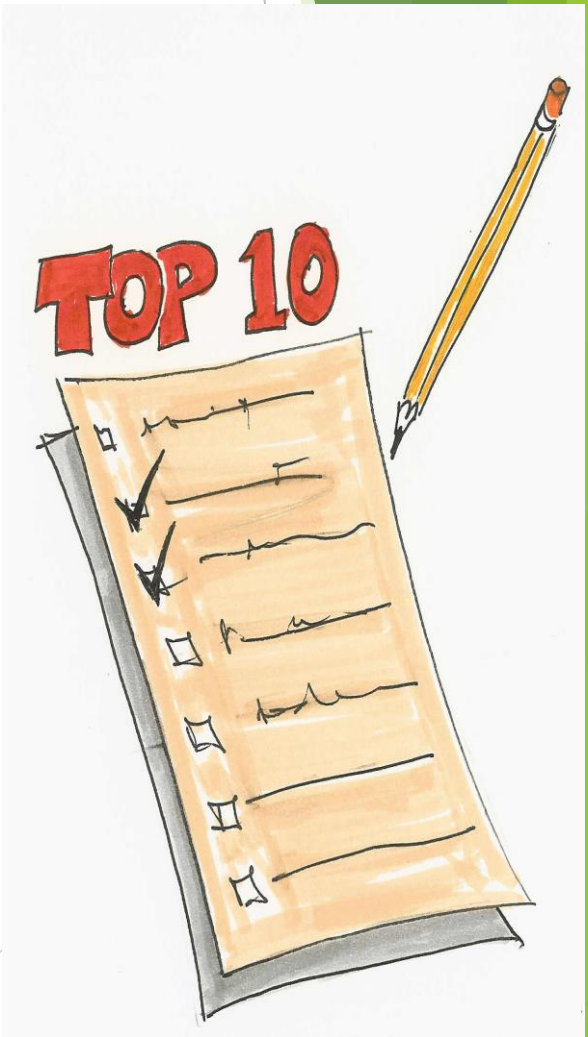
Autorità di controllo indipendenti

Cooperazione e coerenza

Ricorsi, responsabilità e sanzioni

Specifiche situazioni di trattamento dati

Disposizioni finali



Le assolute novità in sintesi

Accountability

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di *dimostrare*, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

Protezione sin dalla progettazione

Le misure a protezione di dati devono essere adottate già al momento della progettazione di un processo di lavoro o sistema IT al fine di garantire in ogni caso che siano trattati solo i dati necessari per ogni specifica finalità.

Registro dei trattamenti

Elenco dei dati trattati, delle finalità del trattamento, delle categorie di interessati, dei destinatari di comunicazione, degli eventuali trasferimenti verso Paesi terzi e delle misure di sicurezza.

Responsabile della protezione dei dati

DPO: figura indipendente nell'ambito dell'ente .
Informa e consiglia il Titolare o il Responsabile in merito agli obblighi del Regolamento, ne verifica l'applicazione e l'attuazione, fornisce pareri, funge da punto di contattato sia con gli interessati che con il Garante.

Responsabilità solidale tra Titolare e Responsabile

Il Titolare e il Responsabile del trattamento sono responsabili in solido nei confronti dell'interessato per eventuali danni causati dal trattamento.

Responsabilità dei Contitolari

I contitolari del trattamento possono essere responsabili parziari (non solidali) solo allorché abbiano determinato in modo trasparente e completo le rispettive responsabilità.

Designazione di Sub responsabili del trattamento

Il Titolare può autorizzare il Responsabile a nominare Sub Responsabili del trattamento a determinate condizioni.

Violazione di dati

Nel caso si verifichino violazioni di dati personali, il Titolare ne deve dare comunicazione all'Autorità di Controllo e, nei casi più gravi, anche agli interessati.

Eliminazione dell'obbligo di notifica	Viene eliminato l'obbligo generale di notificare all'autorità di controllo.
Valutazione d'impatto	È la valutazione del rischio da trattamento dati. Necessita di alcune attività come la mappatura dei dati e dei trattamenti, la pianificazione degli interventi tecnologici e organizzativi di protezione dei dati con una valutazione complessiva di riduzione dello stato di rischio
Certificazioni	Attestano la conformità delle operazioni di trattamento dei dati al Regolamento.
Diritto all'oblio	Diritto dell'interessato di ottenere la cancellazione dei dati che lo riguardano, purché non sussistano motivi legittimi per conservarli.
Trattamento e consenso per i minori di anni 16	Per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore, tale trattamento è lecito soltanto se il consenso è prestato o autorizzato dal titolare della potestà genitoriale.

Diritto alla portabilità dei dati

Possibilità per l'interessato di ricevere i propri dati personali in un formato strutturato, leggibile da dispositivo automatico e di uso comune.

Entità delle sanzioni

Parametrate sul fatturato.

Pseudonimizzazione

Sostituzione di nome e cognome con codici.
Conservazione di chiave di lettura dei codici in data base separato.

Ruoli e responsabilità nel sistema GDPR

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

Restano sostanzialmente invariati

- Definizione di trattamento e dato personale
- Principi relativi al trattamento di dati
- Informativa
- Consenso
- Protezione delle sole persone fisiche

Art. 4 n. 1 del RGPD
(Definizione di DATO PERSONALE)

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

Art. 4 n. 2 del RGPD
(Definizione di TRATTAMENTO)

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

Art. 5 del RGPD

(PRINCIPI applicabili al trattamento di dati)

I dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («**liceità, correttezza e trasparenza**»);

b) raccolti per **finalità determinate, esplicite e legittime**, e successivamente trattati in modo compatibile con tali finalità;

(PRINCIPI applicabili al trattamento di dati)

I dati personali sono:

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («**minimizzazione dei dati**»);

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («**esattezza**»);

(PRINCIPI applicabili al trattamento di dati)

I dati personali sono:

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati … («**limitazione della conservazione**»);

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione da trattamenti non autorizzati/illeciti e dalla perdita, dalla distruzione o dal danno accidentale («**integrità e riservatezza**»).

Art. 6 del RGPD
(Liceità del trattamento)

Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

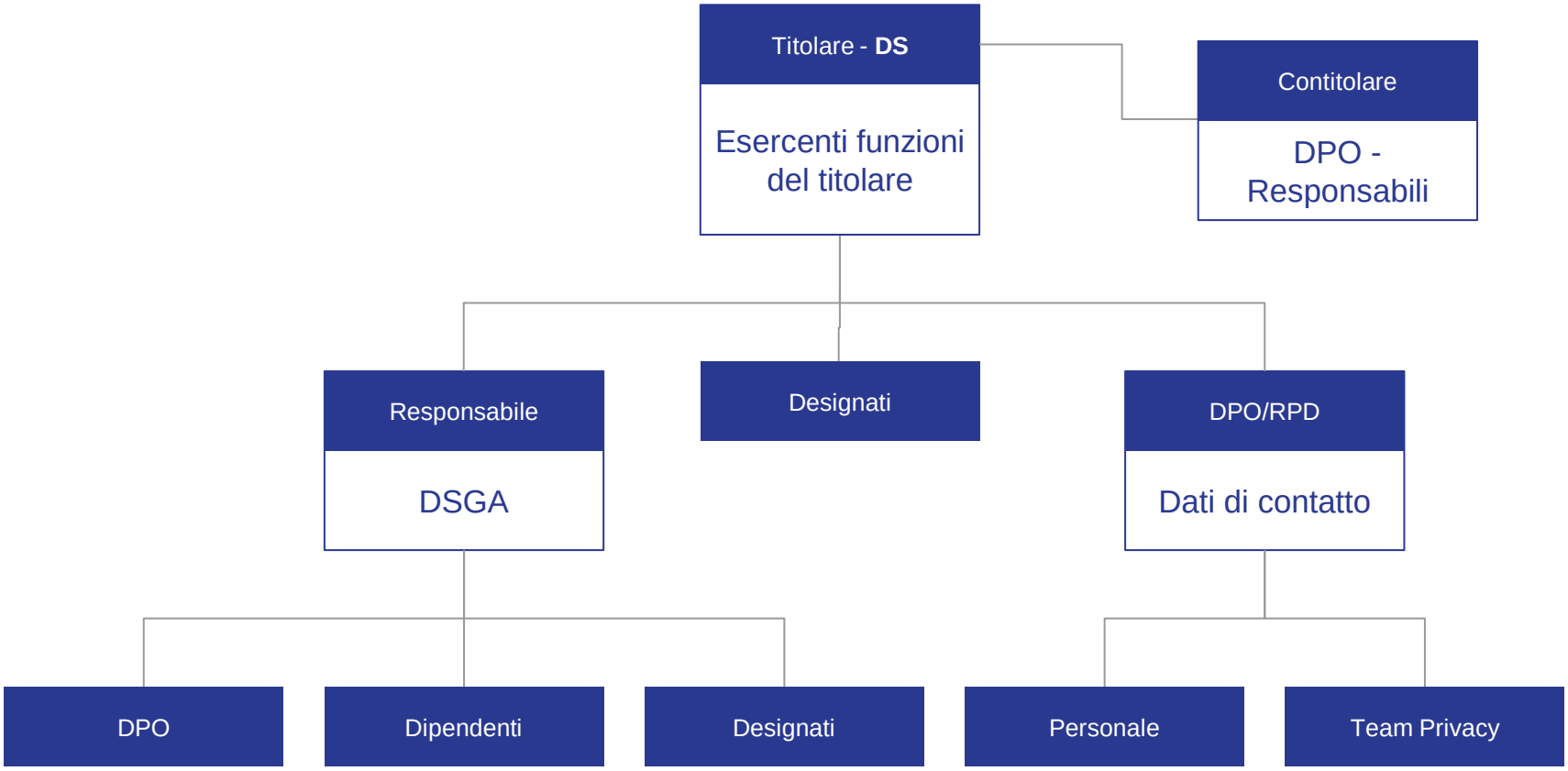
a) l'interessato ha **espresso** il **consenso** al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento ***è necessario all'esecuzione di un contratto*** di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento **è necessario per adempiere un obbligo legale** al quale è soggetto il titolare del trattamento;
d) il trattamento **è necessario per la salvaguardia degli interessi vitali** dell'**interessato** o di un'altra persona fisica;
e) il trattamento **è necessario per l'esecuzione di un compito di interesse pubblico** o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
f) il trattamento **è necessario per il perseguimento del legittimo interesse del titolare** del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Privacy e scuola

Adempimenti essenziali:

- Nomina DPO / RPD
- Registro dei trattamenti
- Valutazione d'impatto dei trattamenti
- Informative
- Sicurezza trattamenti

Organigramma



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

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

Informazioni e informativa

GDPR (considerando 60)	Elementi	GDPR (art. 13-14)
I principi di trattamento corretto e trasparente implicano che l'interessato sia **informato** dell'esistenza del trattamento e delle sue finalità	**Identità e dati di contatto** del titolare, DPO Finalità Destinatari Periodo di conservazione Diritti	Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato

Informazioni

Raccolta dati

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

Informazioni

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

Consenso

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

Consenso - GDPR (considerando 32)

Consenso espresso

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

Silenzio

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

Mezzi elettronici

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

Consenso - GDPR (considerando 42)

Accountability	Comprensibile	Evidente squilibrio
Il titolare del trattamento dovrebbe essere in grado di **dimostrare** che l'interessato ha acconsentito al trattamento	dichiarazione di consenso predisposta dal titolare del trattamento in una **forma comprensibile** e facilmente accessibile, che usi un linguaggio semplice e chiaro e non contenga clausole abusive	**evidente squilibrio** tra l'interessato e il titolare del trattamento, specie quando il titolare del trattamento è un'autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato espresso liberamente

Il personale designato/autorizzato:

è tenuto a seguire i corsi di formazione in materia di disciplina della protezione dei dati con le seguenti modalità:

- effettuare il trattamento in modo lecito e secondo correttezza;
- raccogliere e registrare i dati per gli scopi inerenti l'attività svolta;
- verificare, ove possibile, l'esattezza dei dati e, se necessario, aggiornarli;
- verificare che i dati siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal titolare/autorizzato, rispettando, nella conservazione, le misure di sicurezza predisposte nell'istituzione scolastica; in ogni operazione di trattamento deve essere garantita la massima riservatezza, anche tra colleghi appartenenti a consigli di classe diversi;

Il personale autorizzato:

è tenuto a seguire i corsi di formazione in materia di disciplina della protezione dei dati con le seguenti modalità:

- **non far uscire documenti dalla sede scolastica, neanche temporaneamente;**
- **non fare copie della documentazione salvo autorizzazione del responsabile o del titolare;**
- **durante il trattamento mantenere i documenti contenenti dati personali fuori dalla portata di vista di terzi anche se dipendenti dell'istituzione;**
- **al termine del trattamento custodire i documenti all'interno di archivi muniti di serratura o nei locali ad accesso vigilato;**

- **in caso di allontanamento anche temporaneo dal posto di lavoro, o comunque dal luogo dove vengono trattati i dati l'autorizzato dovrà verificare che non vi sia possibilità da parte di terzi, anche se dipendenti non autorizzati, di accedere a dati personali per i quali era in corso un qualunque tipo di trattamento.**

- **nessun dato può essere comunicato a terzi o diffuso in qualsiasi forma, anche ad altri dipendenti non autorizzati, senza la preventiva specifica autorizzazione del titolare o del referente;**

- le comunicazioni agli interessati contenenti dati personali dovranno avvenire in forma riservata; se effettuate per scritto dovranno essere consegnate direttamente all'interessato o in modo che non risultino accessibili i dati in essi contenuti (foglio piegato e spillato o in busta chiusa), tranne quando si tratti di dati pubblici come, ad esempio, voti e giudizi riportati dagli alunni nelle prove di profitto di qualsiasi tipo, le valutazioni intermedie e conclusive, ecc.;

- all'atto della consegna di documenti l'autorizzato dovrà assicurarsi dell'identità dell'interessato o di chi è stato delegato al ritiro del documento in forma scritta.

Tutto il personale autorizzato è contrattualmente soggetto, anche al di fuori dell'orario di lavoro e anche dopo la cessazione del rapporto stesso, ad osservare il segreto professionale e a non divulgare quindi dati, fatti o informazioni di qualsiasi tipo di cui è venuto a conoscenza nello svolgimento dell'incarico conferito.

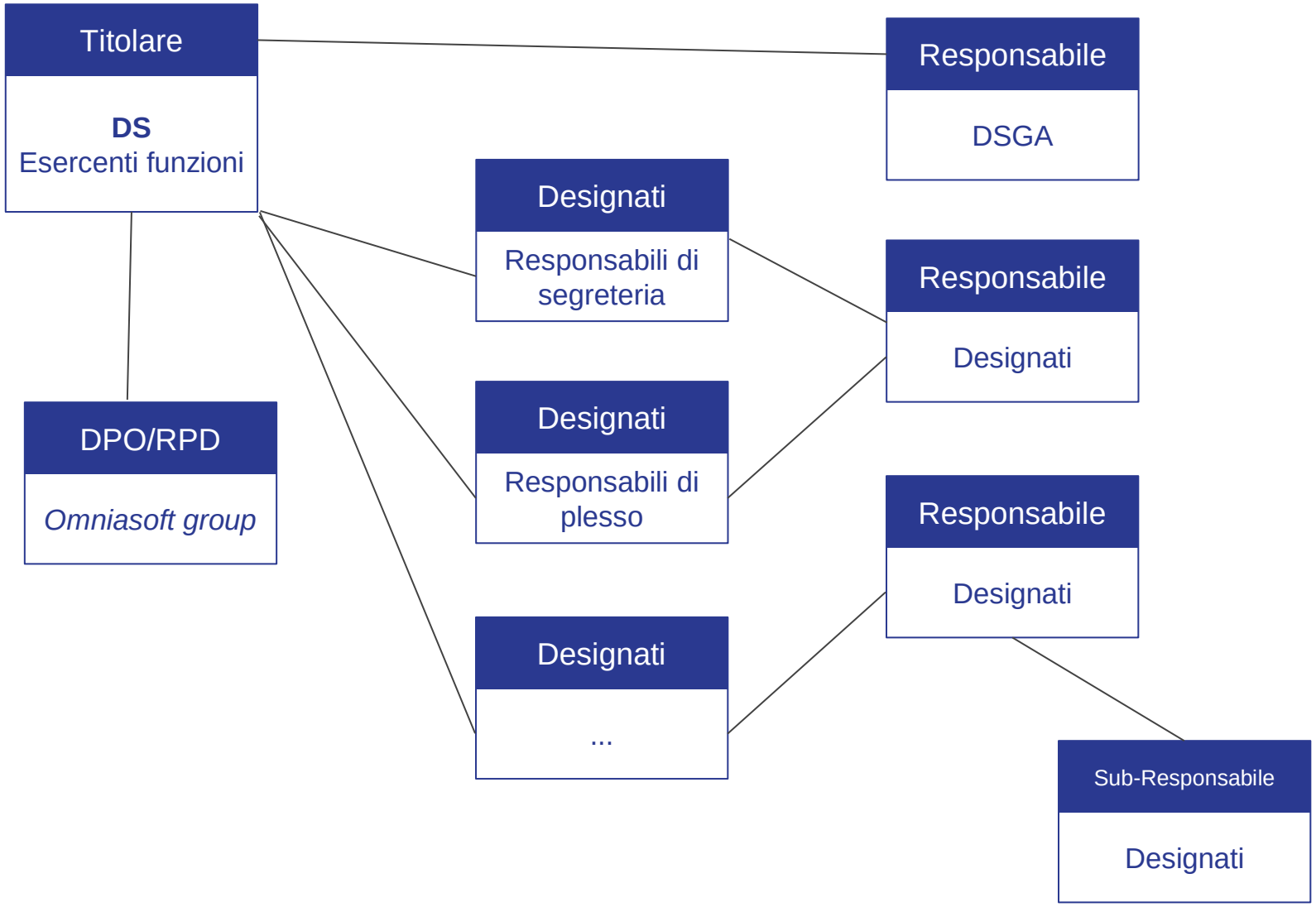
DESIGNATI

Art. 10

DPCM 25 maggio 2018

- 1. I dirigenti della Presidenza del Consiglio dei ministri che trattano dati personali in relazione alle competenze attribuite o comunque esercitate ..sono autorizzati al trattamento nel rispetto delle misure e delle istruzioni adottate da chi esercita le funzioni di titolare del trattamento dei dati personali.
  2. E' autorizzato al trattamento dei dati personali tutto il personale in servizio presso la PCM che tratta dati personali in relazione alle competenze della unita' organizzativa alla quale e' stato assegnato, salvo eventuali diverse determinazioni adottate dai soggetti di cui all'art. 3 (esercenti funzioni di titolare).

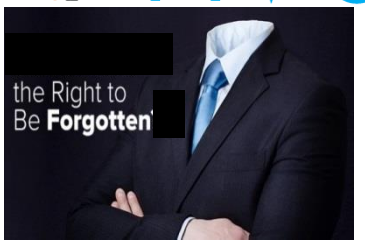
Titolare - Responsabile – Designati/Autorizzati



Accesso e riservatezza

Art. 59	Art. 59	Art. 60
Accesso ai **DOCUMENTI** rimane disciplinato dalla legge 7 agosto 1990, n. 241 e **regolamenti** di attuazione	I presupposti, le modalità e i limiti per l’esercizio del diritto di **accesso civico** restano disciplinati dal decreto legislativo 14 marzo 2013, n. 33.	salute - vita sessuale - orientamento sessuale trattamento consentito **se** la situazione giuridicamente rilevante e' di rango almeno pari ai diritti dell'interessato, **ovvero** diritto della personalita' o libertà fondamentale

Diritti dell’interessato

 rectification right	 to be forgotten right
 portability right	 to object right

RETTIFICA – Art. 16

Diritto di ottenere senza ritardo la rettifica dei dati inesatti

Diritto di ottenere l'integrazione dei dati incomplete, anche fornendo una dichiarazione integrativa

Diritto di ottenere comunicazione delle rettifiche e integrazioni sui dati

Cancellazione («Oblio») – Art. 17

Diritto di ottenere senza ritardo la cancellazione dei dati

Non si appica seil trattamento è necessario:

(a) per l'esercizio del diritto alla libertà di espressione e informazione

(b) per l'adempimento di un obbligo legale o per l'esecuziine di un compito svolto nel pubblico interesse o nell'esercizio di pubblici poteri

(c) per motivi di interesse pubblico nella sanità pubblica

(d) per finalità di archiviazione nel pubblico interesse, ricercar scientifica o storica o statistica

(e) per l'eserciz

«*Il Diritto all'oblio è uno slogan meglio parlare di diritto all'opacizzazione*»
Caselli, Funzionario Garante Privacy
Milano 17.01.207

Portabilità – Art. 20

Diritto di ricevere in formato strutturato, di uso commune e leggibile da dispositivo automatico, i dati personali forniti e diritto di vedere trasmessi tali dati a un altro soggetto senza impedimenti, ove

(a) il trattamento sia basato sul consenso

(b) il trattamento sia effettuato con mezzi automatizzati

Trasmissione diretta dei dati se tecnicamente fattibile

Opposizione – Art. 21

Diritto di opporsi al trattamento dei dati e di ottenere la cessazione del trattamento, salvo che esistano motivi legittimi cogenti per continuare il tarttamento

Il diritto di opporsi deve essere evidenziato nell'informativa separatamente dalle altre informazioni e in modo chiaro

Ove il trattamento avvenga per finalità di ricerca scientifica, storica o statistica il diritto di opposizione potrà cedere se il trattamento è necessario per realizzare le specifiche finalità e l'interesse pubblico

Sanzioni

SANZIONI AMMINISTRATIVE

RIFERIMENTO	VIOLAZIONE
Registro trattamenti	Assenza o mantenimento non corretto
Privacy by design/by default	Assenza di conformità privacy by design/default di prodotti e servizi
Contitolarità	Assenza di accordo e ripartizione responsabilità tra contitolari
Rappresentanti non stabiliti in UE	Assenza di designazione di un rappresentante in UE
Responsabile trattamento	Assenza autorizzazione scritta da parte del Titolare

Fino a 10 Mln Euro o 2% del fatturato MONDIALE totale annuo dell'esercizi o precedente, se superiore

SANZIONI AMMINISTRATIVE (art. 78)

RIFERIMENTO	VIOLAZIONE
Sicurezza	Assenza di adozione di misure tecniche e organizzative adeguate
Notifica di violazione	Mancata notifica all'Autorità
Comunicazione di violazione	Mancata comunicazione agli interessati
Valutazione di impatto	Assenza di valutazione di impatto
Designazione DPO	Assenza di designazione
Posizione DPO	Assenza di tempestivo e adeguato coinvolgimento; ingerenza su attività DPO; assenza di risorse

Fino a 10 Mln Euro o 2% del fatturato MONDIALE totale annuo dell'esercizio precedente, se superiore

SANZIONI AMM.VE
(art. 78)

RIFERIMENTO	VIOLAZIONE
Principi del trattamento	Violazione principi di liceità, correttezza, trasparenza, non eccedenza, integrità, riservatezza
Consenso	Assenza di consenso o finalità
Categorie particolari di dati	Assenza di consenso per dati sensibili
Diritto di accesso/oblio /rettifica/portabilità /opposizione	Violazioni
Trasferimenti in paese terzo	Inosservanza dei principi, assenza

Fino a 20 Milioni Euro o 4% del fatturato MONDIALE totale annuo dell'esercizio precedente se superiore

SANZIONI AMMINISTRATIVE

Art. 79 n. 3 ter del RGPD

Ogni Stato Membro può prevedere norme che dispongano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad AUTORITA' PUBBLICHE ed ORGANISMI PUBBLICI nello Stato membro.

SANZIONI PENALI

Art. 79 ter del RGPD

Gli **Stati membri stabiliscono le norme relative alle altre sanzioni** per le violazioni del presente regolamento in particolare per le violazioni non soggette sanzioni amministrative pecuniarie

- ❑ Effettive
- ❑ Proporzionate
- ❑ Dissuasive

ILLECITI PENALI

D. Lgs. 30 Giugno 2003 n. 196

- Trattamento illecito di dati

Reclusione 6-24 mesi

- Falsità nelle dichiarazioni e notificazioni al Garante

Reclusione 6 mesi-3 anni

- Omissione di misure di sicurezza

Arresto sino a 2 anni

- Inosservanza dei provvedimenti del Garante

Reclusione da 3 mesi a 2 anni

Legge 20 Maggio 1970 n. 300

- Divieto di utilizzo di apparecchi audiovisivi per controllo a distanza di lavoratori

Arresto-Ammenda

RESPONSABILITA' CIVILE

RISARCIMENTO DEL DANNO

Responsabilità solidale

- Titolare/Responsabile

Responsabilità concorrente

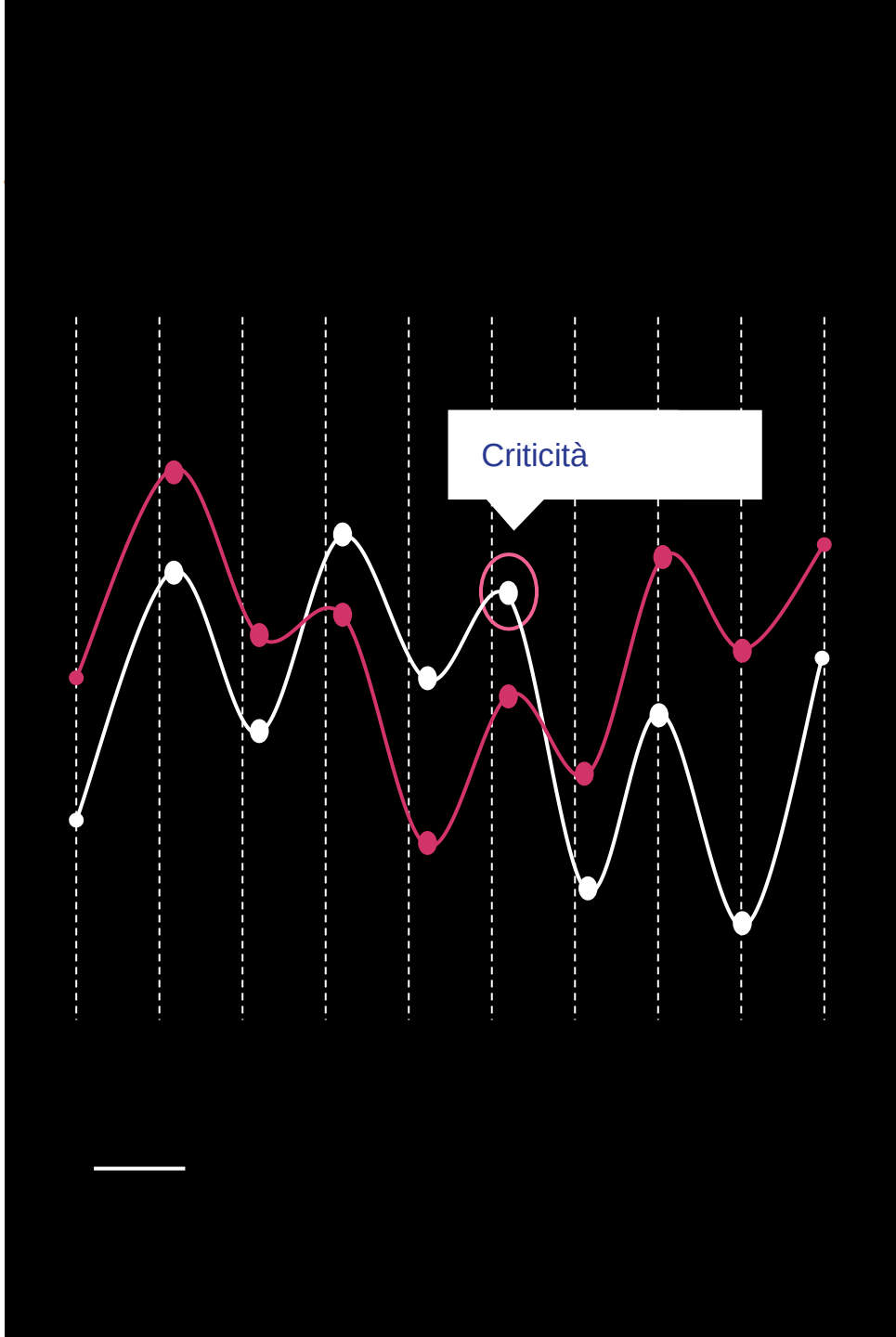
- Con-Titolari

Ulteriori appunti e spunti di riflessione


Descrizione del trattamento previsto
Valutazione della necessità e della proporzionalità
Misure previste per dimostrare la conformità
Valutazione dei rischi per i diritti e le libertà
Misure previste per affrontare i rischi
Documentazione
Monitoraggio e riesame

Valutazione d’impatto

Analisi dei rischi



Grazie !

Avv. Rita Di Carlo

CEO e Founder Studio Legale Di Carlo

Specializzata in Privacy e data protection

Formatrice certificata

rita.dicarlo@omniasoft.it