CERTIFICAZIONE E AUDIT GDPR.
ISDP©10003, LA PROPOSTA ITALIANA

Riccardo Giannetti,
Chairman Inveo group

PRIVACYDAY

LA CERTIFICAZIONE

GDPR: quanto legge e quanto norma tecnica?

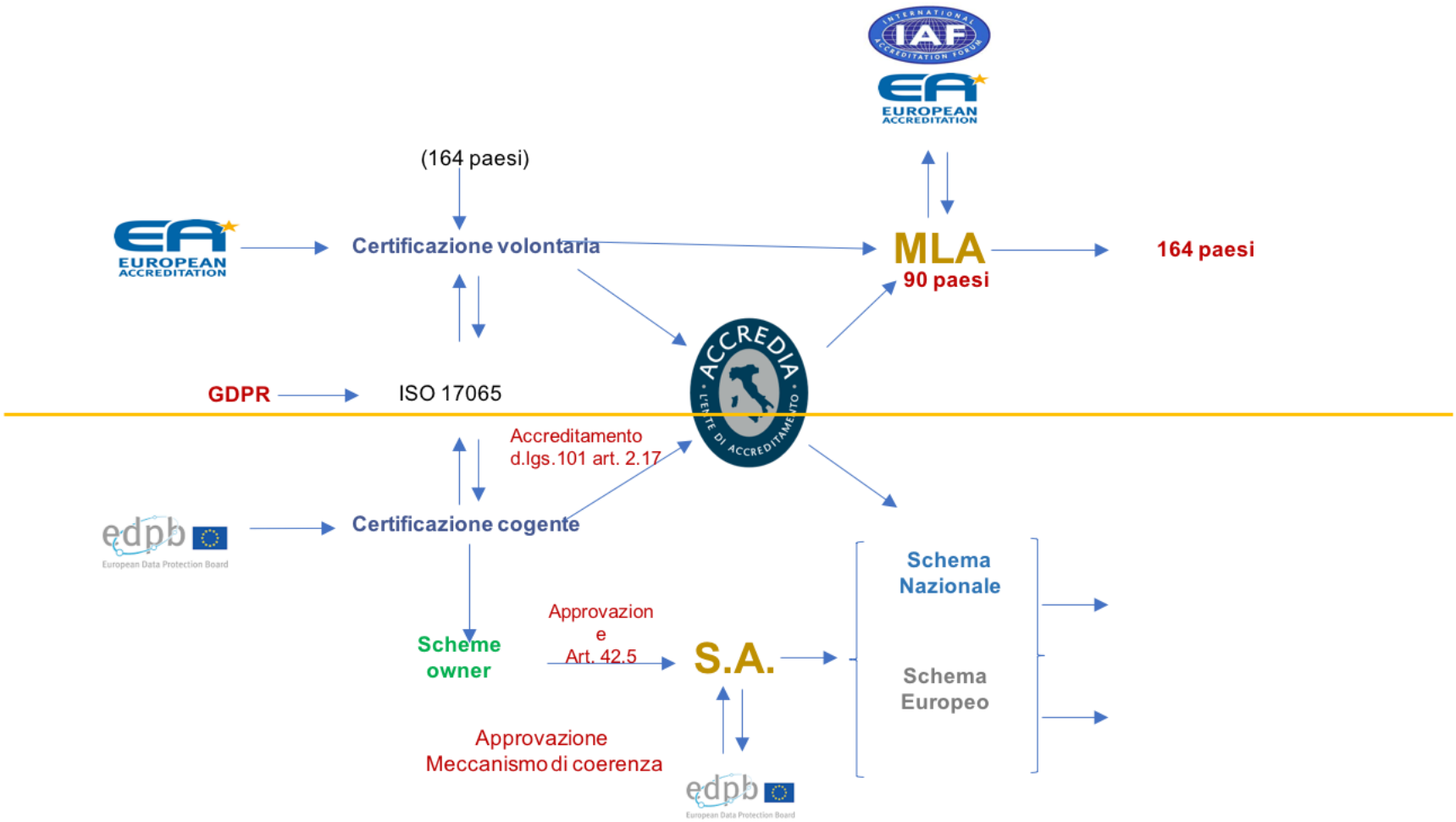
Recital 100

Al fine di migliorare la trasparenza e il rispetto del presente Regolamento dovrebbe incoraggiare l'istituzione di meccanismi di certificazione e sigilli nonché marchi di protezione dei dati che consentano agli interessati di **valutare rapidamente il livello di protezione dei dati dei…**

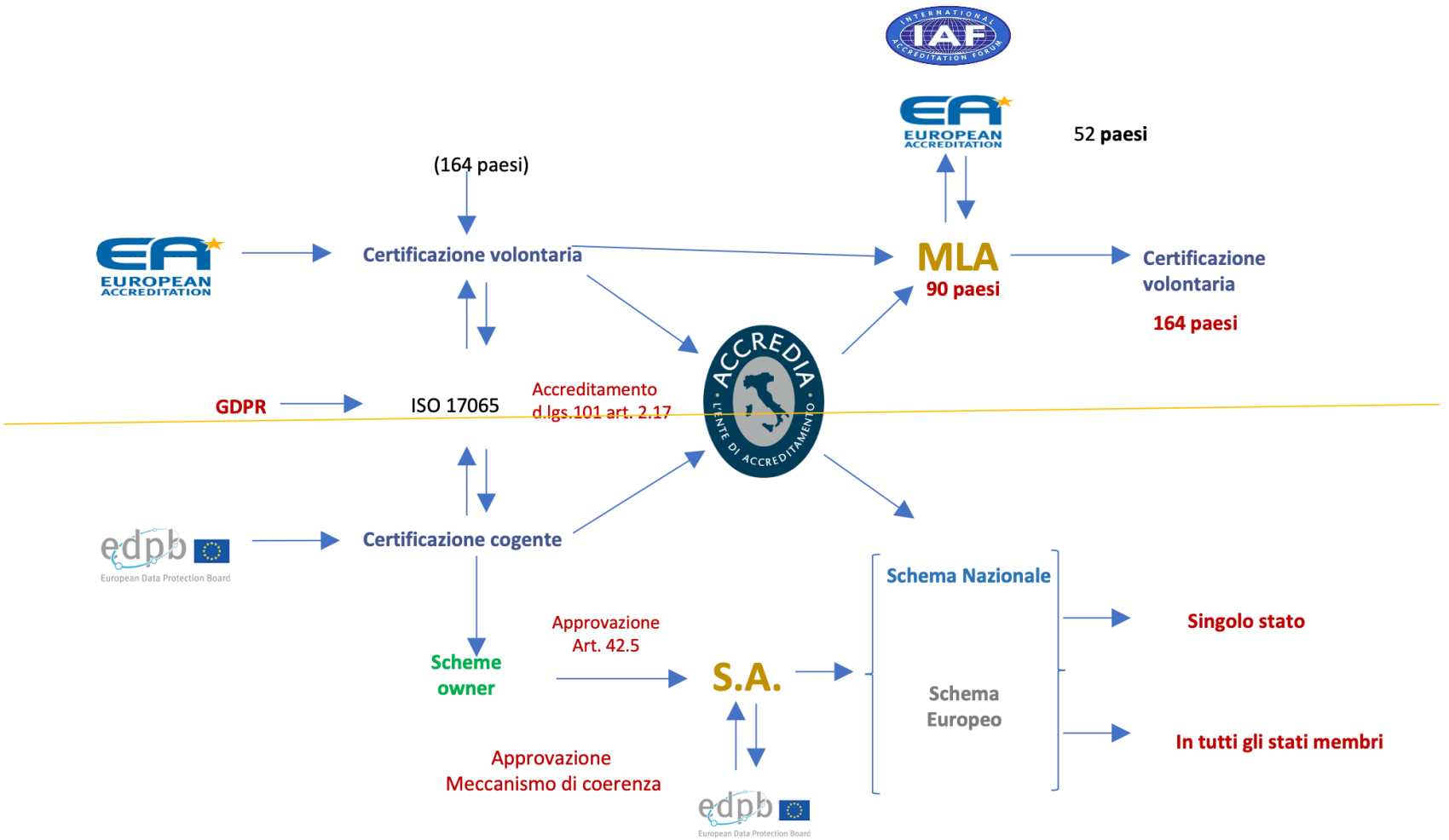
…relativi **prodotti e servizi**

ISO/IEC 17065

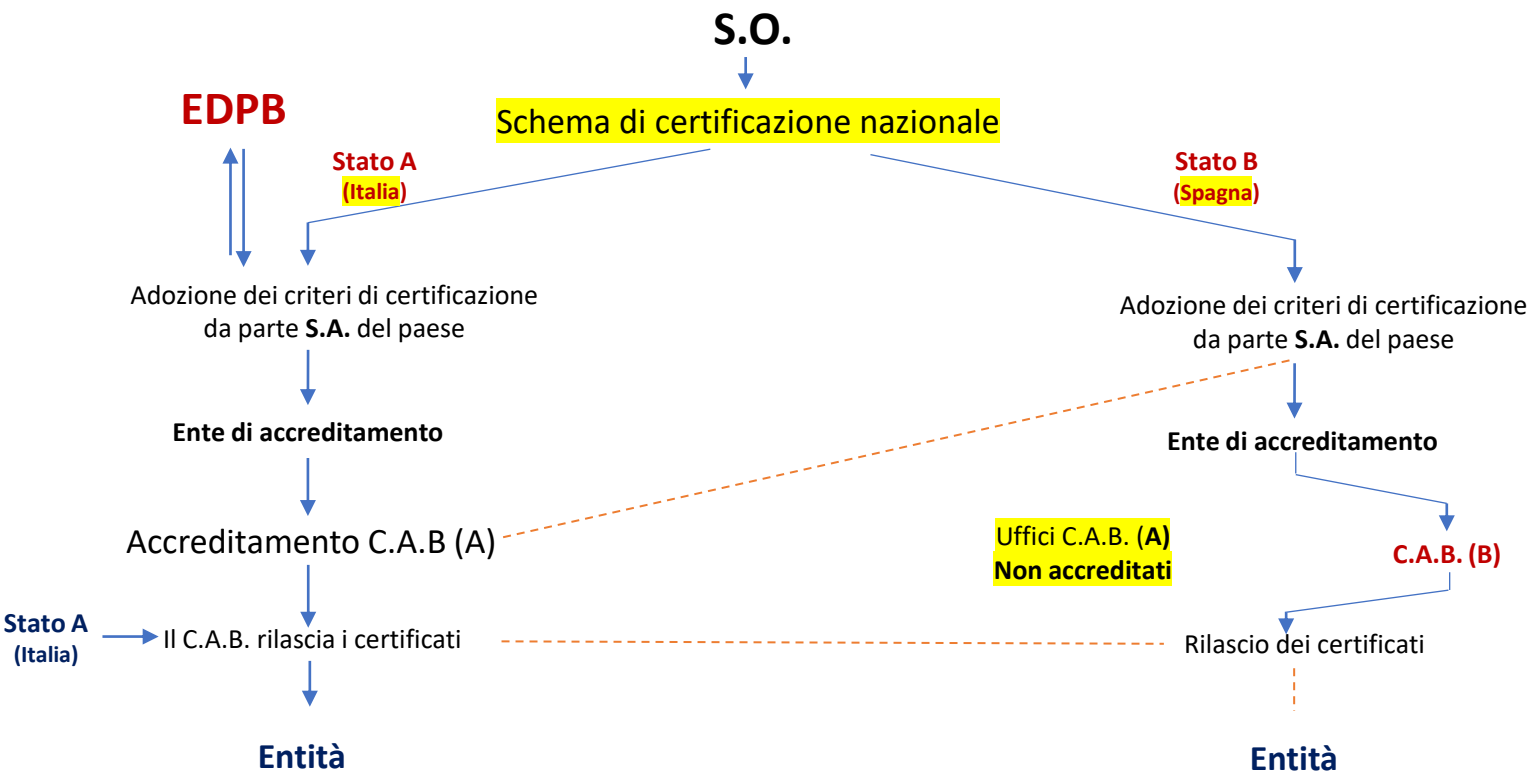
LA CERTIFICAZIONE



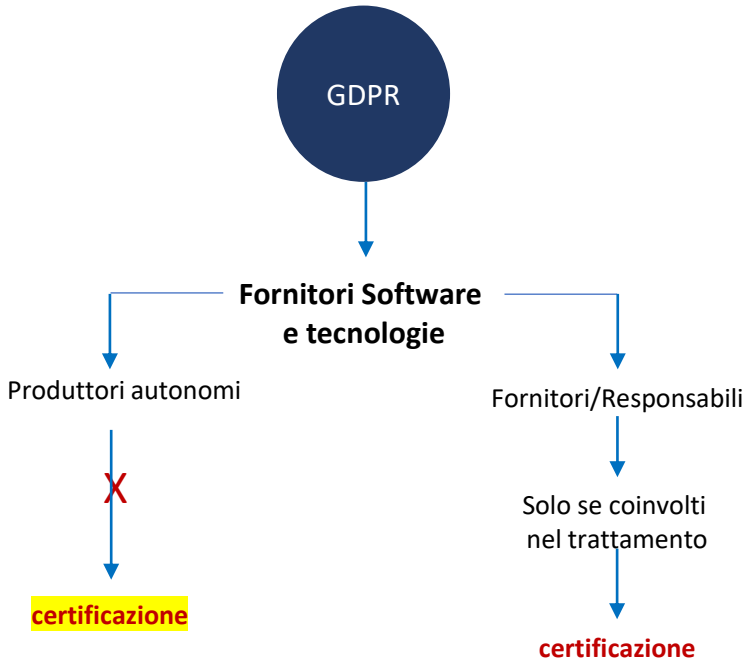
LA CERTIFICAZIONE



LA CERTIFICAZIONE



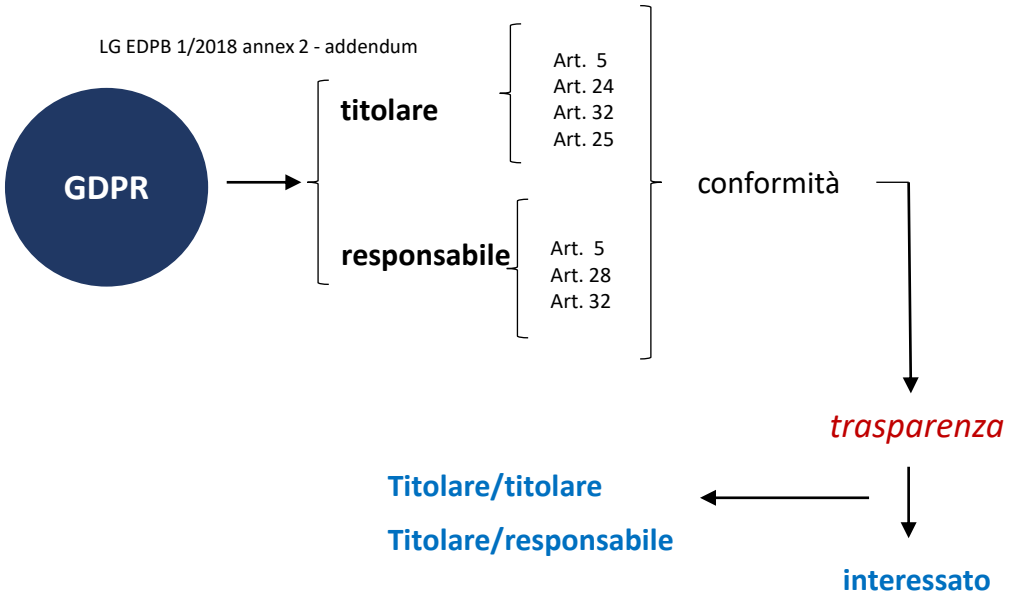
LA CERTIFICAZIONE



Ambito della certificazione: cosa può essere certificato…

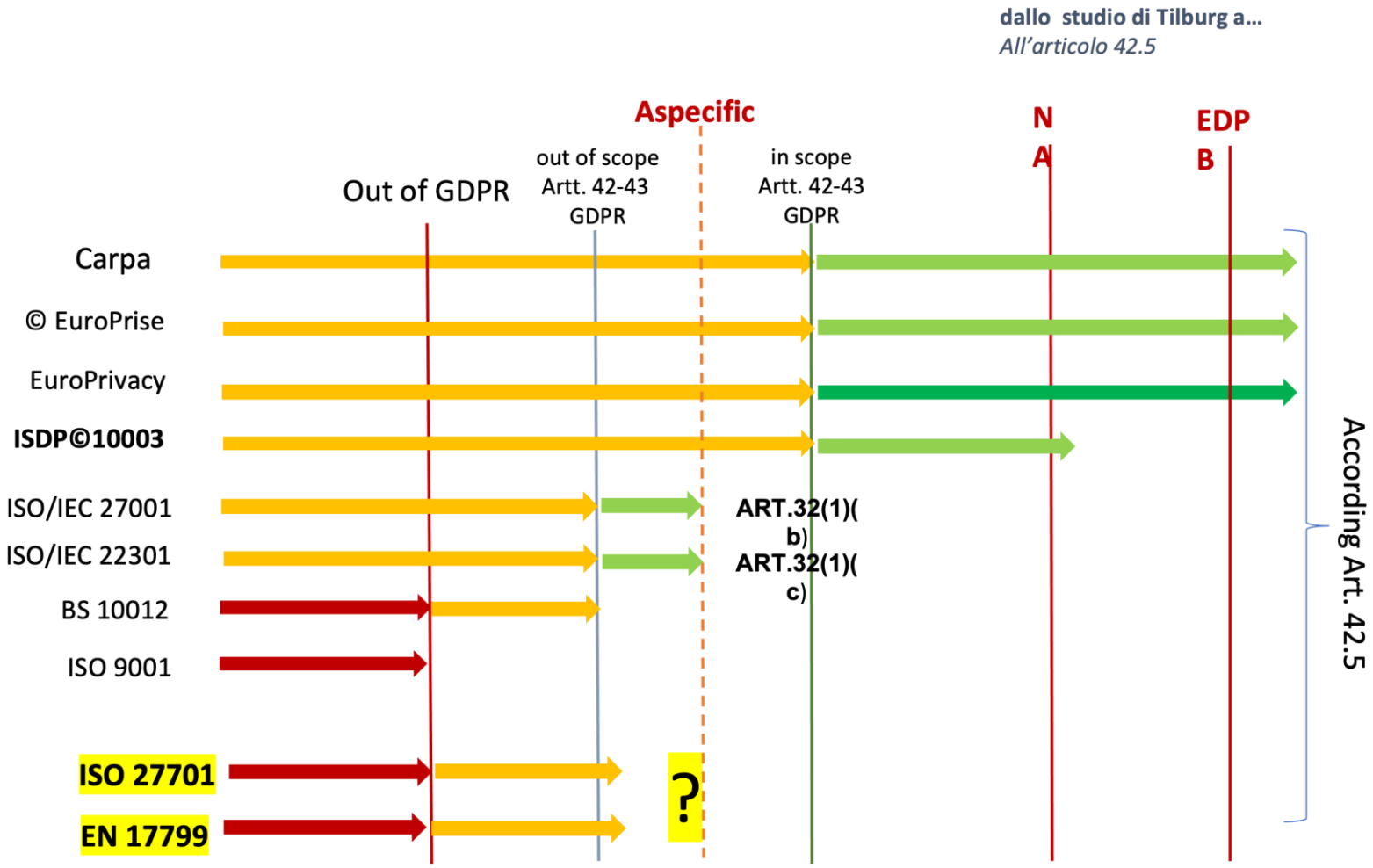
T.O.E: cosa è certificato…

COSA E' CERTIFICABILE?



LE NORME TECNICHE

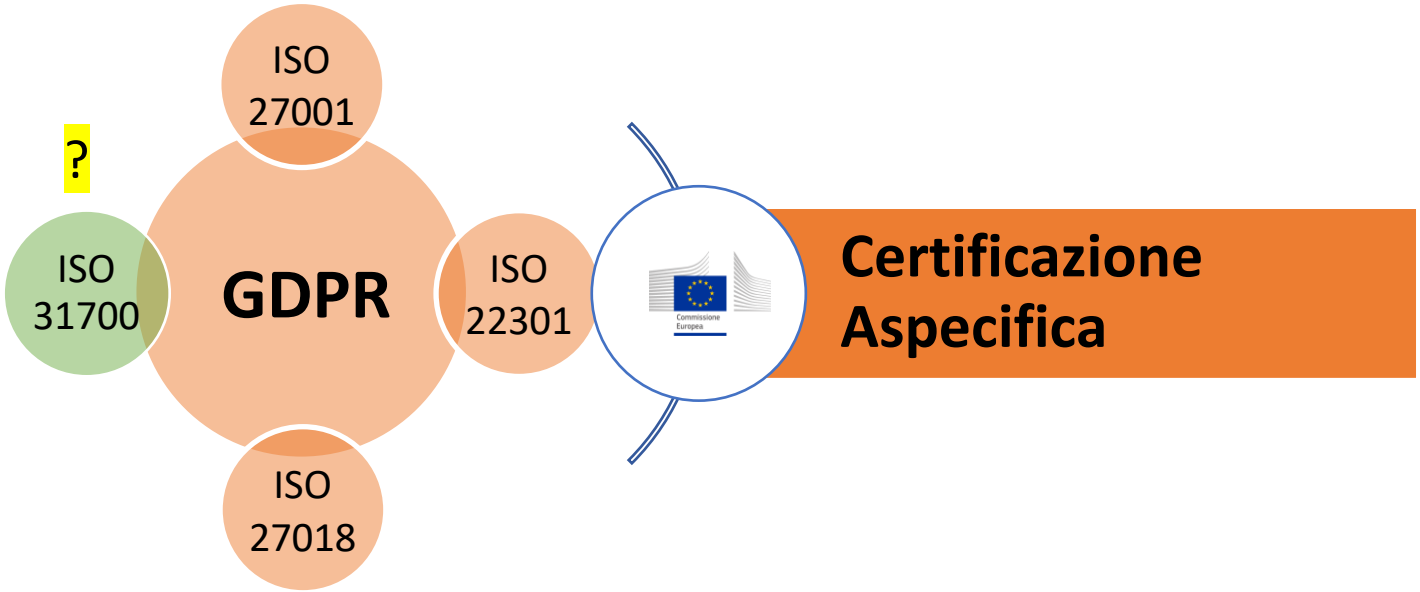
LE NORME TECNICHE



LE NORME TECNICHE

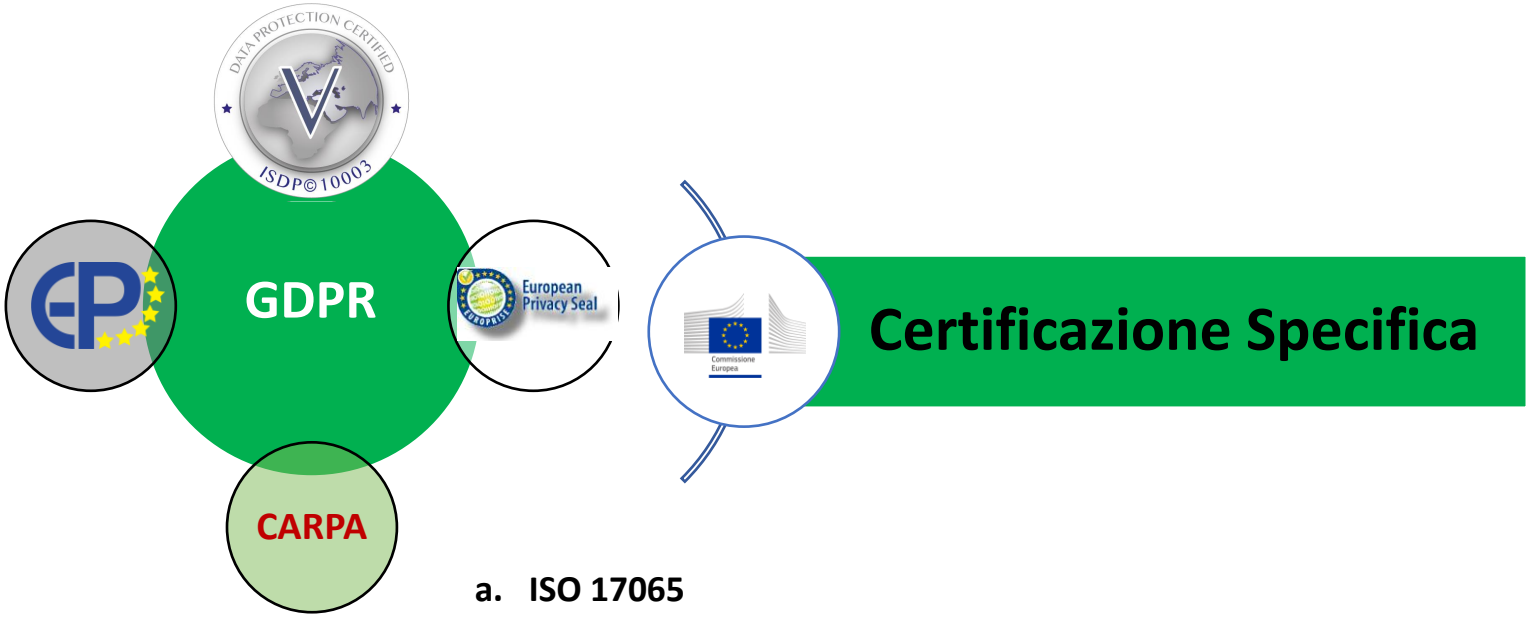
- **No ISO 17065**
- Norme o linee guida che non prevedono la tutela dei diritti e delle libertà degli interessati, bensì delle informazioni

LE NORME TECNICHE



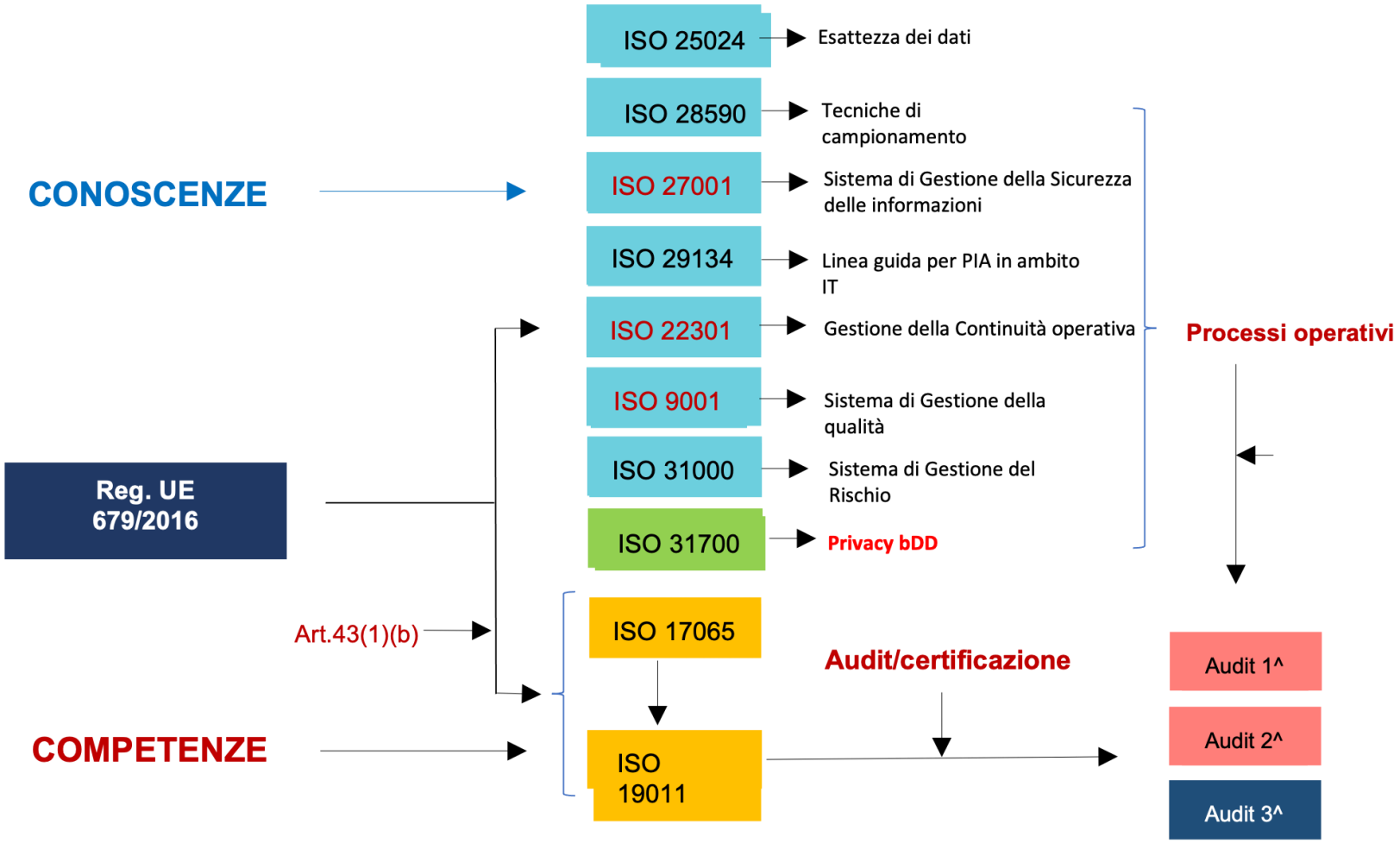
- ISO 17021-1
- Richiamate dall'art. 32(b) e (c) per rispondere esclusivamente a requisiti specifici del GDPR
- E' focalizzata su esigenze di business della sicurezza delle informazioni
- Assicura la **capacità dell'azienda** di gestire le risorse e i processi interni in modo da soddisfare i bisogni dei clienti
- Utilizzabili esclusivamente come best practice

LE NORME TECNICHE

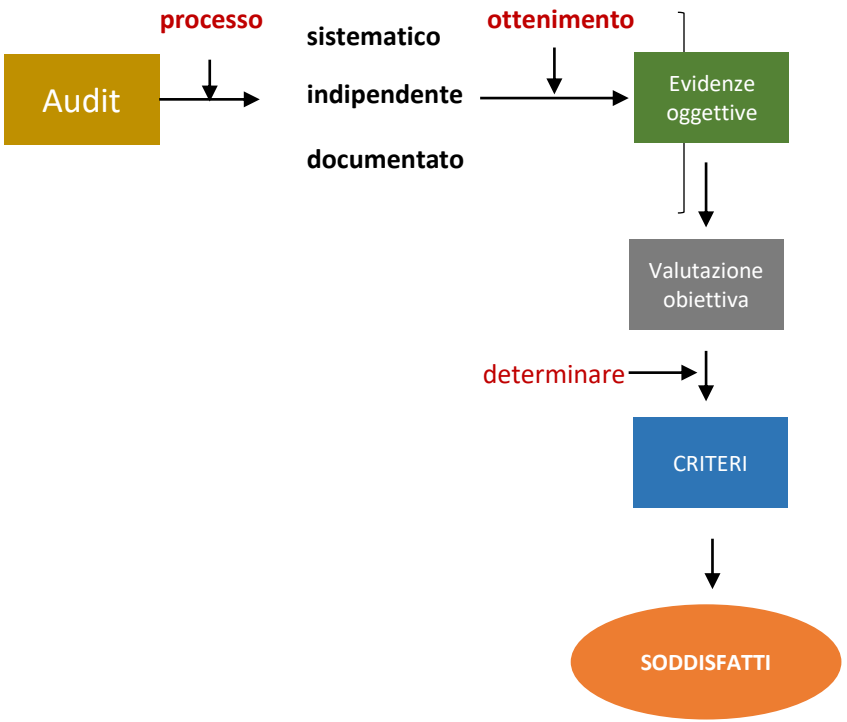


a. **ISO 17065**
b. Tutela dei diritti e delle libertà degli interessati *(art. 8 «carta diritti fondamentali» e art. 16 TFUE)*
c. E' una forma di «*assicurazione diretta*» di conformità, con cui si accerta la rispondenza diretta di un prodotto o servizio ai requisiti applicabili
d. Trasposizione delle disposizioni (articoli, considerando e linee guida) del GDPR
e. Schemi non precostituiti

LA CERTIFICAZIONE

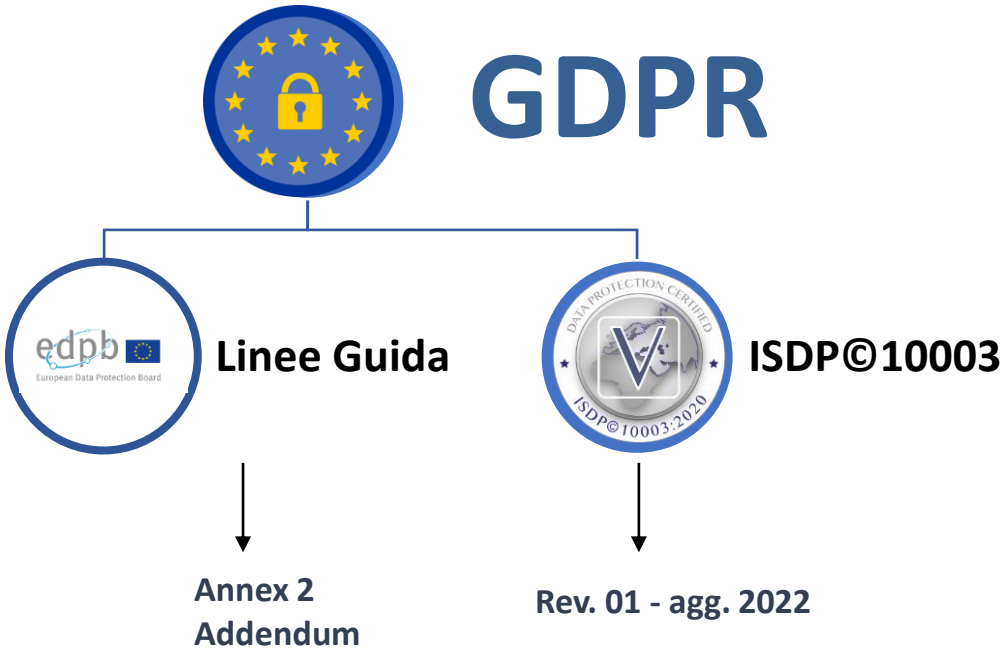


COS'E' UN AUDIT GDPR



UNI EN ISO 19011:2018		UNI EN ISO 17021-1
Audit I^ parte	Audit II^ parte	Audit III^ parte
Audit interno	Audit di fornitori esterni	Audit di certificazione e/o di accreditamento
	Audit di altre parti interessate esterne	Audit per fini legislativi, regolamentari e similari

LA PROPOSTA ITALIANA: ISDP©10003



ISDP©10003:2020 | Data Protection

Schema internazionale per la valutazione della conformità al regolamento europeo per la protezione dei dati personali ISDP©10003 - Criteri e regole di controllo per la Certificazione dei processi per la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione degli stessi

LA PROPOSTA ITALIANA: ISDP©10003

ASPETTI DI CONFORMITA'	Rif.	SEZIONI	Rif.	SOTTOSEZIONI
Principio di responsabilizzazione ai sensi degli articoli 5 e 24	A.1	Responsabilizzazione e consapevolezza	A.1.1	Responsabilizzazione del titolare
			A.1.2	Responsabilizzazione del responsabile
	A.2	Soggetti coinvolti nel processo del trattamento	A.2.1	Titolare del trattamento
			A.2.2	Contitolari
			A.2.3	Responsabile del trattamento
			A.2.4	Responsabile della protezione dei dati
Principi applicabili al trattamento di dati personali ai sensi dell'articolo 5	A.3	Principi applicabili, fondamento di legittimità del trattamento dei dati e meccanismi di tutela degli interessati	A.3.1	Principi applicabili al trattamento dei dati personali
Presupposti di liceità del trattamento ai sensi dell'articolo 6			A.3.2	Basi giuridiche del trattamento
			A.3.3	Consenso come base giuridica del trattamento e condizioni per il consenso
Diritti degli interessati, a norma degli articoli da 12 a 23			A.3.4	Informativa
			A.3.5	Diritti dell'interessato
			A.3.6	Diritto di opposizione e processo automatizzato
Obbligo della protezione dei dati fin dalla progettazione e dalla protezione dei dati per impostazione predefinita a norma art. 25	A.4	Processi di adeguamento in fase di ideazione ed all'atto del trattamento a norma art. 25	A.4.1	Protezione dei dati fin dalla progettazione e per impostazione predefinita
Misure tecniche e organizzative messe in atto a norma dell'art. 32	A.5	Obblighi generali, gestione del rischio e sicurezza dei trattamenti (§ A.5.4) (*nota 1 e nota 2*)	A.5.1	Mappatura e Registri del trattamento
			A.5.2	Sicurezza del trattamento
			A.5.3	Misure organizzative per la protezione dei dati
			A.5.4	Misure tecniche per la protezione dei dati
Valutazione d'Impatto a norma art. 35	A.6	Gestione e impostazione della Valutazione d'impatto	A.6.1	Necessità e metodologie per lo svolgimento della valutazione d'Impatto
Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali ai sensi degli articoli da 44 a 50	A.7	Trasferimento dei dati personali verso paesi terzi,	A.7.1	Corretta modalità di trasferimento dei dati fuori dall'UE verso paesi terzi
Obbligo di notifica delle violazioni dei dati ai sensi dell'art. 33	A.8	Violazione dei dati personali Obblighi generali, gestione del rischio e sicurezza dei trattamenti	A.8.1	Violazione dei dati personali

LA PROPOSTA ITALIANA: ISDP©10003

ISDP©10003 (2020 vs 2023)					
PROCESSI	Annex A	n. Processi	Controlli Vers. 2020	n. Sezioni	Controlli Vers. 2023
Politica e obbligazioni del titolare	A.1	1	**6** (5)	3	18
Soggetti coinvolti nel processo del trattamento	A.2	4	**21** (18)	4	20
Principi applicabili al trattamento e tutela dei diritti	A.3	5	**34** (25)	6	38
Processi di adeguamento in fase di ideazione ed all'atto del trattamento	A.4	1	**10** (6)	2	10
Obblighi generali, **gestione del rischio** e sicurezza dei dati personali	A.5	4	**31** (25)	3	8
Valutazione d'impatto	A.6	1	**7** (6)	1	2
Trasferimento dei dati personali verso paesi terzi e Gestione del Cloud e IoT	A.7	2	**13**	1	4
Violazione dei dati personali	A.8	-	-	1	4
		TOTALE	**122**		**104**

LA PROPOSTA ITALIANA: ISDP©10003

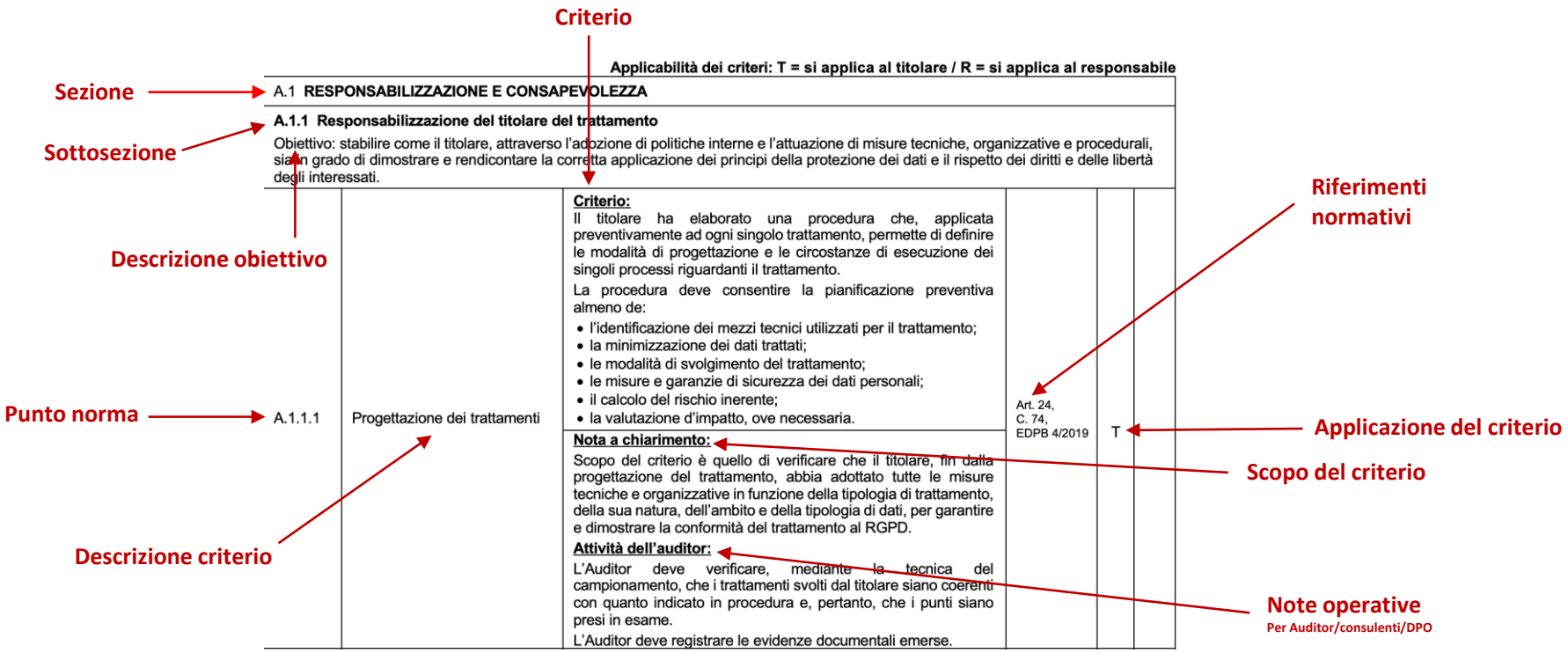
Macro processo

Processo

controllo

A.1 - POLITICA E OBBLIGAZIONI DEL TITOLARE		
A.1.1 - Obblighi generali e consapevolezza del Titolare *Obiettivo: Stabilire la corretta percezione e declinazione formale, del concetto di responsabi are del trattamento.*		
A.1.1.1	Consapevolezza del titolare del trattamento	*Obiettivi e metodo di controllo* Verificare la reale consapevolezza del titolare del trattamento e come la stessa venga gestita all'interno dell'organizzazione. Devono essere verificate tutte le azioni di sensibilizzazione interna.

LA PROPOSTA ITALIANA: ISDP©10003



Applicabilità dei criteri: T = si applica al titolare / R = si applica al responsabile

A.1 **RESPONSABILIZZAZIONE E CONSAPEVOLEZZA**

A.1.1 Responsabilizzazione del titolare del trattamento

Obiettivo: stabilire come il titolare, attraverso l'adozione di politiche interne e l'attuazione di misure tecniche, organizzative e procedurali, sia in grado di dimostrare e rendicontare la corretta applicazione dei principi della protezione dei dati e il rispetto dei diritti e delle libertà degli interessati.

A.1.1.1	Progettazione dei trattamenti	**Criterio:** Il titolare ha elaborato una procedura che, applicata preventivamente ad ogni singolo trattamento, permette di definire le modalità di progettazione e le circostanze di esecuzione dei singoli processi riguardanti il trattamento. La procedura deve consentire la pianificazione preventiva almeno de: • l'identificazione dei mezzi tecnici utilizzati per il trattamento; • la minimizzazione dei dati trattati; • le modalità di svolgimento del trattamento; • le misure e garanzie di sicurezza dei dati personali; • il calcolo del rischio inerente; • la valutazione d'impatto, ove necessaria. **Nota a chiarimento:** Scopo del criterio è quello di verificare che il titolare, fin dalla progettazione del trattamento, abbia adottato tutte le misure tecniche e organizzative in funzione della tipologia di trattamento, della sua natura, dell'ambito e della tipologia di dati, per garantire e dimostrare la conformità del trattamento al RGPD. **Attività dell'auditor:** L'Auditor deve verificare, mediante la tecnica del campionamento, che i trattamenti svolti dal titolare siano coerenti con quanto indicato in procedura e, pertanto, che i punti siano presi in esame. L'Auditor deve registrare le evidenze documentali emerse.	Art. 24, C. 74, EDPB 4/2019	T	

LA PROPOSTA ITALIANA: ISDP©10003

I vantaggi

L'organizzazione certificata ISDP©10003

- Opera secondo norma, valutando la conformità del trattamento al GDPR
- Dimostra Accountability
- Dimostra alle S.A. di avere in forma volontaria, applicato un atto di diligenza *(ex art. 83.2 lett. K)*
- Basa la propria attività su procedure valutate, standardizzate e monitorate
- E' un elemento di trasparenza verso le parti interessate

LA PROPOSTA ITALIANA: ISDP©10003

Vi aspettiamo ai nostri corsi…

Grazie!

Riccardo Giannetti

Chairman INVEO group

r.giannetti@in-veo.com

riccardo-giannetti-8758688

www.in-veo.com

Via Australia 29, 00144 Roma, Italy

+39 0669400048