inveo GROUP

PRIVACYDAY

CERTIFICAZIONE GDPR DOVE SIAMO?

Stato dell’arte per la governance del futuro

Riccardo Giannetti, *Chairman Inveo group*

www.in-veo.com

Certificazione, perché?

Certificazione, perché?

Recital 100

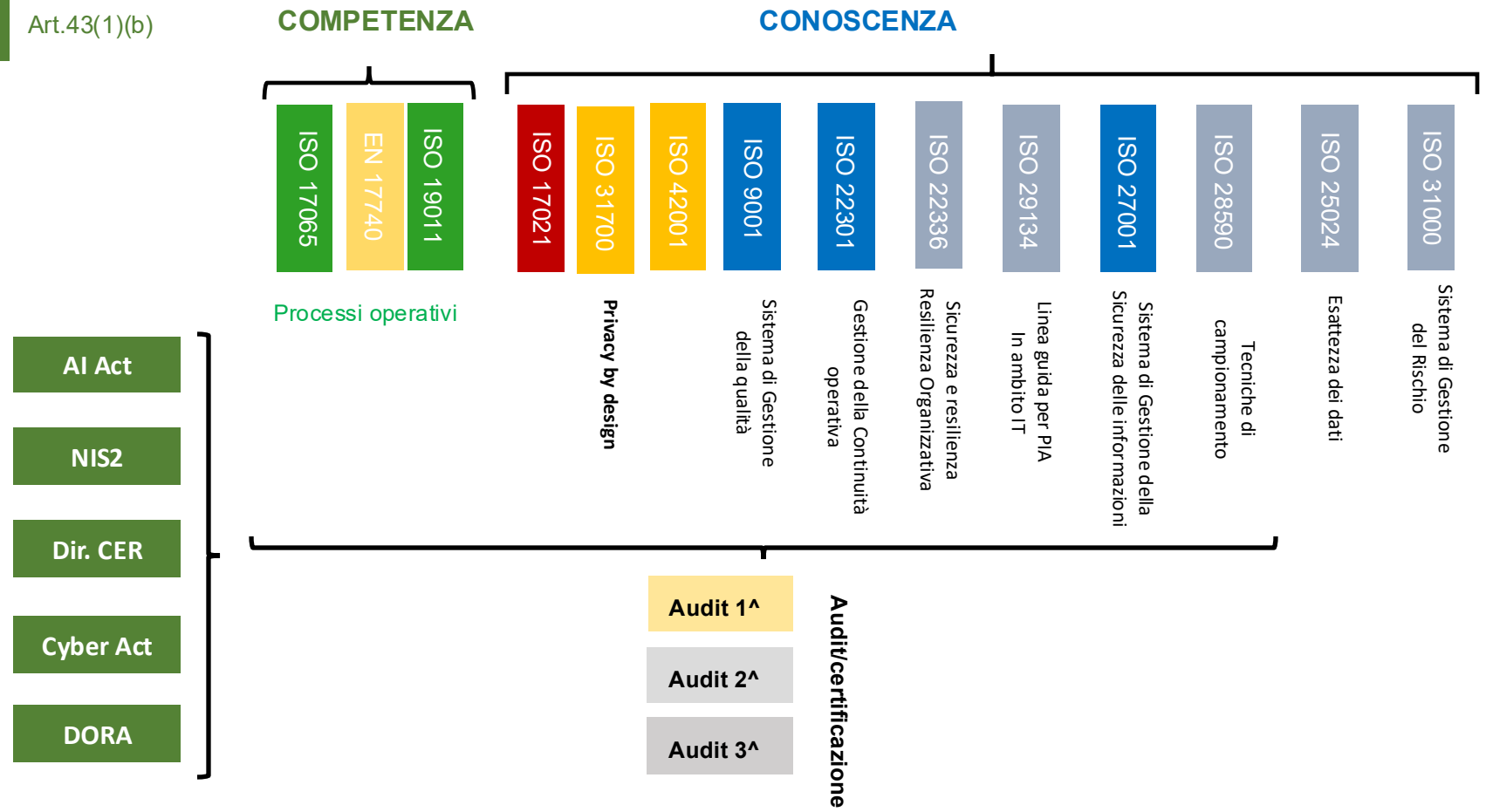
Al fine di migliorare la trasparenza e il rispetto del presente Regolamento dovrebbe incoraggiare l'istituzione di meccanismi di certificazione e sigilli nonché marchi di protezione dei dati che consentano agli interessati di **valutare rapidamente il livello di protezione dei dati dei…**

…relativi **prodotti e servizi**

Le norme..

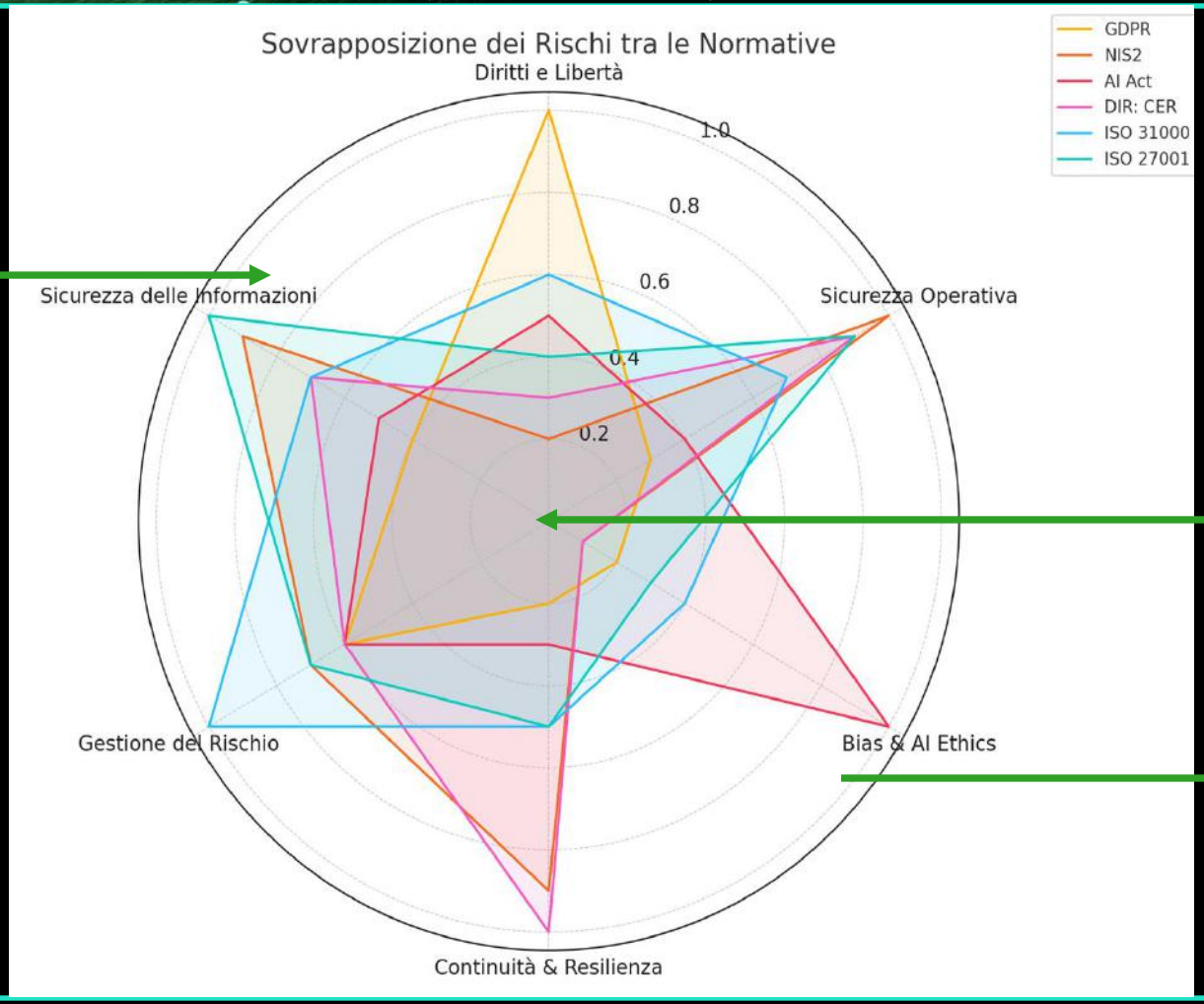
Reg. UE 679/2016

Art.43(1)(b)



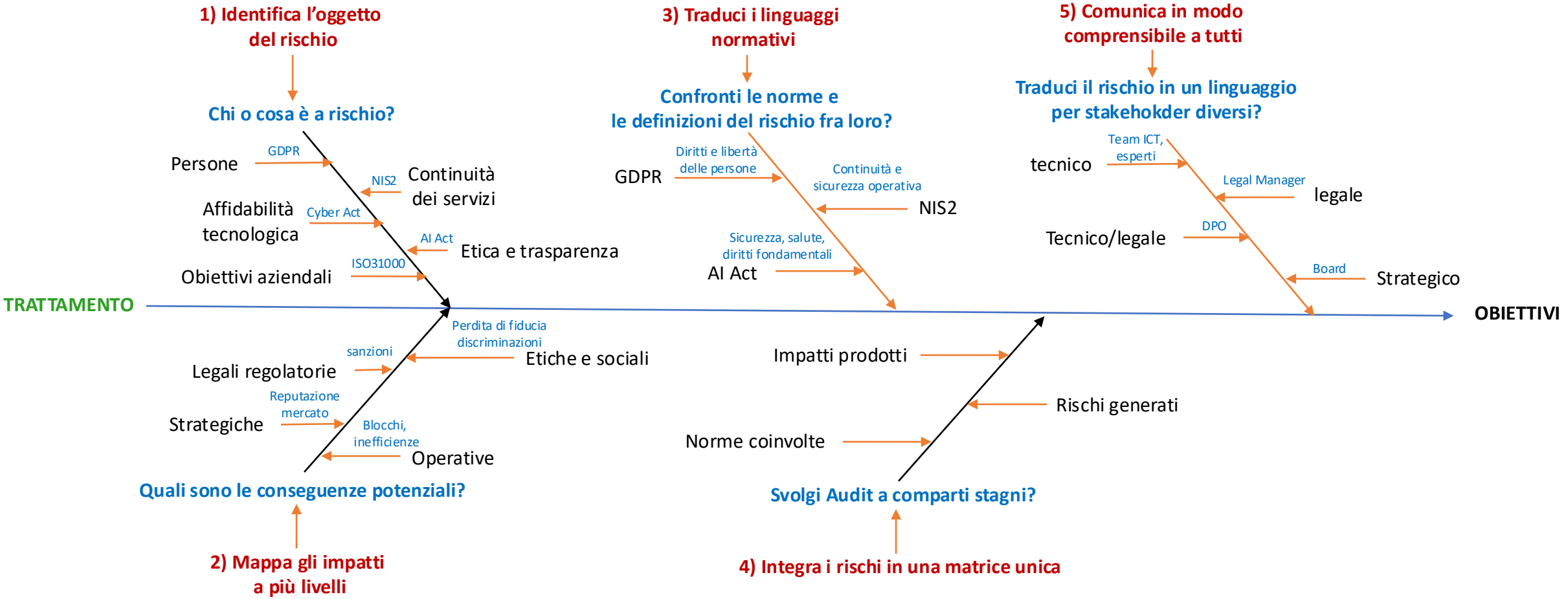
Rischi	GDPR	NIS2	AI ACT	DIR. CER	ISO31000	ISO27001
Diritti e Libertà	1,0	0,2	0,5	0,3	0,6	0,4
Sicurezza operativa	0,3	1,0	0,4	0,9	0,7	0,9
Bias & AI Ethics	0,2	0,1	1,0	0,1	0,4	0,3
Continuità e resilienza	0,2	0,9	0,3	1,0	0,5	0,5
Gestione del rischio	0,6	0,7	0,6	0,6	1,0	0,7
Sicurezza delle informazioni	0,4	0,9	0,5	0,7	0,7	1,0

Rischi

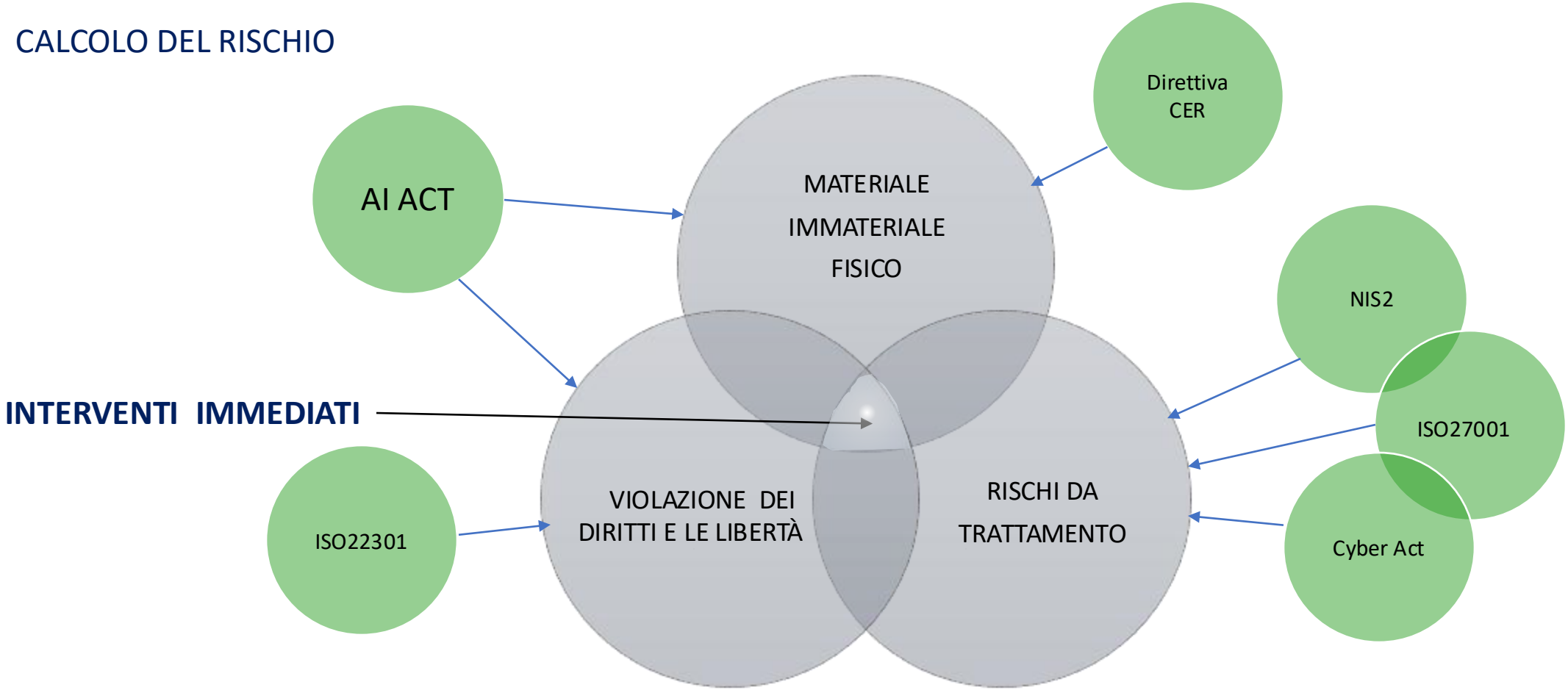


Area di meta-rischio

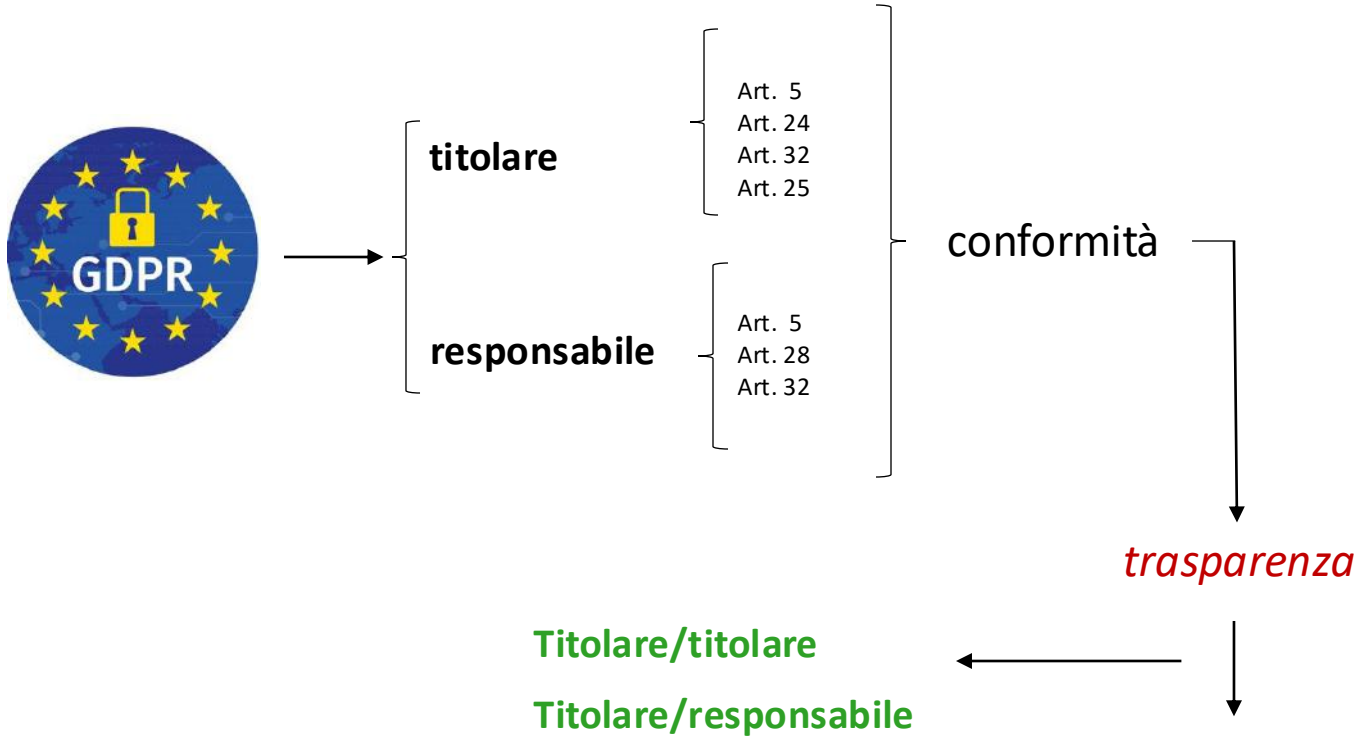
Complementarietà e integrazione


1) Identifica l'oggetto del rischio
Chi o cosa è a rischio?
Persone
GDPR
NIS2
Continuità dei servizi
Affidabilità tecnologica
Cyber Act
AI Act
Etica e trasparenza
Obiettivi aziendali
ISO31000
3) Traduci i linguaggi normativi
Confronti le norme e le definizioni del rischio fra loro?
GDPR
Diritti e libertà delle persone
Continuità e sicurezza operativa
NIS2
Sicurezza, salute, diritti fondamentali
AI Act
5) Comunica in modo comprensibile a tutti
Traduci il rischio in un linguaggio per stakehokder diversi?
tecnico
Team ICT, esperti
Legal Manager
legale
Tecnico/legale
DPO
Board
Strategico
TRATTAMENTO
OBIETTIVI
Perdita di fiducia discriminazioni
Etiche e sociali
sanzioni
Legali regolatorie
Reputazione mercato
Strategiche
Blocchi, inefficienze
Operative
Quali sono le conseguenze potenziali?
2) Mappa gli impatti a più livelli
Impatti prodotti
Rischi generati
Norme coinvolte
Svolgi Audit a comparti stagni?
4) Integra i rischi in una matrice unica

CALCOLO DEL RISCHIO



LG EDPB 1/2018 annex 2 - addendum



Fornitori Software e tecnologie

Produttori autonomi

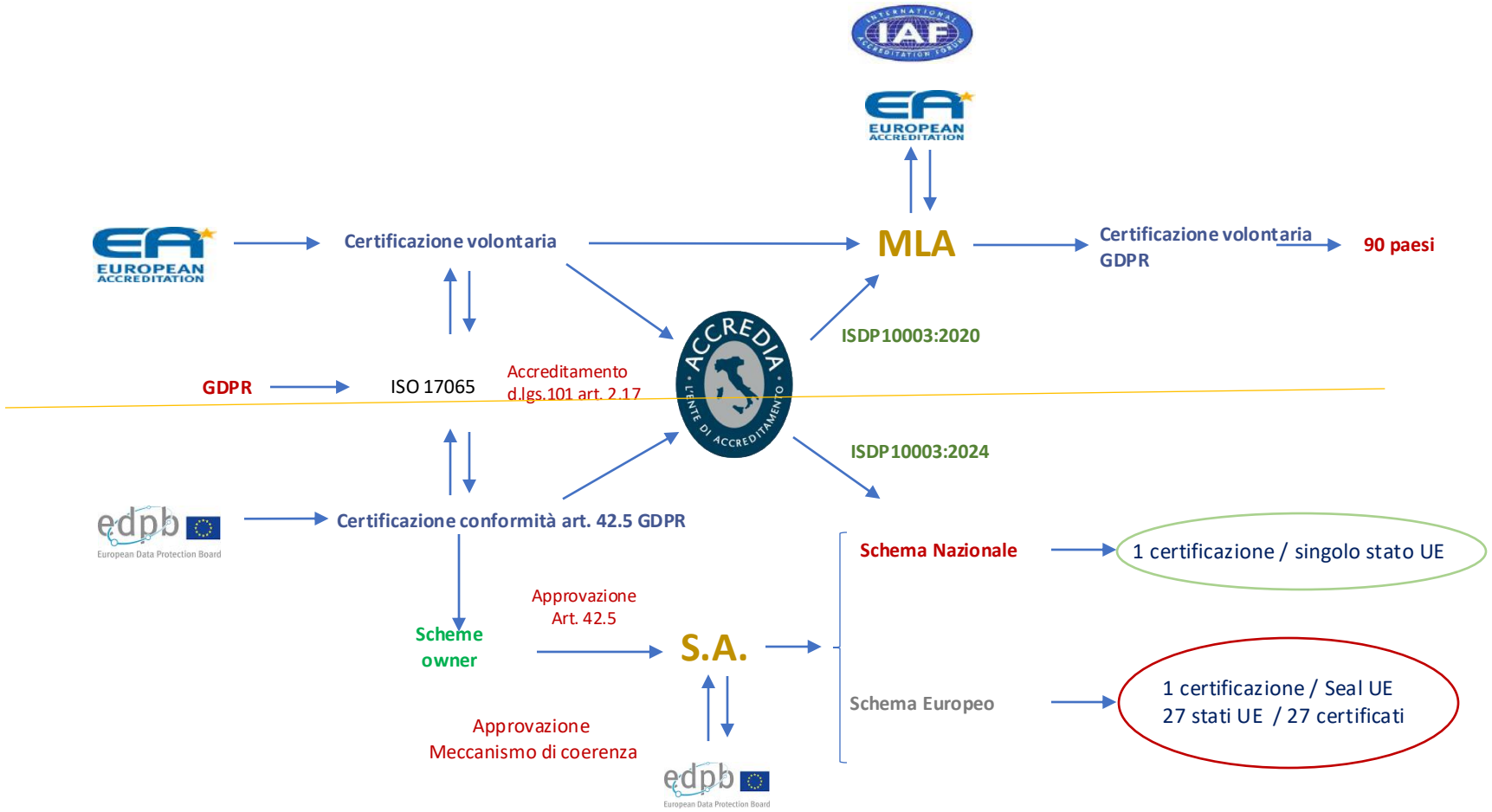
X

certificazione

Fornitori/Responsabili

Solo se coinvolti nel trattamento

certificazione → **T.O.E**: cosa è certificato (oggetto della certificazione)…


Certificazione volontaria
MLA
Certificazione volontaria GDPR
90 paesi
ISDP10003:2020
GDPR
ISO 17065
Accreditamento d.lgs.101 art. 2.17
ISDP10003:2024
Certificazione conformità art. 42.5 GDPR
Schema Nazionale
1 certificazione / singolo stato UE
Approvazione Art. 42.5
Scheme owner
S.A.
Schema Europeo
1 certificazione / Seal UE
27 stati UE / 27 certificati
Approvazione Meccanismo di coerenza

Nome schema	Scheme owner	DPA competente	Trasferimento dei dati	criterio
EUROPRIVACY	European Centre for Certification and Privacy (ECCP)	LU	No	EU Data Protection Seal
GDPR-CARPA	LU	LU	No	National certification criteria
EUROPRISE	EuroPriSe Cert GmbH	DE/LDI NRW	No	National certification criteria
BC5701:2023	Brand Compliance B.V.	NL	No	National certification criteria
AUDITOR conformity assessment	Competence Centre Trusted Cloud e.V.	DE/LDI NRW	No	National certification criteria
EuroPriSe European Privacy Seal	EuroPriSe Cert GmbH	DE/LDI NRW	No	EU Data Protection Seal
DSGVO-zt GmbH Certification criteria	DSGVO-zt GmbH	AT	No	National certification criteria
ISDP10003:2024*	INVEO srl	IT	No	National certification criteria

Certificazione Specifica (GDPR, Articoli 42-43)

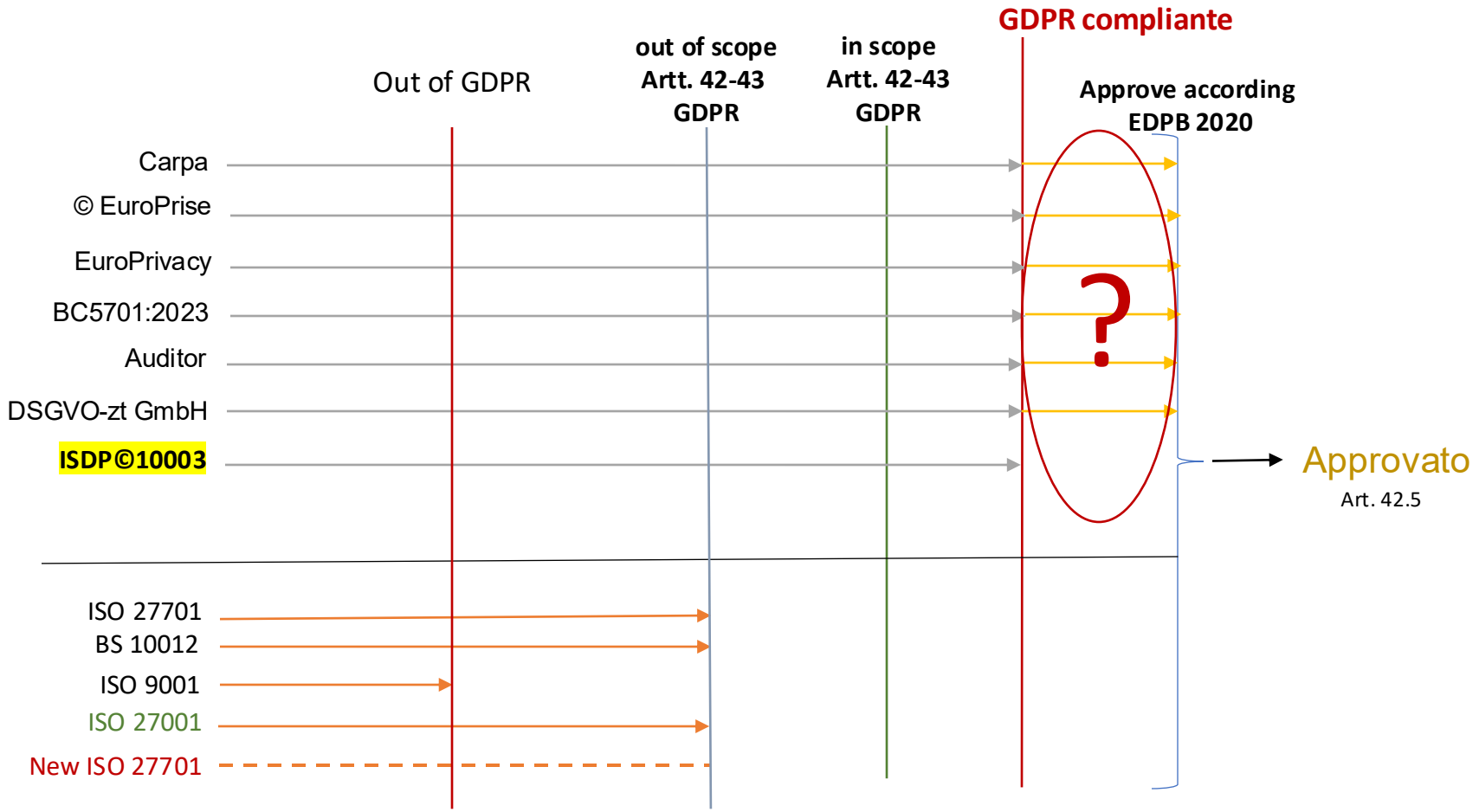
La certificazione specifica è un meccanismo di attestazione volontaria che verifica la conformità di determinati trattamenti di dati personali ai requisiti del GDPR. È basata su criteri approvati dalle autorità di controllo ed è finalizzata a garantire trasparenza, sicurezza e accountability nel trattamento dei dati (*Studio Tilburg*).

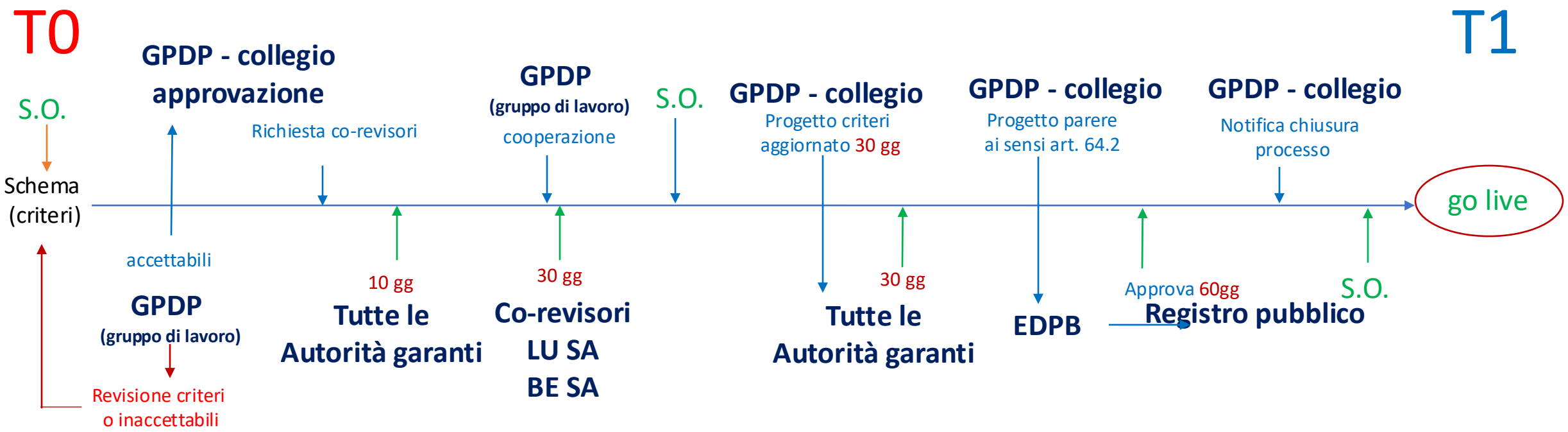
Caratteristiche	Certificazione specifica
Ambito mirato	Riguarda processi, servizi o prodotti che gestiscono dati personali.
Basata su criteri definiti	Conforme agli standard approvati da DPA o EDPB
Destinata a titolari e responsabili	Utile per dimostrare la conformità al GDPR
Volontaria ma strategica	Incrementa la fiducia e riduce il rischio di sanzioni
Integrabile con standard ISO	Compatibile ISO 17065 (*Certificazione di prodotti/servizi*).

Certificazione Aspecifica (GDPR, Articoli 42-43)

La **certificazione aspecifica** è un'attestazione che **non è direttamente legata alla conformità al GDPR**, ma riguarda aspetti più generali della gestione aziendale, della sicurezza delle informazioni o della qualità dei processi. Sebbene possa includere elementi di protezione dei dati, non è progettata per certificare specificamente il rispetto del GDPR.

Caratteristiche	Certificazione Aspecifica
Non focalizzata sui trattamenti di dati personali	Può riguardare sistemi di gestione, sicurezza IT o qualità aziendale.
Non rientra negli Articoli 42 - 43 GDPR	Non segue i criteri approvati da DPA o EDPB.
Valutazione più ampia	Certifica la gestione organizzativa o la sicurezza delle informazioni in modo generico.
Non garantisce la conformità GDPR	Può supportare la gestione della protezione dei dati in un contesto più ampio.


GDPR compliante
Out of GDPR
out of scope
Artt. 42-43
GDPR
in scope
Artt. 42-43
GDPR
Approve according
EDPB 2020
Carpa
© EuroPrise
EuroPrivacy
BC5701:2023
Auditor
DSGVO-zt GmbH
ISDP©10003
?
Approvato
Art. 42.5
ISO 27701
BS 10012
ISO 9001
ISO 27001
New ISO 27701


T0
S.O.
Schema
(criteri)
Revisione criteri
o inaccettabili
GPDP - collegio
approvazione
accettabili
GPDP
(gruppo di lavoro)
Richiesta co-revisori
10 gg
Tutte le
Autorità garanti
GPDP
(gruppo di lavoro)
cooperazione
30 gg
Co-revisori
LU SA
BE SA
S.O.
GPDP - collegio
Progetto criteri
aggiornato 30 gg
30 gg
Tutte le
Autorità garanti
GPDP - collegio
Progetto parere
ai sensi art. 64.2
EDPB
GPDP - collegio
Notifica chiusura
processo
Approva 60gg
Registro pubblico
S.O.
T1
go live


DATA PROTECTION CERTIFIED
ISDP©10003

ALLEGATO TOE

DEFINIZIONE DELL'OBIETTIVO DELLA VALUTAZIONE (Target of Evaluation)

Il titolare o il responsabile del trattamento, in collaborazione con l'Organismo di certificazione, deve definire l'obiettivo della valutazione (TOE), identificando e specificando tutte le attività di trattamento e le fasi di lavorazione dei processi, dei sistemi fisici e/o tecnologici, che rientrano nel campo di applicazione della presente certificazione.

Un'accurata specificazione dell'obiettivo della valutazione è di fondamentale importanza per una procedura di certificazione, in quanto definisce cosa è coperto dalla certificazione.
Il titolare o il responsabile deve dettagliare sistematicamente ed in modo analitico le attività di trattamento dei dati, nell'ambito dell'obiettivo di valutazione, tenendo conto di quanto riportato nel registro delle attività di trattamento in relazione ai trattamenti di dati per i quali chiede la certificazione.
L'Organismo di certificazione, nel valutare se l'obiettivo della valutazione (TOE) è compatibile con lo scopo di certificazione, può decidere di adattare l'obiettivo di valutazione nel corso del processo di certificazione.
In ogni caso l'obiettivo della valutazione (TOE) deve essere descritto in modo chiaro sul certificato.

In particolare, devono essere indicati i seguenti elementi:

- descrizione delle attività di trattamento nell'ambito dell'obiettivo di valutazione;
- definizione dell'inizio e della fine del trattamento;
- inclusione di tutti i flussi di dati, i punti di accesso e le interfacce tecnologiche, i rapporti, la trasformazione o l'esportazione dei dati, le combinazioni o fusioni di set di dati;
- descrizione degli elementi chiave, delle fasi e dei flussi dei dati, in particolare:
  - descrizione dei tipi di dati personali trattati;
  - categorie di interessati;
  - soggetti a cui i dati vengono comunicati o messi a disposizione;
  - soggetti coinvolti nel trattamento (contitolari, responsabili, sub-responsabili);
- combinazioni o fusion di banche dati;
- descrizione dell'origine dei dati;
- luoghi di svolgimento dell'attività di trattamento;
- luoghi della conservazione dei dati personali;
- diagramma di flusso o disegno, che includa anche flussi di dati esterni, interfacce di interrogazione o programmazione, aggregazioni;
- giustificazione di eventuali esclusioni di operazioni/attività di trattamento dei dati personali.

L'Allegato TOE deve essere compilato in ogni sua singola parte a cura del titolare o del responsabile del trattamento.

T = si applica al titolare
R = si applica al responsabile

ALLEGATO TOE

DEFINZIONE DELL'OBIETTIVO DELLA VALUTAZIONE				
TOE.1	**RUOLO DELL'ENTITÀ**	☐ Titolare del trattamento		
		☐ Responsabile del trattamento		
Riferimento	DEFINIZIONE CONTESTO OPERATIVO	AMBITO	ENTITÀ	
TOE.2	**CONTESTO** La definizione di questo parametro è necessaria affinché ogni componente utilizzata nella fase di certificazione sia valutata in relazione al contesto in cui l'entità opera.	Descrizione sintetica dell'attività economica		
		Settore merceologico - Codice Ateco ISTAT		
Riferimento	DESCRIZIONE ATTIVITÀ DI TRATTAMENTO	DESCRIZIONE	ENTITÀ	
TOE.3	**ATTIVITÀ SVOLTA DALL'ENTITÀ** Descrivere analiticamente la tipologia di attività di trattamento dei dati personali svolta dall'entità, nell'ambito del settore indicato.			
TOE.4	**FLUSSO DEL TRATTAMENTO - DEFINIZIONE DELL'INIZIO E DELLA FINE** Descrivere come i dati personali vengono gestiti, a partire dalla fase di raccolta dei dati fino alla fase di conclusione del trattamento. Si deve delineare in modo chiaro e cronologico il percorso attraverso cui i dati personali vengono acquisiti, elaborati, utilizzati e, infine, eliminati nel contesto dell'oggetto di certificazione. Questo flusso deve essere coerente con le disposizioni			

La tabella 1 riporta la corrispondenza fra gli aspetti di conformità richiamati dalle Linee guida EDPB 1/2018 §48 e le **sezioni** e **sottosezioni** dello schema 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 del trattamento
			A.1.2	Consapevolezza del titolare del trattamento
			A.1.3	Responsabilizzazione del responsabile del trattamento
	A.2	SOGGETTI COINVOLTI NEL PROCESSO DEL TRATTAMENTO	A.2.1	Titolare del trattamento
			A.2.2	Contitolari
			A.2.3	Selezione del responsabile del trattamento e regolamentazione dei rapporti con il titolare
			A.2.4	Responsabile della protezione dei dati
Principi applicabili al trattamento di dati personali ai sensi dell'articolo 5	A.3	PRINCIPI GENERALI, BASI GIURIDICHE DEL TRATTAMENTO E TUTELA DEGLI INTERESSATI	A.3.1	Principi applicabili al trattamento di 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	Tempistiche e contenuto dell'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	PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PER IMPOSTAZIONE PREDEFINITA	A.4.1	Protezione dei dati fin dalla progettazione
			A.4.2	Protezione dei dati per impostazione predefinita

Misure tecniche e organizzative messe in atto a norma dell'art. 32	A.5	GESTIONE DEL RISCHIO E SICUREZZA DEI DATI PERSONALI	A.5.1	Gestione del Rischio del trattamento di dati personali
			A.5.2	Sicurezza del trattamento: misure tecniche per la protezione dei dati personali
			A.5.3	Sicurezza del trattamento: misure organizzative per la protezione dei dati personali
Valutazione d'Impatto a norma art. 35	A.6	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI	A.6.1	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 (SE APPLICABILE)	A.7.1	Modalità di trasferimento dei dati fuori dall'UE
Obbligo di notifica delle violazioni dei dati ai sensi dell'art. 33 e 34	A.8	VIOLAZIONE DEI DATI PERSONALI	A.8.1	Violazione di dati personali

Riferimenti normativi linee guida ISO

2 RIFERIMENTI NORMATIVI

Il riferimento ai documenti e alle disposizioni di seguito riportate è indispensabile ai fini dell'applicazione del presente schema:

- art. 42 del RGPD;
- EDPB, Linee guida 1/2018 relative alla certificazione e all'identificazione di criteri di certificazione in conformità degli articoli 42 e 43 del regolamento (UE) 2016/679 (e relativi allegati, con riferimento all'Allegato 2);
- EN ISO/IEC 17065:2012;
- EN ISO/IEC 17067:2013;

Ai fini del presente schema, devono altresì considerarsi pienamente applicabili le seguenti linee guida[2]:

- EN ISO 19011;
- ISO/IEC 28590;
- ISO 31000.

Sezione

Sottosezione

Criterio

Riferimenti normativi

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.	Art. 24, C. 74, EDPB 4/2019	T	
		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.			

Indicazioni operative per l'Entità

Note Auditor

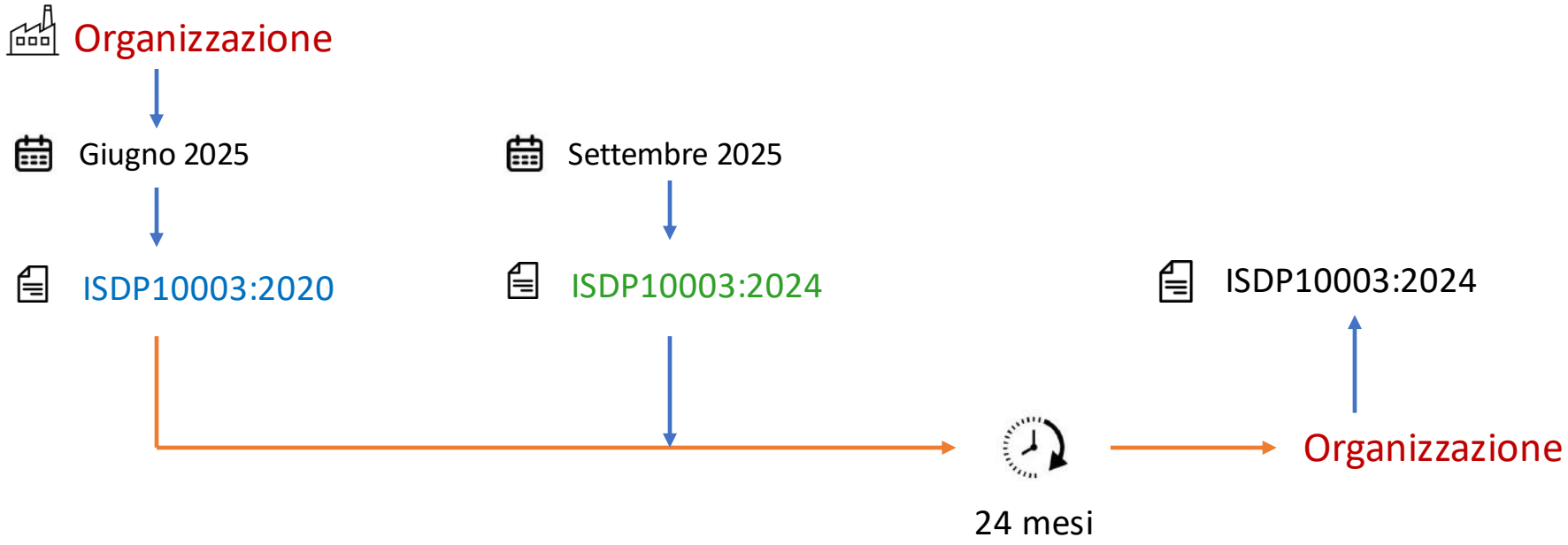
Descrizione criterio

Punto norma

Tabella comparativa NIS2 e certificazione ISDP10003… esempio di Metalinguaggio

Area / Processo	Asset o trattamento	Normativa NIS2 / D.Lgs. / ACN	Criterio ISDP10003:2024	Note sulla corrispondenza
Sicurezza fisica	Data center, sale server	NIS2 Art. 21(2)(g), D.Lgs. 138/2024 Art. 9(2)(g), ACN: protezione accessi fisici	A.5.1.4 (Sicurezza fisica)	Corrispondenza diretta
Backup e continuità operativa	Dati critici / sistemi ERP	NIS2 Art. 21(2)(f), D.Lgs. 138/2024 Art. 9(2)(f), ACN: business continuity plan, backup crittografato, test annuali	A.5.1.8 (Business continuity)	Criterio coerente ma meno dettagliato: ISDP non richiede frequenza test né verifica backup
Logging e tracciamento	File di log / monitoraggio attività	NIS2 Art. 21(2)(e), ACN: log retention ≥ 6 mesi, integrità log, protezione da accessi non autorizzati	A.5.1.3 (parte su logging)	Copertura parziale: ISDP suggerisce logging ma non entra nel dettaglio tecnico richiesto da ACN
Formazione e consapevolezza	Personale dipendente e amministratori	NIS2 Art. 21(2)(j), D.Lgs. 138/2024 Art. 9(2)(j), ACN: obbligo di formazione periodica, simulazioni, awareness	A.5.1.2 (Consapevolezza e formazione)	Coincidenza piena
Crittografia e sicurezza dei dati	Dati in transito e archiviati	NIS2 Art. 21(2)(c-d), D.Lgs. 138/2024 Art. 9(2)(c-d), ACN: cifratura obbligatoria dei dati sensibili, controllo chiavi	A.5.1.6 (Protezione dati personali)	ISDP considera protezione logica dei dati, ma è meno prescrittivo su algoritmi e gestione crittografica

Transizione



NEXT
GENERATION

Grazie dell’attenzione
e… seguitemi su Linkedin!

Riccardo Giannetti

riccardo-giannetti-8758688

inveo GROUP