la progettazione dei trattamenti e loro valutazione utilizzando lo schema ISDP 10003:2020

Andrea Piccoli
Chief Digital Officer

D&L Network
ANORC Triveneto

Mi presento!

Andrea Piccoli

Professionista della digitalizzazione e privacy.

Valutatore per lo schema ISPD 10003:2020.

Delegato territoriale e Chief Digital Officer in ANORC Professioni, membro del D&L Network.

- Seguo da anni progetti di digitalizzazione dei processi aziendali con un approccio multidisciplinare che coniughi gli aspetti normativi, informatici e archivistici.
- Mi occupo si sistemi di gestione per la Compliance, Risk and Management con particolare riferimento alla sicurezza e protezione delle informazioni.

I miei corsi:

- GDPR in pratica per aziende e titolari
- Formare, firmare, gestire, archiviare e conservare i documenti informatici
- Il responsabile della conservazione e dell'archivio digitale nelle aziende

ANORC Triveneto

D&L net

Privacy by design , privacy by default

Sono tutte le attività aziendali che **per conto dell'azienda** stessa o **per conto di altri** gestiscono **dati personali**

Trattamento è **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.

Ad esempio: 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.**

I soggetti che procedono al trattamento dei dati personali altrui devono adottare particolari **misure per garantire il corretto e sicuro utilizzo dei dati.**

ANORC Triveneto

D&L net

Privacy by design , privacy by default

I trattamenti devono essere progettati, non basta documentarli

- Essere pronti a rispondere quando qualcosa va male
- Poter evidenziare quanto fatto e valutato
- Per poter misurare quando valutato e accaduto
- Per poter migliorare costantemente la gestione dei rischi sulla protezione dei dati personali

ANORC Triveneto

D&L net

Valutare i trattamenti **prima** del loro avvio

Valutare i trattamenti, ovvero la loro conformità al GDPR, è **nettamente più ampio della valutazione dei rischi sulla protezione delle informazioni**.

- Il focus **della valutazione parte dalla accountability del Titolare** e deve valutare le misure organizzative e tecniche poste in essere focalizzandosi sul grado di preparazione e consapevolezza dei trattamenti e della loro gestione.

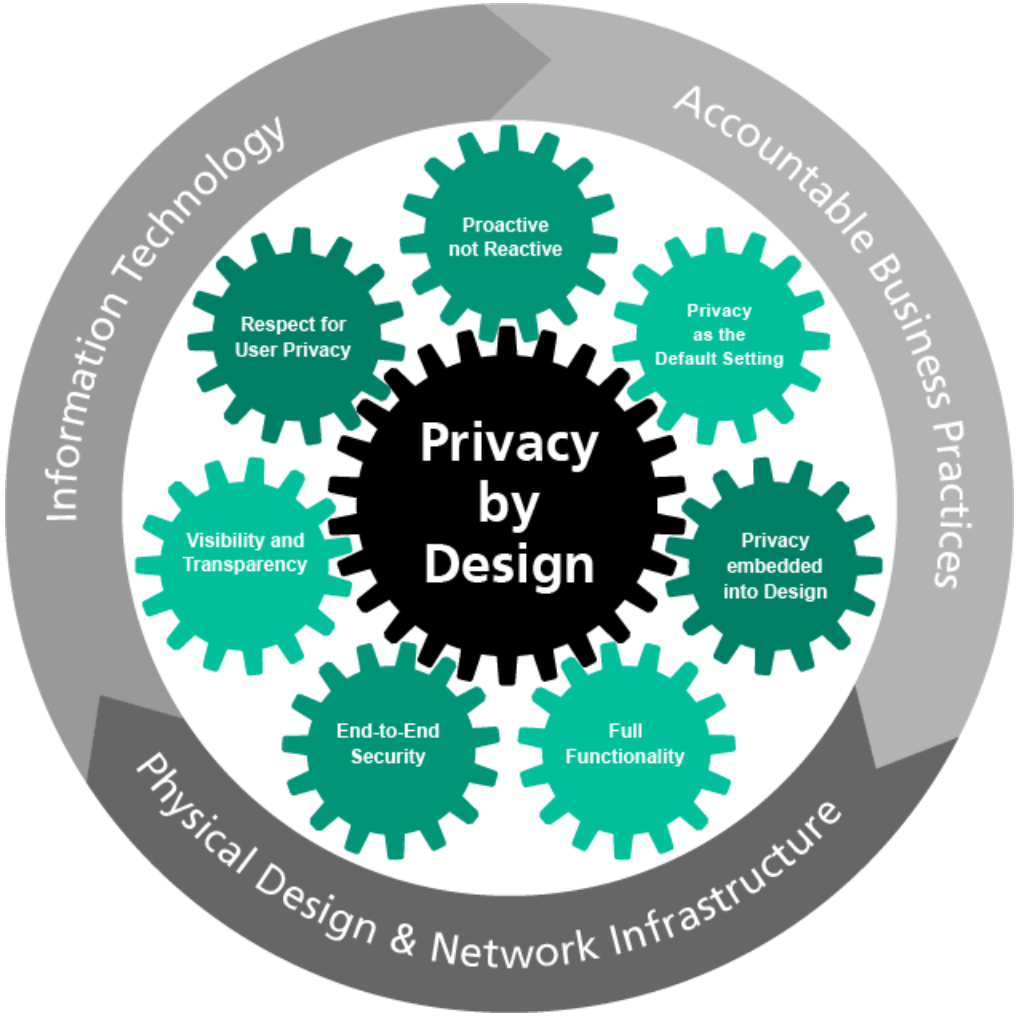
- Il focus della seconda è **valutare gli accadimenti che possono minare l'obiettivo della protezione delle informazioni trattate e delle misure poste in essere per mitigarne i rischi conseguenti**. (Risk , DPIA)

Entrambe sono attività richieste da fare **prima** dell'avvio del trattamento e da **revisionare periodicamente sulla base degli accadimenti registrati e delle modifiche organizzative e tecniche apportate**

ANORC Triveneto

D&L net

Privacy di design -> Progettazione



L'accadimento del Data Breach non deve essere ritenuto un evento «improbabile» ma come parte integrante del trattamento stesso.

- Come reagisce l'organizzazione al Data Breach ?
- Come reagiscono le soluzioni ai Data Breach ?
- Come reagiscono le infrastrutture ai Data Breach ?

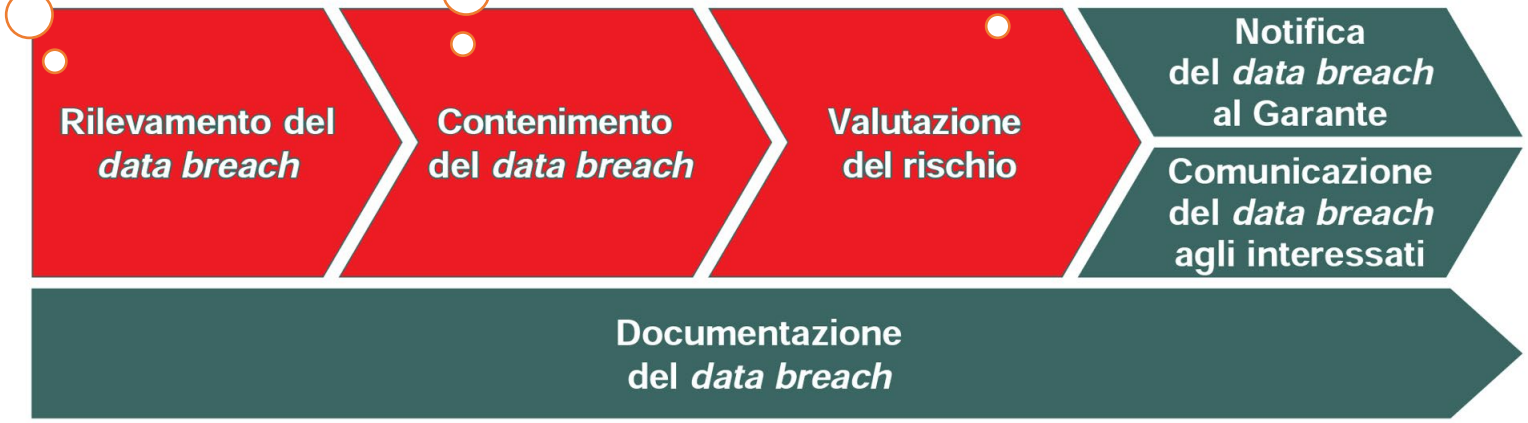
Includere la gestione del Data Breach nella progettazione

Come me ne accorgerò ?

Cosa farò ?
Cosa potrò fare?

Quali rischi per gli interessati se accadrà

Violazione della disponibilità	Violazione dell'integrità	Violazione della riservatezza
distruzione o perdita non autorizzate di dati personali	*modifica non autorizzata di dati personali*	*divulgazione o accesso non autorizzati a dati personali*



ANORC Triveneto

D&L net

I rischi e il GDPR

Rischi GDPR

i diritti e le libertà delle persone fisiche

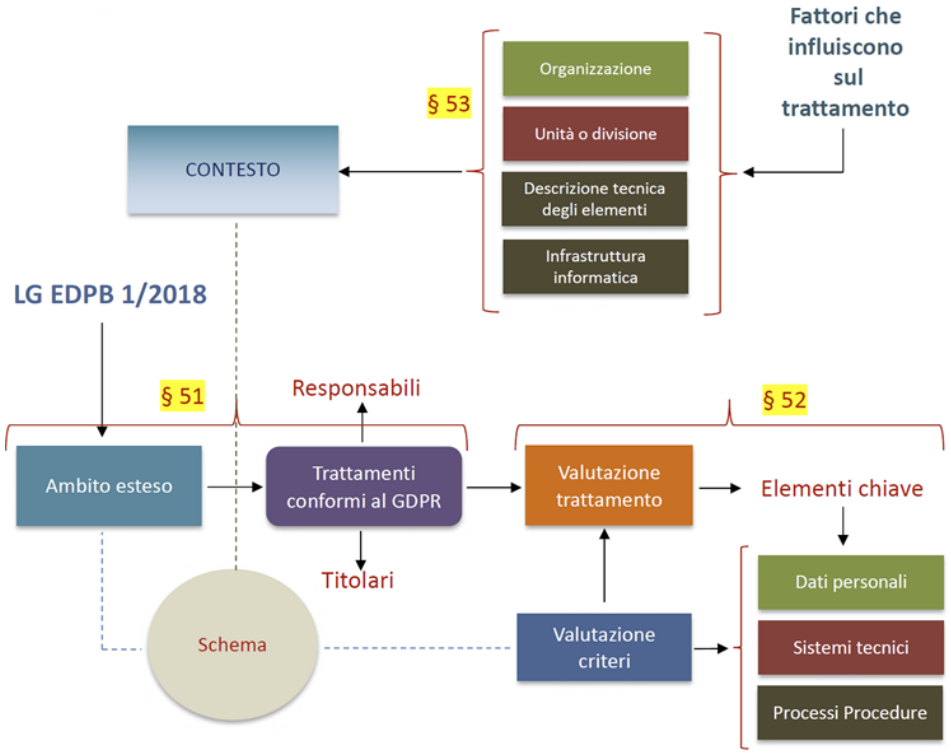
	Scopo	Fattori da considerare	Valutazioni	Rischio
Rischio inerente Calcolare sempre	Mantenere la sicurezza e prevenire trattamenti in violazione al GDPR	Rischi inerenti al trattamento	Ipotetica previsionale	Distruzione accidentale Distruzione illegale Perdita Modifica Rivelazione Accesso non autorizzato
Rischio di Impatto Solo rischio elevato/art. 35(3)	Potenziare il rispetto del GDPR qualora i trattamenti possano presentare un **rischio elevato** per i diritti e le libertà	Rischi del trattamento dei dati e **ipotesi di rischio** in caso di violazione per i diritti e libertà	Ipotetica previsionale	Discriminazione Furto o usurpazione identità Perdite finanziarie Pregiudizio alla reputazione Perdita riservatezza Decifratura non autorizzata Altro danno economico o sociale significativo
Rischio Data breach Calcolare entro 72h	Affrontare in modo adeguato e tempestivo le violazioni dei dati personali al fine di evitare danni, fisici materiali , immateriali.	Rischio risultante dall'impatto della **violazione avvenuta**, sulle persone fisiche	effettiva qualitativa	Discriminazione Furto o usurpazione identità Perdite finanziarie Pregiudizio alla reputazione Perdita riservatezza Decifratura non autorizzata Altro danno economico o sociale significativo

Danno cagionato
Materiale, Immateriale, Fisico

Abbiamo progettato correttamente ?

L'adesione a un **codice di condotta** approvato di cui all'articolo 40 GDPR o a un **meccanismo di certificazione** approvato di cui **all'articolo 42 GDPR** può essere utilizzata come elemento per dimostrare la conformità ai requisiti

valutare l'adozione volontaria a schemi di valutazione per la conformità al GDPR come ISPD 10003:2020 (o altri schemi riconosciuti)



MACRO PROCESSI DELLO SCHEMA DI VALUTAZIONE PER LA CONFORMITA' DEL TRATTAMENTO	Applicazione
4.1 - POLITICA E OBBLIGAZIONI DEL TITOLARE	5 / 0
4.2 - SOGGETTI COINVOLTI NEL PROCESSO DEL TRATTAMENTO	20 / 0
4.3 - PRINCIPI APPLICABILI AL TRATTAMENTO E TUTELA DEI DIRITTI	50 / 0
4.4 - PROCESSI DI ADEGUAMENTO IN FASE DI IDEAZIONE ED ALL'ATTO DEL TRATTAMENTO (privacy by design e by default)	10 / 0
4.5 - OBBLIGHI GENERALI, GESTIONE DEL RISCHIO E SICUREZZA DEI DATI PERSONALI	50 / 0
4.6 - VALUTAZIONE D'IMPATTO	5 / 0
4.7 - TRASFERIMENTO DEI DATI PERSONALI VERSO PAESI TERZI E CLOUD COMPUTING	10 / 0

inveo
ACCREDITED CERTIFICATION BODY

ANORC Triveneto

D&L net

ISPD 10003:2020

PRIVACY TOOLS (in-veo.com)

inveo
ACCREDITED CERTIFICATION BODY

Struttura tecnica 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 respon[illegible] generale del titolare 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.

Allegato B

ALLEGATO B MAPPATURA CORRISPONDENZE ARTICOLI DEL GDPR E SCHEMA ISDP©10003

schema ISDP©10003	GDPR
Requisiti generali	Articolo GDPR – Linea guida 1/2018 4/2018 EDPB
§ 0.1	§1 EDPB 1/2018, §5 EDPB 1/2018 art. 42.1
§ 0.2	§5 EDPB 1/2018,
§ 0.3 – nota 1 (a) (b)	§5 EDPB 1/2018, art. 32 (1) (d), art. 32 (1) (b),
§ 0.4	§6.1 EDPB 1/2018
§ 1.1	§1.2 EDPB 1/2018, §5.2 EDPB 1/2018, art.42(1), art. 42(7), art. 32(1)(d)
§ 1.2	§5.1 EDPB 1/2018, art. 28(1), art. 42(1)
§ 4	§1 WP29 260 rev. 01, art. 5 (1)
§ 5	§7 EDPB 1/2018 allegato 2, Art. 5 (1) (2), cons. 83
§ 6	Art. 32(1) (2), art. 35(1) (7), art. 36, cons. 78, 83, 84
§ 7	Art. 32(1) (2), art. 35(1) (7), art. 36, cons. 78, 83, 84, allegato 2 EDPB 1/2018,
§ 8	Art. 30, cons.82, art. 25, art. 32, art. 35,
§ 9	Art. 5, art.24, art.28
§ 10	Art. 5, art.24, art.28
Controlli Allegato A	Articolo GDPR – Linea guida
A.1.1.1	Art. 5 (2), art. 24, cons. 74, 79, §5 EDPB 1/2018
A.1.1.2	Art. 5 (2), art. 24,
A.1.1.3	Art. 5 (2), art. 24, cons. 79,
A.1.1.4	Art. 5 (2), art. 24,
A.1.1.5	Art. 5 (2), art. 24,
A.1.1.6	Art. 24
A.2.1.1	Art. 4 (7), art. 24, cons. 74
A.2.1.2	Art. 4 (7), art. 24, cons. 80
A.2.1.3	Art. 4 (7), art. 24, cons. 74
A.2.2.1	Art. 4 (7), art. 26, cons. 74, 79
A.2.2.2	Art. 4 (7), art. 26, cons. 74, 79

ANORC Triveneto

D&L net

EDPB <-> ISPD

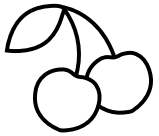
EDPB 1/2018	ISPD 10003:2020
Liceità del trattamento (art.6)	A.1 Politiche e obbligazioni del titolare
	A.2. Soggetti coinvolti nel processo del trattamento
Principi del trattamento (art. 5)	A.3 Principi applicabili al trattamento e tutela dei diritti
Diritti degli interessati (art. da 12 a 23)	
Obbligo di notifica delle violazioni dei dati (art. 33)	A.5 Obblighi generali, gestione del rischio e sicurezza dei trattamenti
Obbligo della protezione dei dati fin dalla progettazione e dalla protezione dei dati per impostazione predefinita (art.25)	A.4 Processi di adeguamento in fase di ideazione e all'atto del trattamento
Valutazione d'impatto (art.35)	A.6 Valutazione d'impatto
Misure tecniche e organizzative messe in atto (art. 32)	A.5 Obblighi generali, gestione del rischio e sicurezza dei trattamenti
	A.7 Trasferimento dei dati personali verso paesi terzi, IOT e Cloud

edpb
European Data Protection Board

ANORC Triveneto

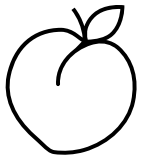
D&L net

lo schema ISDP 10003:2020 vs ENISA (DPIA CNIL)



Gli strumenti di valutazione dei rischi di ENISA e lo strumento delle DPIA del CNIL sono molto utili come guida per la valutazione dei rischi, delle minacce, misure applicate. Sono fondamentali per la valutazione d'impatto e forniscono informazioni utili alla valutazione dei trattamenti.

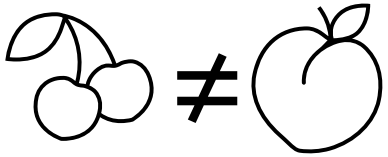
Mancano della parte «organizzativa» del trattamento



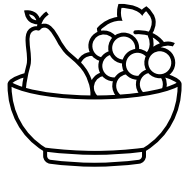
Esiste la certificazione GDPR (art. 42 e 43) che ha il preciso compito di garantire i diritti e le libertà' degli interessati, aiutando il titolare e responsabile a tutelare la sua accountability.

Valutano l'intero contesto del trattamento

Sono comparabili ? … **NO**



Sono compatibili ? **SI**



lo schema ISDP 10003:2020 vs ISO 27701

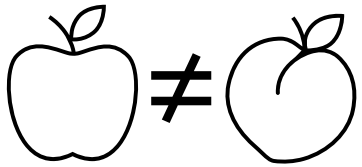
Esistono certificazioni (ISO 9001, ISO 27001, ISO 27701, ISO ecc.) che hanno lo scopo di garantire la sicurezza, protezione, della qualità, delle informazioni, della continuità operativa, ecc.

Sono sistemi di gestione (prodotto / servizio)

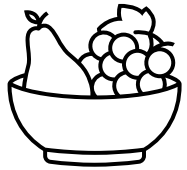
Esiste la certificazione GDPR (art. 42 e 43) che ha il preciso compito di garantire i diritti e le libertà' degli interessati, aiutando il titolare e responsabile a tutelare la sua accountability.

Non sono un sistema di gestione, ma integrabili in quest'ultimi

Sono comparabili ? … **NO**



Sono compatibili ? **SI**



GRAZIE

andrea.piccoli@dlnetwork.it
https://www.linkedin.com/in/piccolia