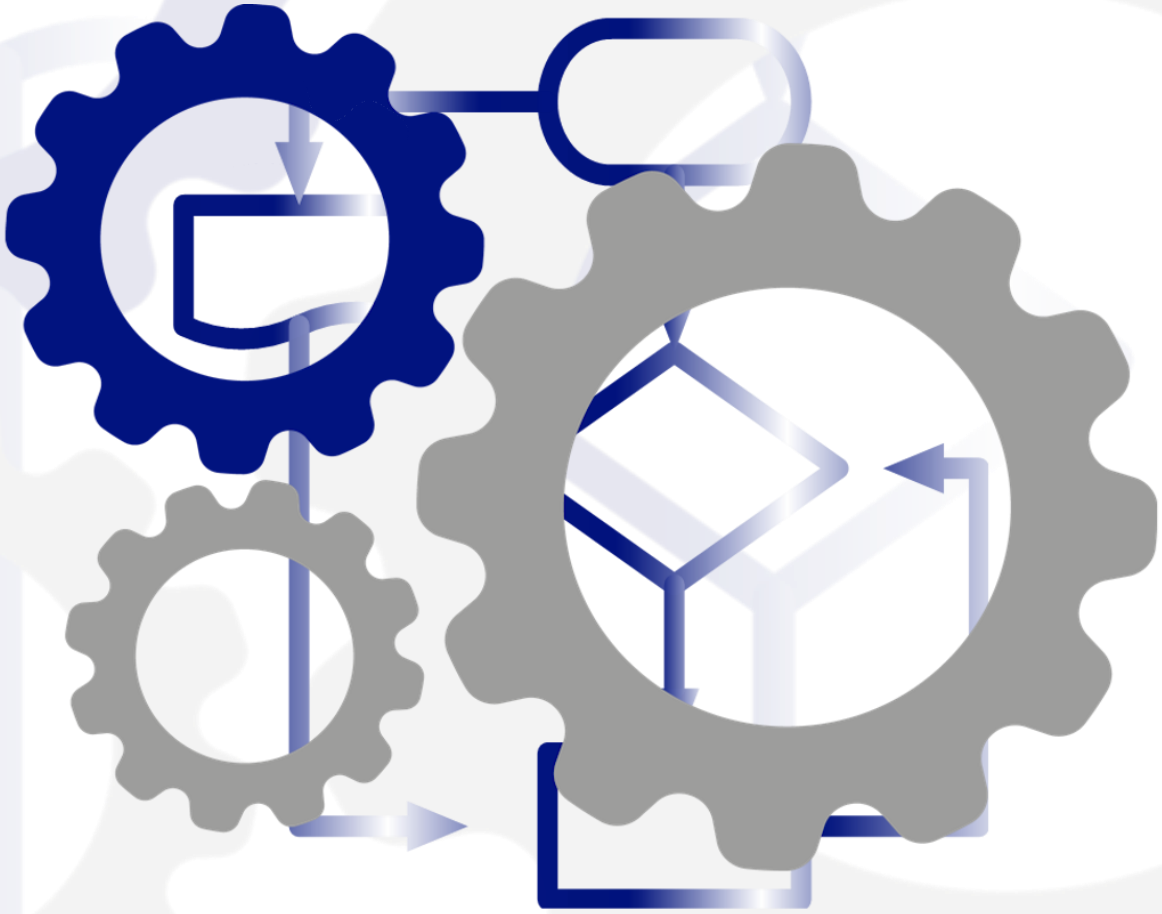
www.acsweb.it

acs srl
SYSTEM & CONSULTING



Data Protection & Governance Framework

ORGANIZZARE PER PROTEGGERE

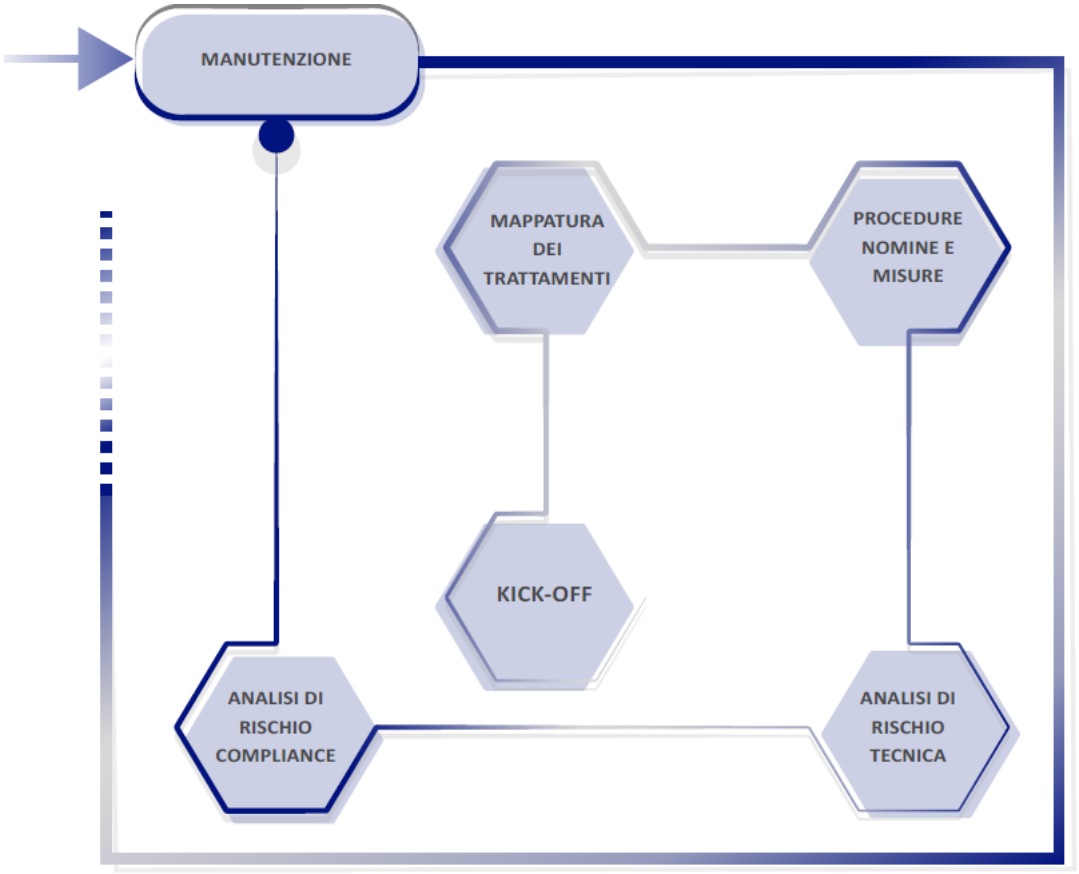
Il Regolamento (UE) 2016/679, rappresenta una pietra miliare nella protezione dei dati personali in un'epoca in cui la tecnologia e l'uso di dati personali sono diventati elementi centrali nella vita quotidiana e nell'economia.

Il GDPR può essere interpretato come un “foglio bianco” nel quale sono definiti solo i margini entro cui le organizzazioni possono “disegnare” i loro processi di funzionamento, avendo quindi la libertà di definire il modello di gestione che più si adatta alle esigenze specifiche.

In tale direzione abbiamo sviluppato un modello organizzativo altamente scalabile e flessibile capace di analizzare e strutturare le fasi del processo consentendo di progettare le proprie attività nel modo più efficace possibile.

Grazie alla ventennale esperienza nel settore della protezione dei dati e alle nostre precise competenze, siamo quindi in grado di guidare, supportare e affiancare le aziende in questo processo organizzativo.

IL FRAMEWORK



IL METODO

KICK-OFF

Descrizione delle finalità e della struttura del modello organizzativo.

Redigere un modello organizzativo completo e aggiornato è fondamentale per garantire che un'azienda funzioni in modo efficace.

In questo modo si promuove l'innovazione, la crescita sostenibile e la cultura del dato.

MAPPATURA DEI TRATTAMENTI

Il fulcro del metodo è costituito dal Registro dei trattamenti.

Questo rappresenta l'elemento cardine e il principale strumento di controllo dei trattamenti posti in essere dall'azienda.

Disporre di un registro aggiornato e schematizzato consente infatti di garantire il principio dell'accountability.

PROCEDURE, NOMINE E MISURE

Allo scopo di completare il quadro informativo, il metodo proposto prevede:

- la proceduralizzazione dei processi;
- l'individuazione e formalizzazione di tutte posizioni critiche nelle attività di trattamento:
- l'indicazione delle misure tecniche e organizzative messe in atto per garantire adeguati livelli di protezione.

ANALISI DI RISCHIO TECNICA

Si tratta di una valutazione dei rischi conseguenti alla messa in atto di qualsiasi attività che implica l'utilizzo di risorse IT.

Tale valutazione viene effettuata sulla base di un apposito registro dei servizi IT presenti in un'organizzazione.

La metodologia applicata è basata sulla CIA Triad (confidenzialità, integrità e disponibilità).

ANALISI DI RISCHIO COMPLIANCE

Si tratta di una valutazione dei rischi conseguenti alla messa in atto di attività di trattamento dei dati personali.

Questa è basata sui principi definiti dall'Art.6 del GDPR (liceità, correttezza e trasparenza, limitazione delle finalità, minimizzazione dei dati, esattezza e aggiornamento dei dati, limitazione della conservazione, integrità e riservatezza).

MANTENIMENTO

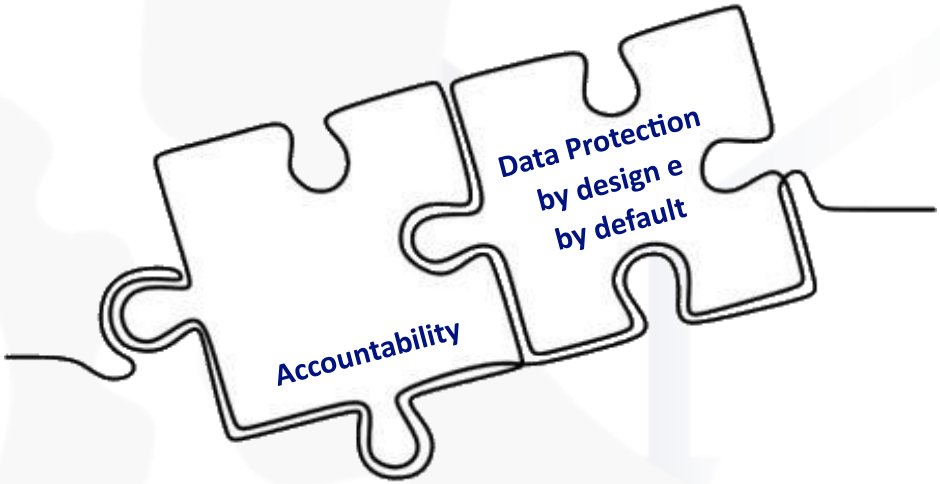
Quando si parla di manutenibilità, nel contesto organizzativo, si fa riferimento alla capacità dell'azienda di gestire e far evolvere il proprio impianto organizzativo nel corso del tempo.

Il mantenimento è pertanto un processo continuo di monitoraggio, adattamento e miglioramento per garantire la protezione dei dati trattati ed il successo a lungo termine dell'organizzazione.

IL GDPR

dalla privacy alla protezione dei dati

Il GDPR rappresenta un vero e proprio cambio di approccio poiché introduce due concetti fondamentali relativi alla protezione dei dati personali:



Non si parla più di oneri formali legati alla "privacy",
ma di oneri sostanziali legati alla
"protezione dei dati personali".

LA DIRETTIVA NIS 2

La Direttiva NIS 2 (Network and Information Security 2) ha come scopo principale quello di rafforzare la sicurezza informatica nell'Unione, in risposta alle crescenti minacce.

I principi cardine di questa normativa sono:

- approccio di valutazione basato sul rischio
- adozione di misure tecniche e organizzative appropriate
- responsabilità diretta degli organi di gestione (management)
- obbligo di formazione
- estensione alla sicurezza della supply chain

Se non sono direttamente soggetto a NIS 2, ma lo sono uno o più clienti, dovrò aspettarmi che vengano analizzati e valutati i miei comportamenti e processi in tema di cybersecurity.

GDPR e NIS 2

diversi punti di vista, stesso obiettivo

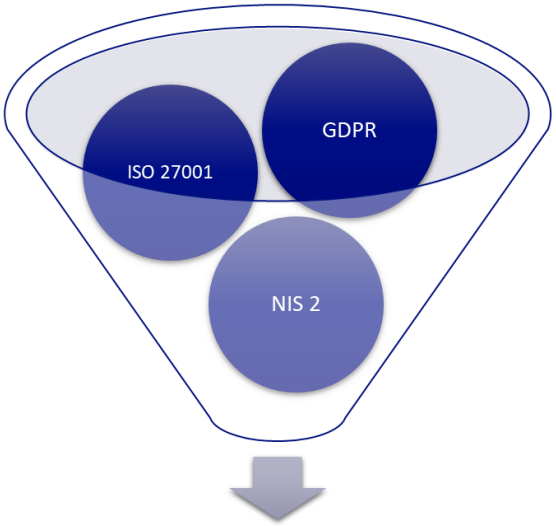
Il GDPR e la NIS 2, pur avendo approcci diversi, condividono l'obiettivo di migliorare la sicurezza e la protezione delle informazioni nell'Unione Europea.

Entrambi i regolamenti contribuiscono a creare un ambiente digitale più sicuro e affidabile, affrontando aspetti complementari della protezione dei dati e sicurezza informatica.

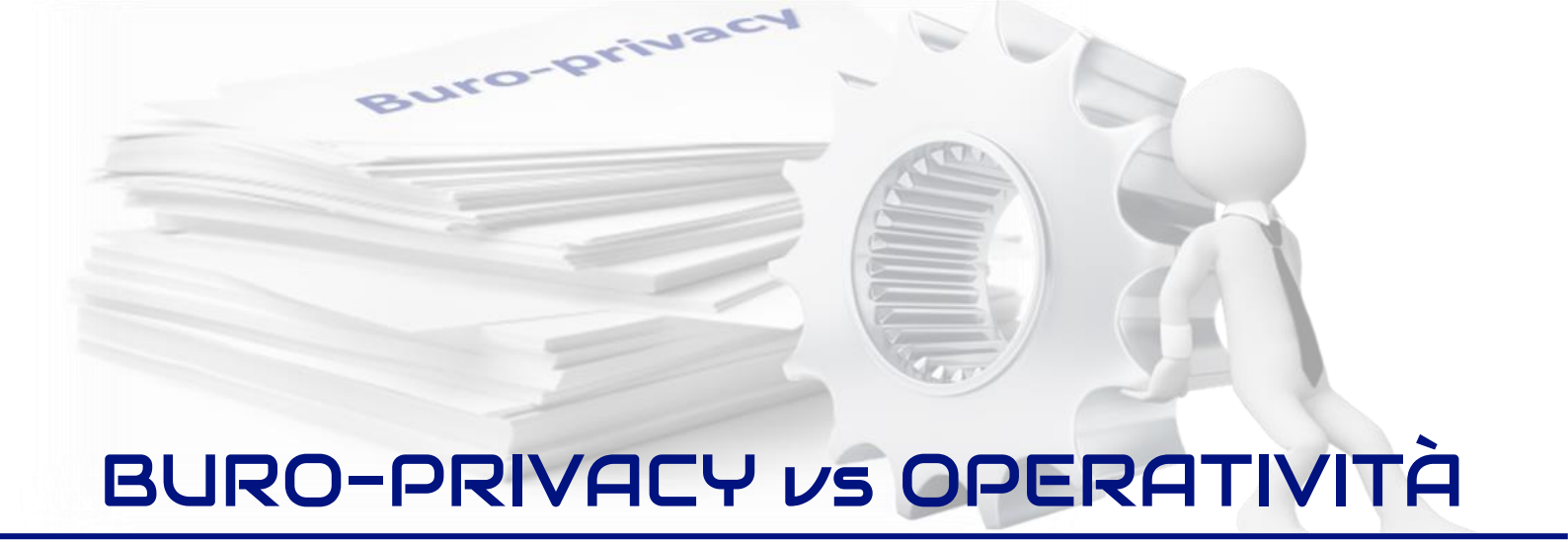
La NIS 2 quindi può essere rappresentata come un naturale complemento del GDPR poiché estende il campo applicativo della protezione dai dati personali ai dati e informazioni in generale.

IL MODELLO INTEGRATO

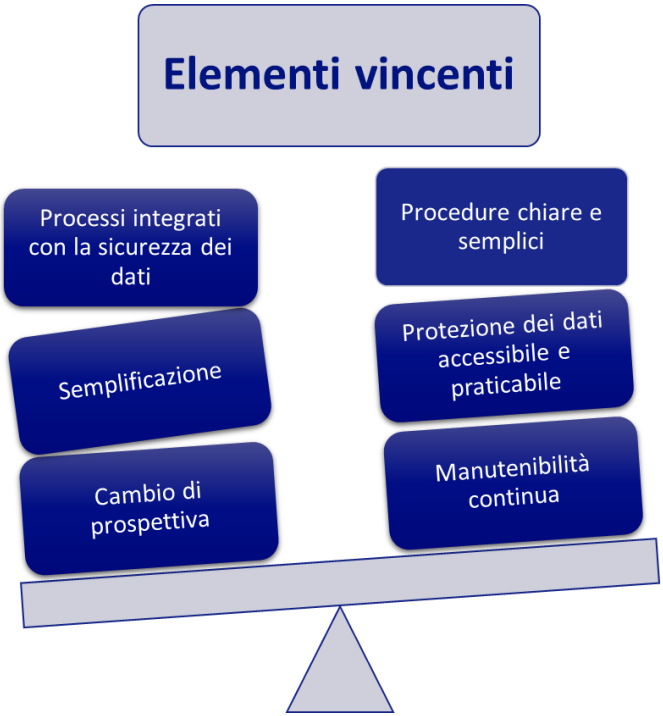
Il DPGF è un modello organizzativo **integrato** e **scalabile** che viene adattato ad ogni realtà aziendale in grado di valutare, gestire e monitorare la maturità dei processi e dei comportamenti aziendali in ottica di protezione dei dati e delle informazioni, personali e non.



Modello organizzativo integrato

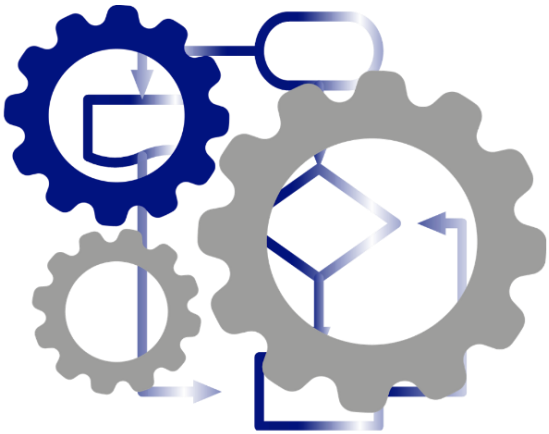


BURO-PRIVACY vs OPERATIVITÀ



La protezione dei dati e delle informazioni non deve schiacciare l'azienda, ma farla crescere al meglio!

Il nostro team avrà il compito di accompagnare e guidare l'azienda nel **processo** e nel **mantenimento continuo** del modello organizzativo configurato.



ACS srl – Amministrazioni & Consulenze Sistemi srl

Via Cesari 1/A – 26100 Cremona
C.C.I.A.A. CR 01361380197 | R.E.A. 164622 | C.F. e P.I. 01361380197
+39 0372 800543 | pec@pec.acsweb.it | info@acsweb.it | www.acsweb.it