REGIONE PIEMONTE

CSI your digital partner

SICURI di essere SICURI?

Privacy e cybersecurity per gli Enti locali

Le misure di sicurezza adeguate: dalla teoria alla pratica

10 maggio| ore 10.30 - 12.00

Presentiamoci:
Chi siamo

Salvatore Maugeri

Avvocato – Ordine Avvocati Tribunale di Enna

Data Protection Officer presso enti pubblici e Collegi professionali

Consulente privacy

Socio del Centro Studi di informatica Giuridica di Ivrea e Torino

Il processo di gestione del rischio

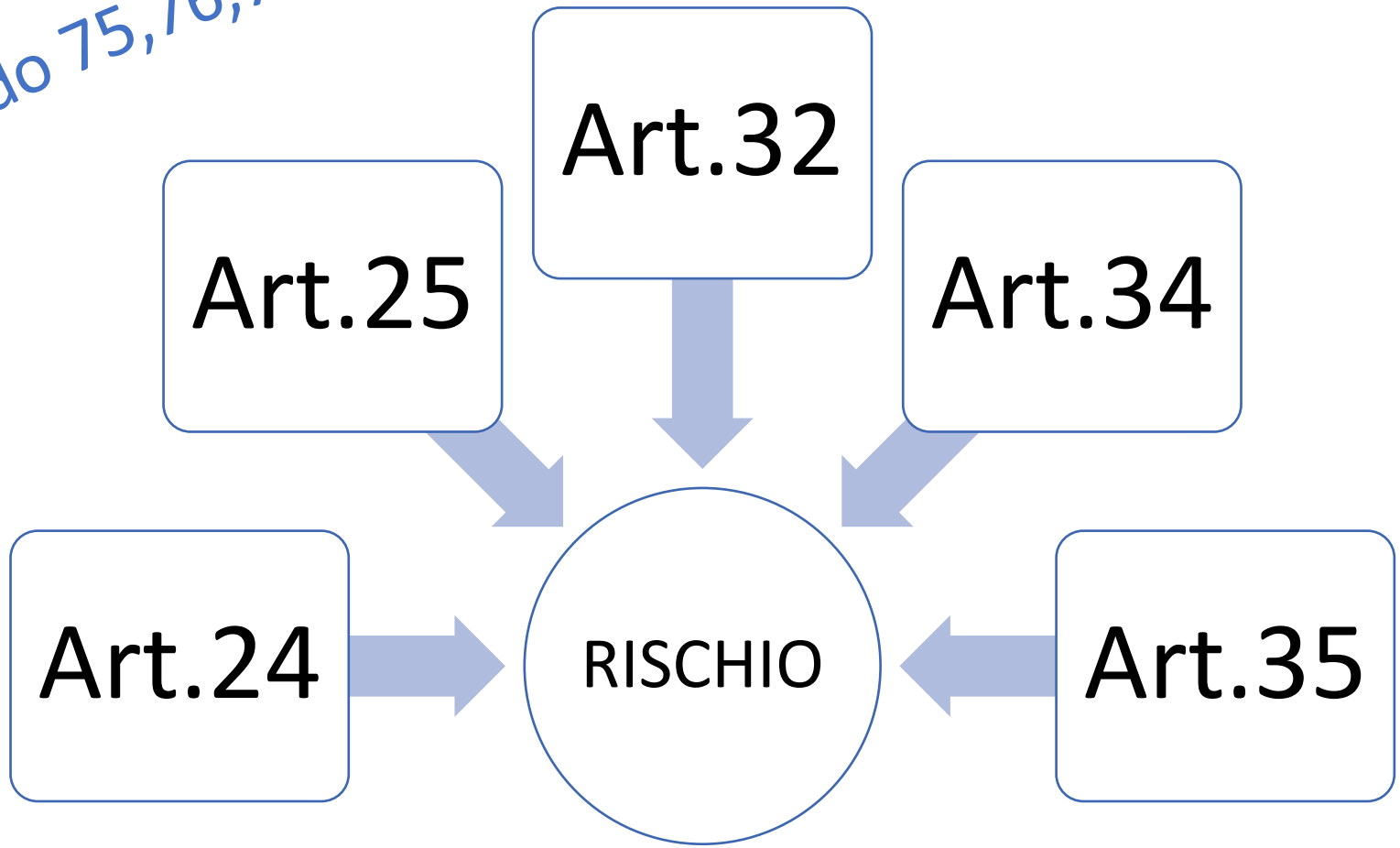
***

suggerimenti utili per

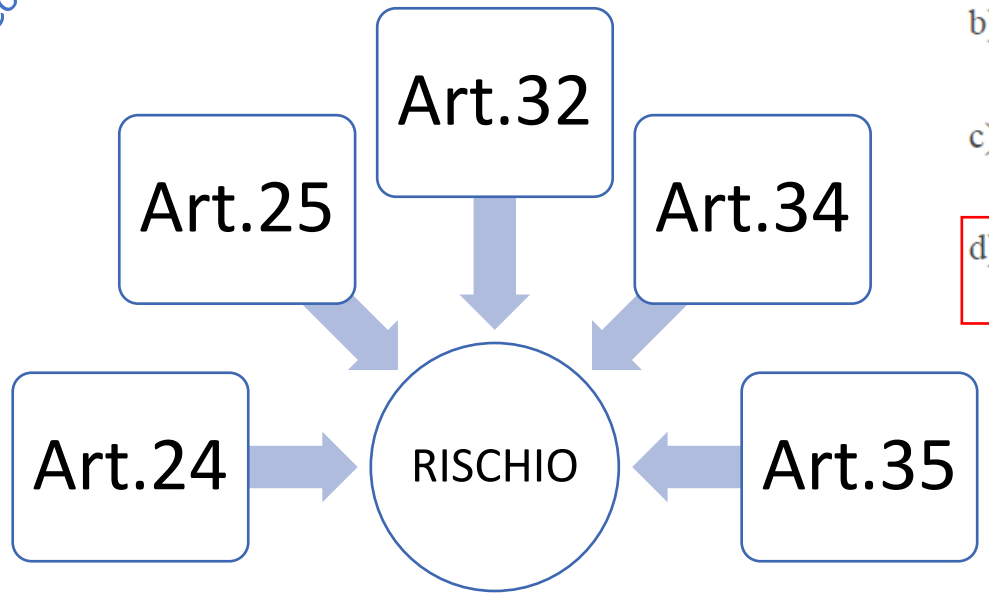
*l'adozione di una **metodologia di valutazione del rischio** del trattamento*

GDPR e rischio

Considerando 75,76,77



Considerando 75,76,77



Sezione 2
Sicurezza dei dati personali

Articolo 32

Sicurezza del trattamento

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

.... adottare una buona **metodologia**....

Definizione di «rischio» ?

- Rischi concernenti la **SICUREZZA** dei DATI (informatica/fisica) o del TRATTAMENTO in sé
- Rischi per i **diritti e le libertà delle persone** fisiche
- Rischi indipendenti da una violazione e rischi conseguenti a una **violazione**

- …. anche la «***non conformità***» è un rischio …

➔ vedi art. 3, 2 comma, lett. n) del D.Lgs. 65/2018, attuazione alla Direttiva NIS 1148/2016

"…*ogni circostanza o evento ragionevolmente individuabile con potenziali effetti pregiudizievoli*…"

E’ come muoversi in un labirinto...

Labirinto di Arianna
1990 – Italo Lanfredini
opera d’arte contemporanea che fa parte della Fiumara d’Arte
Castel di Lucio (ME) – Nebrodi -

Quale metodologia ?

ISO/IEC 29134:2017
Guidelines for privacy impact assessment.

standard ISO 31000:2018 - Risk management

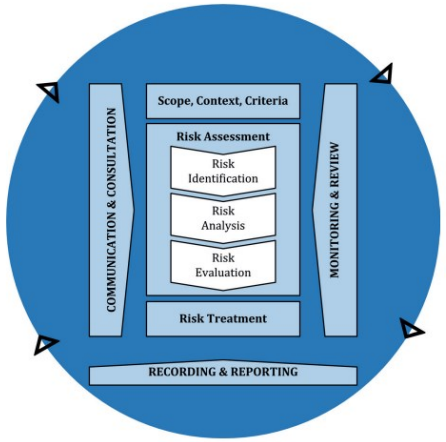
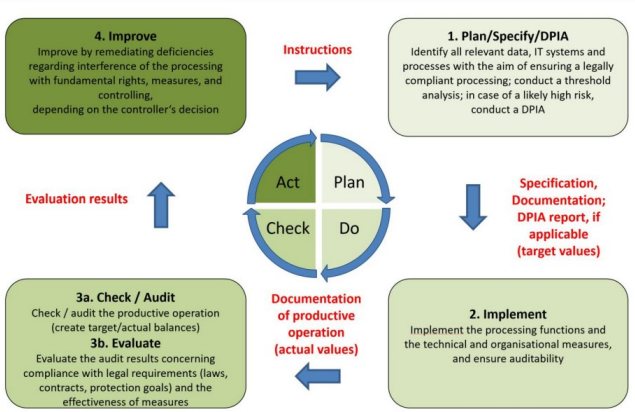
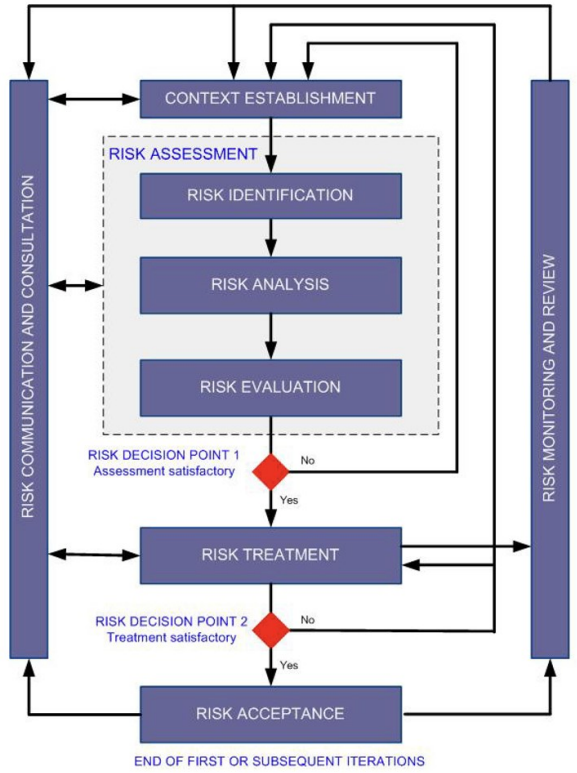


Figure 4 — Process



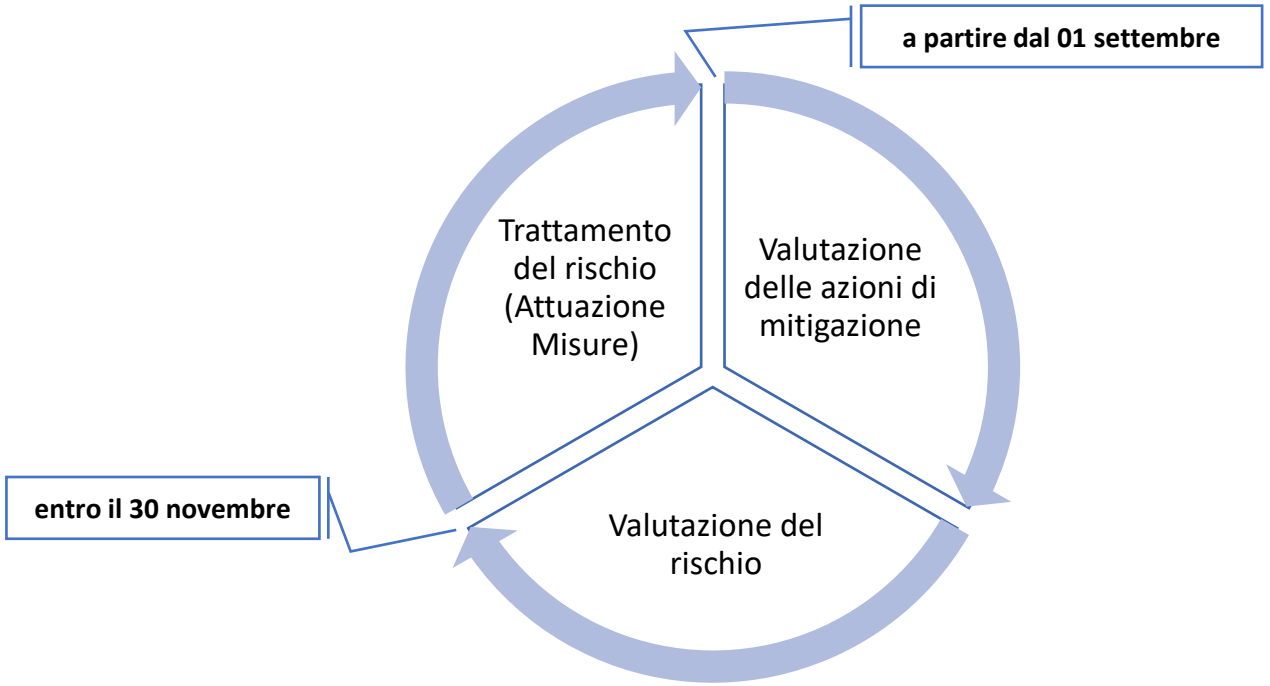
SDM
Standard Data Protection Model

ISO 27005:2011
Information Security Risk Management Process



https://www.enisa.europa.eu/risk-level-tool/risk

Definisci la «tua» procedura ! pianifica tempi e modalità

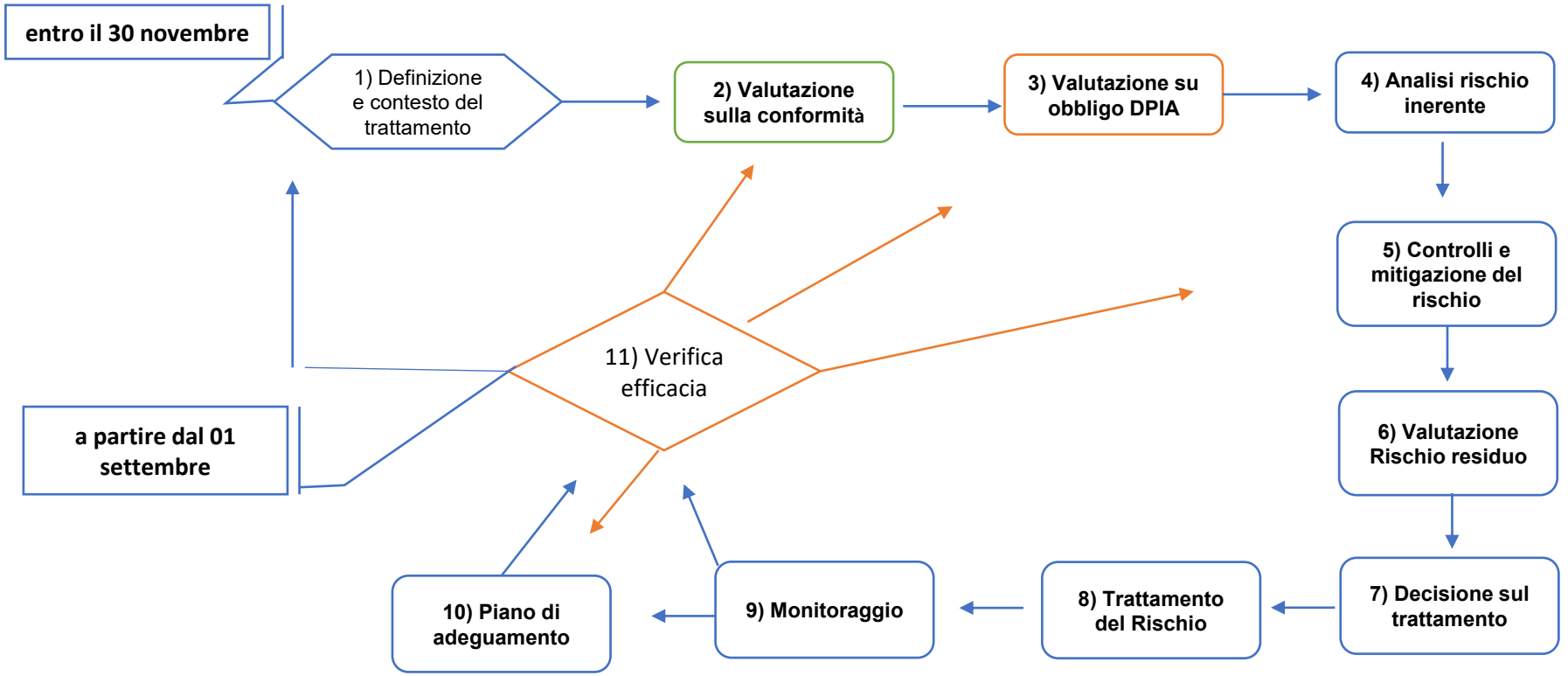


L’importanza del contesto…

Data della Valutazione	Incaricato che effettua la Valutazione	Definizione e contesto delle operazioni di trattamento									
		codice ID tratt.	Denominazione	Finalità	Autorizzati che effettuano il trattamento	Dati trattati	Categorie di interessati	Operazioni eseguite	Destinatari	Mezzi di elaborazione Dispositivi	Elaboratore utilizzato (*Archiviazione interna/esterna; Responsabile*)

…. ed eventuali **altri** indicatori …..

Procedura di gestione dei rischi del trattamento



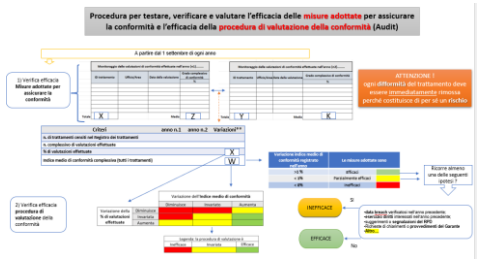
Procedura di gestione dei rischi del trattamento

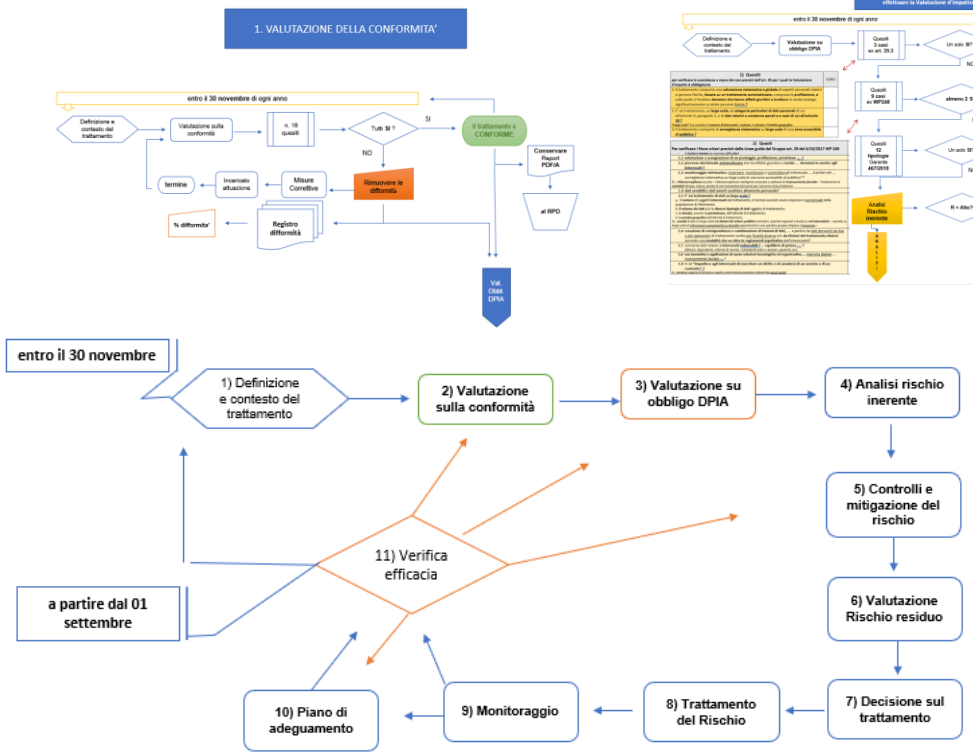
Verifica dell'efficacia della procedura di valutazione circa l'obbligo di effettuare una DPIA

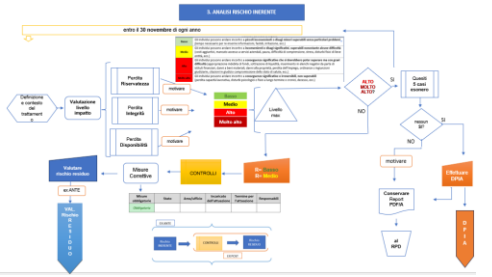
CRITERI PER VALUTARE L'EFFICACIA DELLA PROCEDURA DI VALUTAZIONE CIRCA L'OBBLIGO DI EFFETTUARE LA DPIA	
% dei trattamenti peri quali è stata fatta la Valutazione > o = al 90%	**% dei trattamenti peri quali è stata fatta la Valutazione** < al 90%
Effettuare controlli **a campione** sulle verifiche effettuate	
valutazioni esatte e corrette = 100%	valutazioni esatte e corrette < 100%
LA PROCEDURA E' EFFICACE	**LA PROCEDURA E' INEFFICACE** ➢ **revisionare** e **modificare** la procedura o effettuare altre **azioni di adeguamento**.

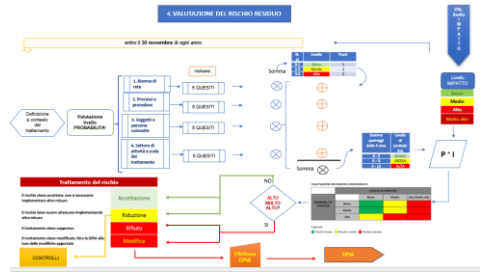
Procedura per testare, verificare e valutare dell'efficacia della procedura di valutazione circa l'obbligo di effettuare una DPIA (Audit)

Procedura per testare, verificare e valutare l'efficacia delle misure adottate per assicurare la conformità e l'efficacia della procedura di valutazione della conformità (Audit)









Validazione del rischio residuale dopo l'applicazione delle misure

ESITO COMPLIANCE TEST:

POSITIVO	NEGATIVO
Non sono state rilevate anomalie o le anomalie rilevate sono giudicate non significative	Le anomalie rilevate dimostrano che le azioni poste a mitigazione non stanno mitigando il rischio
VALIDAZIONE DEL RISCHIO RESIDUO	APERTURA PIANO DI ADEGUAMENTO
	VALUTAZIONE RISCHIO RESIDUO

In caso di esito POSITIVO, si procederà alla VALIDAZIONE del rischio residuo (ex post) redigendo il seguente report:

VALIDAZIONE DEL RISCHIO RESIDUALE					
Descrizione	Frequenza	Tester	Metodologia	Esito	Rischio RESIDUO (EX POST)

In caso di esito NEGATIVO, si procederà a

- attivare un **PIANO DI ADEGUAMENTO** che descriva le criticità rilevate e indichi le azioni da mettere in atto per rimuoverle e i tempi di attuazione in base ad un cronoprogramma
- VALUTARE nuovamente il rischio inerente applicando le misure adeguate a mitigarlo seguendo la procedura descritta al punto 5).

All'esito di tali verifiche **le misure adottate**, oggetto di monitoraggio, **saranno così classificate:**

VALUTAZIONE DEI POST-TEST SULLE MISURE DI MITIGAZIONE	
NON ADEGUATA	non esiste alcuna mitigazione,
PARZIALMENTE ADEGUATA	la misura prevista solo in parte il rischio
PREVALENTEMENTE ADEGUATA	la misura prevista una parte rilevante del rischio
ADEGUATA	la misura prevista integralmente il rischio

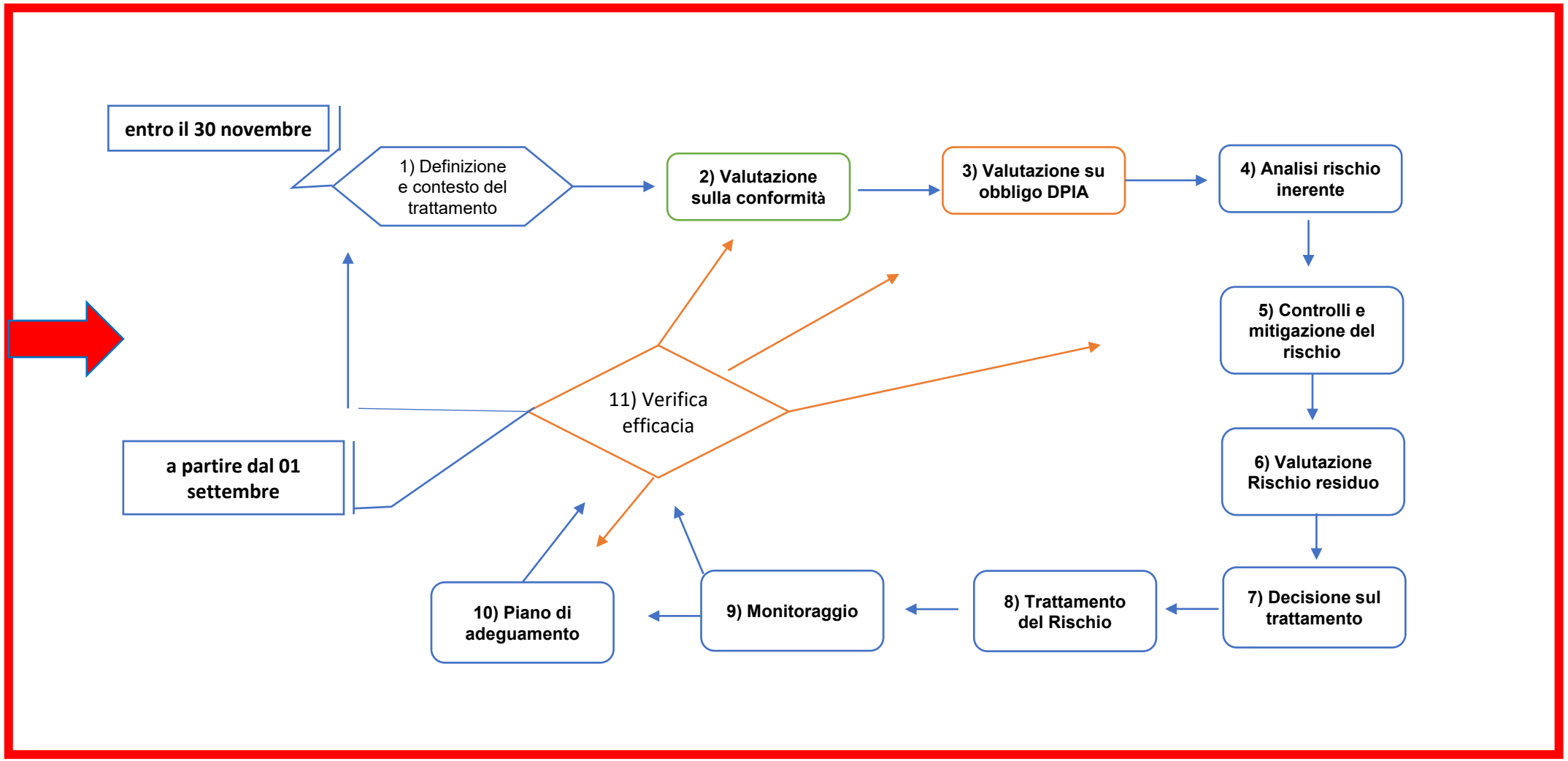
- Per **valutare l'efficacia** occorre necessariamente avere dei **riferimenti numerici**, in termini di obiettivi e di risultati.
- Prevedere lo sviluppo di **almeno tre tipologie di indicatori di rischio** come di seguito indicati:

Progettare la fase di attuazione delle misure...

- Se il **rischio residuo** è **BASSO e MEDIO**: il trattamento può
  - essere ACCETTATO (senza adottare altre misure);
  - essere RIDOTTO (adottando altre misure); **le misure selezionate** da applicare al trattamento dovranno essere **riportate nel dettaglio nella documentazione della valutazione,** compilando la seguente tabella nella quale, per ciascuna misura verranno indicati:
- **l'obbligatorietà** dell' attuazione della misura;
- **lo Stato** in cui si trova la misura:
  - ✓ **Misura già adottata**
  - ✓ **Attuazione in corso**
- **l'Area/Ufficio** che effettua il trattamento
- **congome e nome dell'incaricato dell'attuazione**
- **il termine** entro il quale la misura dovrà essere attuata
- **eventuali Responsabili esterni** coinvolti nell'attuazione delle misure

Misure obbligatorie	Stato	Area/ufficio	Incaricato dell'attuazione	Termine per l'attuazione	Responsabili esterni
Obbligatorie					

Procedura di gestione dei rischi del trattamento



La Misure ENISA

European network and information security Agency

livello Basso

livello Medio

livello Alto

.. ma anche **altre** misure **....**

Id.	Categorie delle misure
A.1	Politica di sicurezza e procedure per la protezione dei dati personali
B.1	Ruoli e responsabilità
C.1	Politica di controllo degli accessi
D.1	Gestione risorse/asset
E.1	Gestione delle modifiche
F.1	Responsabili del trattamento
G.1	Gestione degli incidenti / Personal data breaches
H.1	Continuità operativa
I.1	Obblighi di riservatezza imposti al personale
J.1	Formazione
K.1	Controllo degli accessi e autenticazione
L.1	Generazione di file di log e monitoraggio
M.1	Sicurezza di Server e Database
N.1	Sicurezza delle Postazioni di lavoro
O.1	Sicurezza della rete e delle Infrastrutture di comunicazione elettronica
P.1	Backup
Q.1	Dispositivi mobili / portatili
R.1	Sicurezza del ciclo di vita delle applicazioni
S.1	Cancellazione / eliminazione dei dati
T.1	Sicurezza fisica

Section V – Organizational Security Measures

Si segnala che l'adeguatezza delle misure a specifici livelli di rischio non deve essere percepita come assoluta. A seconda del contesto del trattamento dei dati personali, l'organizzazione può prendere in considerazione l'adozione di misure aggiuntive, anche se attribuite a un livello di rischio più elevato. Inoltre, l'elenco di misure proposto non tiene conto di altri requisiti di sicurezza specifici del settore, nonché di obblighi normativi specifici, derivanti ad esempio dalla direttiva e-privacy o dalla direttiva NIS. Nel tentativo di facilitare ulteriormente questa procedura è inclusa anche una mappatura del gruppo di misure proposto con i controlli di sicurezza ISO/IEC 27001:2013 .

Politica di sicurezza e procedure per la protezione dei dati personali

Identificatore di misura	Descrizione della misura	Livello di rischio
A.1	L'organizzazione dovrebbe documentare la sua politica in merito al trattamento dei dati personali come parte della sua politica di sicurezza delle informazioni.	
A.2	La politica di sicurezza dovrebbe essere rivista e rivista, se necessario, su base annuale.	
A.3	L'organizzazione dovrebbe documentare una politica di sicurezza dedicata separata per quanto riguarda il trattamento dei dati personali. La politica deve essere approvata dalla direzione e comunicata a tutti i dipendenti e alle parti esterne pertinenti	
A.4	La politica di sicurezza dovrebbe riferirsi almeno a: ruoli e responsabilità del personale, misure tecniche e organizzative di riferimento adottate per la sicurezza dei dati personali, responsabili del trattamento o altri soggetti terzi coinvolti nel trattamento dei dati personali.	
A.5	Dovrebbe essere creato e mantenuto un inventario di politiche/procedure specifiche relative alla sicurezza dei dati personali, sulla base della politica di sicurezza generale.	
A.6	La politica di sicurezza dovrebbe essere rivista e rivista, se necessario, su base semestrale.	
	Relativo a ISO 27001:2013 - A.5 Politica di sicurezza	

Ruoli e responsabilità

Identificatore di misura	Descrizione della misura	Livello di rischio
B.1	Ruoli e responsabilità relativi al trattamento dei dati personali dovrebbero essere chiaramente definiti e assegnati in conformità con la politica di sicurezza.	
B.2	In occasione di riorganizzazioni interne o cessazioni e cambi di rapporto di lavoro, dovrebbero essere chiaramente definite le revoche di diritti e responsabilità con le relative procedure di consegna.	
B.3	Dovrebbe essere effettuata una chiara nomina di persone incaricate di specifici compiti di sicurezza, compresa la nomina di un responsabile della sicurezza.	
B.4	Il responsabile della sicurezza dovrebbe essere formalmente nominato (documentato). Anche i compiti e le responsabilità del responsabile della sicurezza dovrebbero essere chiaramente definiti e documentati.	
B.5	Doveri e aree di responsabilità in conflitto, ad esempio i ruoli di responsabile della sicurezza, revisore della sicurezza e DPO, dovrebbero essere considerati separati per ridurre le opportunità di modifica non autorizzata o non intenzionale o uso improprio dei dati personali.	
	Relativo alla ISO 27001:2013 - A.6.1.1 Ruoli e responsabilità della sicurezza delle informazioni	

Politica di controllo degli accessi

Identificatore di misura	Descrizione della misura	Livello di rischio
C.1	A ciascun ruolo (coinvolto nel trattamento dei dati personali) dovrebbero essere assegnati specifici diritti di controllo dell'accesso in base al principio della necessità di conoscere.	
C.2	Una politica di controllo degli accessi dovrebbe essere dettagliata e documentata. L'organizzazione dovrebbe determinare in questo documento le regole di controllo dell'accesso appropriate, i diritti di accesso e le restrizioni per ruoli utente specifici nei confronti dei processi e delle procedure relative ai dati personali.	
C.3	La separazione dei ruoli di controllo dell'accesso (ad es. richiesta di accesso, autorizzazione all'accesso, amministrazione dell'accesso) dovrebbe essere chiaramente definita e documentata.	
C.4	I ruoli con diritti di accesso eccessivi dovrebbero essere chiaramente definiti e assegnati a membri del personale limitati e specifici.	
	Relativo a ISO 27001:2013 - A.9.1.1 Politica di controllo degli accessi	

Gestione delle risorse/risorse

Identificatore di misura	Descrizione della misura	Livello di rischio
D.1	L'organizzazione dovrebbe disporre di un registro delle risorse informatiche utilizzate per il trattamento dei dati personali (hardware, software e rete). Il registro potrebbe includere almeno le seguenti informazioni: risorsa informatica, tipo (ad es. server, workstation), ubicazione (fisica o elettronica). A una persona specifica dovrebbe essere assegnato il compito di mantenere e aggiornare il registro (ad es. responsabile IT).	
D.2	Le risorse IT dovrebbero essere riviste e aggiornate regolarmente.	
D.3	I ruoli che hanno accesso a determinate risorse dovrebbero essere definiti e documentati.	
D.4	Le risorse IT dovrebbero essere riviste e aggiornate su base annuale.	
	Relativo alla ISO 27001:2013 - A.8 Gestione del patrimonio	

Cambio gestione

Identificatore di misura	Descrizione della misura	Livello di rischio
E.1	L'organizzazione dovrebbe assicurarsi che tutte le modifiche al sistema IT siano registrate e monitorate da una persona specifica (ad es. IT o responsabile della sicurezza). Dovrebbe essere effettuato un monitoraggio regolare di questo processo.	
E.2	Lo sviluppo del software deve essere eseguito in un ambiente speciale, non connesso al sistema informatico utilizzato per il trattamento dei dati personali. Quando è necessario eseguire il test, è necessario utilizzare dati fittizi (non dati reali). Nei casi in cui ciò non sia possibile, dovrebbero essere predisposte procedure specifiche per la protezione dei dati personali utilizzati nei test.	
E.3	Dovrebbe essere in atto una politica di cambiamento dettagliata e documentata. Dovrebbe includere: un processo per l'introduzione delle modifiche, i ruoli/utenti che hanno diritti di modifica, le tempistiche per l'introduzione delle modifiche. La politica di modifica dovrebbe essere aggiornata regolarmente.	
	Relativo alla ISO 27001:2013 - A. 12.1 Procedure e responsabilità operative	

Responsabili del trattamento

ENISA

sistema semiquantitativo...

.. ma anche **altre** vulnerabilità ....

Valutazione del livello di probabilità

Rispondere ad ogni domanda con SI / NO
Calcolare il punteggio per ogni Area in base alla seguente tabella e motivare brevemente

N. di risposte affermative	Livello	Punteggio
0-1	Basso	1
2-3	Medio	2
4-5	Alto	3

1. Risorse di rete					
1. Vi sono parti del trattamento svolte attraverso Internet?	2. E' possibile accedere a un Sistema interno di trattamento dati attraverso Internet (per esempio, riguardo a certi utenti o gruppi di utenti)?	3. Il Sistema di trattamento dati personali è interconnesso a un altro Sistema o Servizio IT interno o esterno all'ente?	4. E' facile per soggetti non autorizzati accedere all'ambiente di trattamento dati?	5. Il Sistema di trattamento dati personali è progettato, implementato o manutenuto senza seguire le migliori pratiche del settore?	Punti
				Livello di probabilità	

2. Processi e procedure					
6. Ruoli e procedure relative al trattamento di dati personali sono definiti in modo incerto o insufficiente?	7. L'utilizzo accettabile delle risorse di rete, di Sistema e fisiche all'interno dell'ente è definito in modo incerto o insufficiente?	8. Ai dipendenti è consentito portare con sé e utilizzare i propri dispositivi collegandoli al Sistema di trattamento dati personali?	9. Ai dipendenti è consentito trasferire, memorizzare o comunque trattare dati personali al di fuori del perimetro dell'ente?	10. Le attività di trattamento dati personali possono essere svolte senza che ciò comporti la creazione di file di registrazione eventi (log files)?	Puntl
				Livello di probabilità	

3. Soggetti e persone coinvolte					
11. Il trattamento di dati personali è svolto da un numero indefinito di dipendenti?	12. Vi sono parti del trattamento svolte da un agente o da un soggetto terzo (responsabile del trattamento)?	13. Gli obblighi dei soggetti/delle persone coinvolti nel trattamento di dati personali sono fissati in modo incerto o insufficiente?	14. Il personale che partecipa al trattamento di dati personali non ha conoscenze in materia di sicurezza delle informazioni?	15. I soggetti/le persone che partecipano al trattamento di dati personali omettono di conservare in modo sicuro e/o distruggere i dati personali?	Puntl
				Livello di probabilità	

4. Settore di attività e scala del trattamento					
16. Ritenete che il Vostro settore di attività sia passibile di attacchi cibernetici (cyberattacks)?	17. L'ente ha subito attacchi cibernetici o altre tipologie di violazioni della sicurezza negli ultimi due anni?	18. Sono stati ricevuti notifiche e/o reclami relativamente alla sicurezza dei sistemi IT (utilizzati per il trattamento di dati personali) nell'ultimo anno?	19. Un trattamento riguarda volumi consistenti di dati personali e/o un numero consistente di persone fisiche?	20. Esistono migliori pratiche in materia di sicurezza specifiche del settore di attività dell'ente che non siano state implementate in misura adeguata?	Punti
				Livello di probabilità	

CHI ? Quando ?

Misure obbligatorie	Stato	Area/ufficio	Incaricato dell'attuazione	Termine per l'attuazione	Responsabili esterni
Obbligatoria					

VALUTAZIONE RISCHIO INERENTE	FREQUENZA COMPLIANCE TEST
BASSO	ANNUALE
MEDIO	SEMESTRALE
ALTO	TRIMESTRALE

FREQUENZA dei controlli

- la tempistica di estrazione dell'indicatore è in relazione al livello del rischio.
- Più è alto il **rischio inerente** maggiore sarà la frequenza con cui si dovrà verificare che sia andato tutto bene, secondo la seguente tempistica:

COME ?

- Per **valutare l'efficacia** occorre necessariamente avere dei **riferimenti numerici**, in termini di obiettivi e di risultati.
- Prevedere lo sviluppo di **almeno tre tipologie di indicatori di rischio** come di seguito indicati:

INDICATORI DI RISCHIO	
indicatori di esposizione al rischio:	**n. di minacce** che insidiano il trattamento **n. di eventi formativi non effettuati o non effettuati nelle scadenze programmate** **n. di elementi del piano di miglioramento non effettuati** nei tempi programmati
indicatori di anomalia:	**n. di reclami ricevuti**; **n. di incidenti di sicurezza (data breach)** **n. di incidenti della sicurezza (anche se non c'è stato data breach)** es.: n. di incidenti a seguito di virus o malware; eventi riscontrati di mancato rispetto delle policy e procedure per la sicurezza; n. di **data breach non registrati nel registro** delle violazioni **n. di reclami o lamentele degli interessati** **n. di riscontri agli interessati inevasi o non evasi** nei termini di legge **n. di violazioni del tempo massimo** di conservazione dei dati **n. di non conformità riscontrate negli audit e non risolte** nei tempi programmati n. di **violazioni sugli obblighi di informativa** n. di **nuovi trattamenti non registrati sul registro** o comunque prima di effettuare il trattamento
indicatori di perdita:	**n. di provvedimenti sanzionatori**

FORMALIZZAZIONE

Scheda compliance test			
Rif. Test			
Data del test			
Periodo di riferimento			
Obiettivo del test			
INDICATORI DI RISCHIO UTILIZZATI			
Indicatori di esposizione al rischio	Indicatori di esposizione anomalia		Indicatori di perdita
Frequenza (periodicità)			
Popolazione	descrizione		
	#elementi		
Campione	Tecnica		
	Criterio di selezione		
Metodologia			
Tester: Cognome, nome e ruolo/ufficio di appartenenza			
ESITO			

Adozione di un Piano di adeguamento correttivo

In caso di esito negativo del compliance test, occorre procedere alla definizione di un piano di azione correttivo al fine di:

- sanare le anomalie e criticità riscontrate,
- definire e attuare nuove azioni di mitigazione.

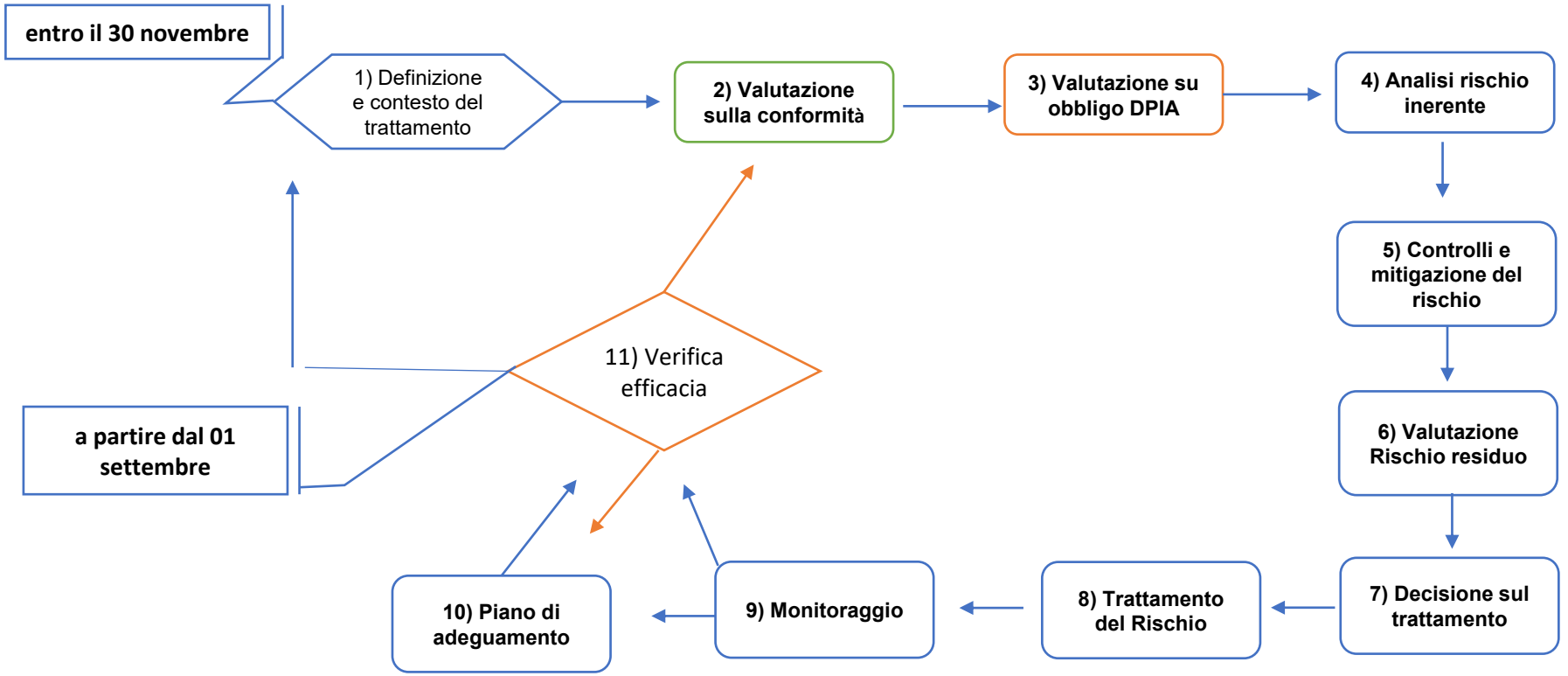
Il **Piano di adeguamento** sarà costituito almeno dai seguenti **elementi**:

- ✓ **Tipologia** di anomalia/criticità riscontrata (inadeguatezza del controllo, superamento del limite accettabile)
- ✓ **Descrizione** dell'anomalia/criticità
- ✓ **Azione** proposta
- ✓ **Data** definita per la realizzazione dell'azione proposta
- ✓ Definizione delle **priorità** di intervento secondo un **CRONOPROGRAMMA**
- ✓ **Incaricato** della **realizzazione**
- ✓ **Incaricato** della **verifica dell'attuazione dell'azione**

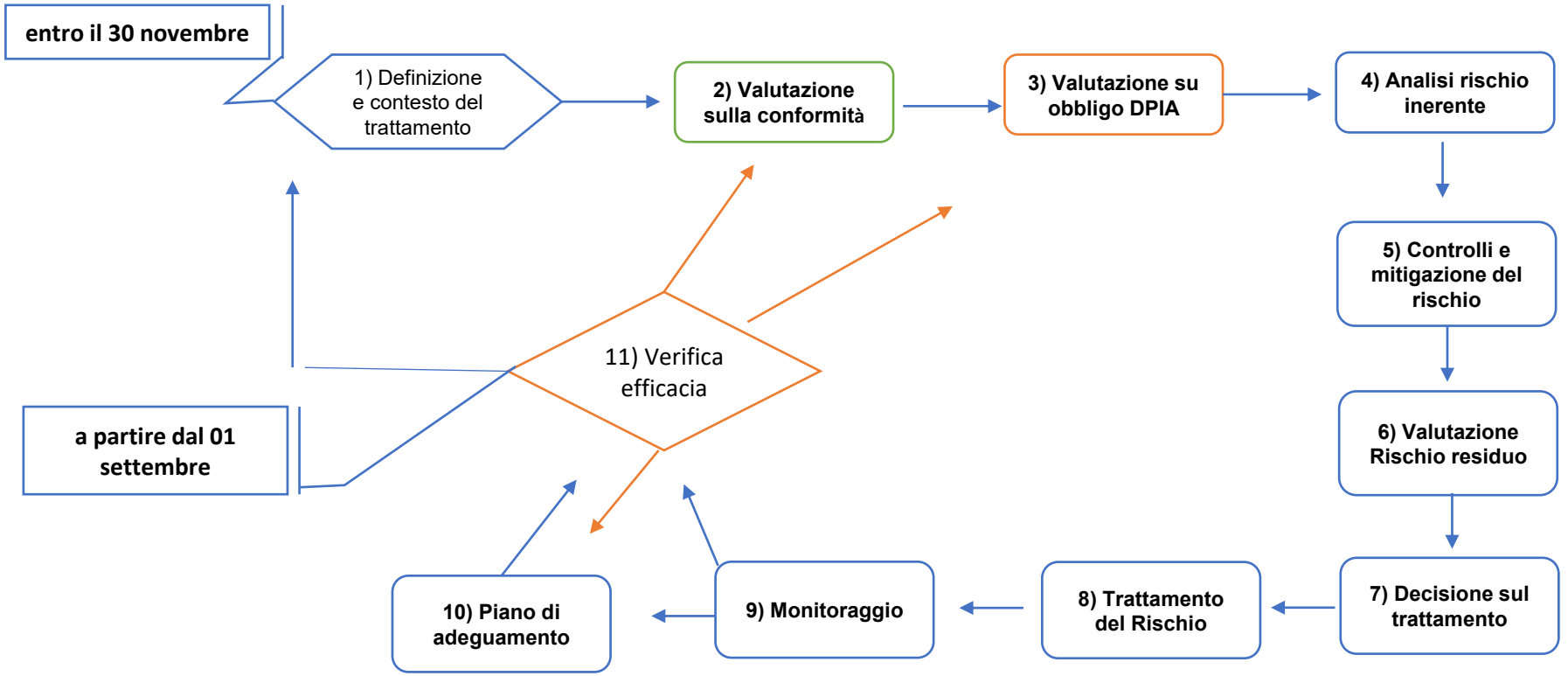
PROCEDURA PER TESTARE, VERIFICARE E VALUTARE L'EFFICACIA DELLE MISURE ADOTTATE...

... E L'EFFICACIA DELLA PROCEDURA STESSA (AUDIT)

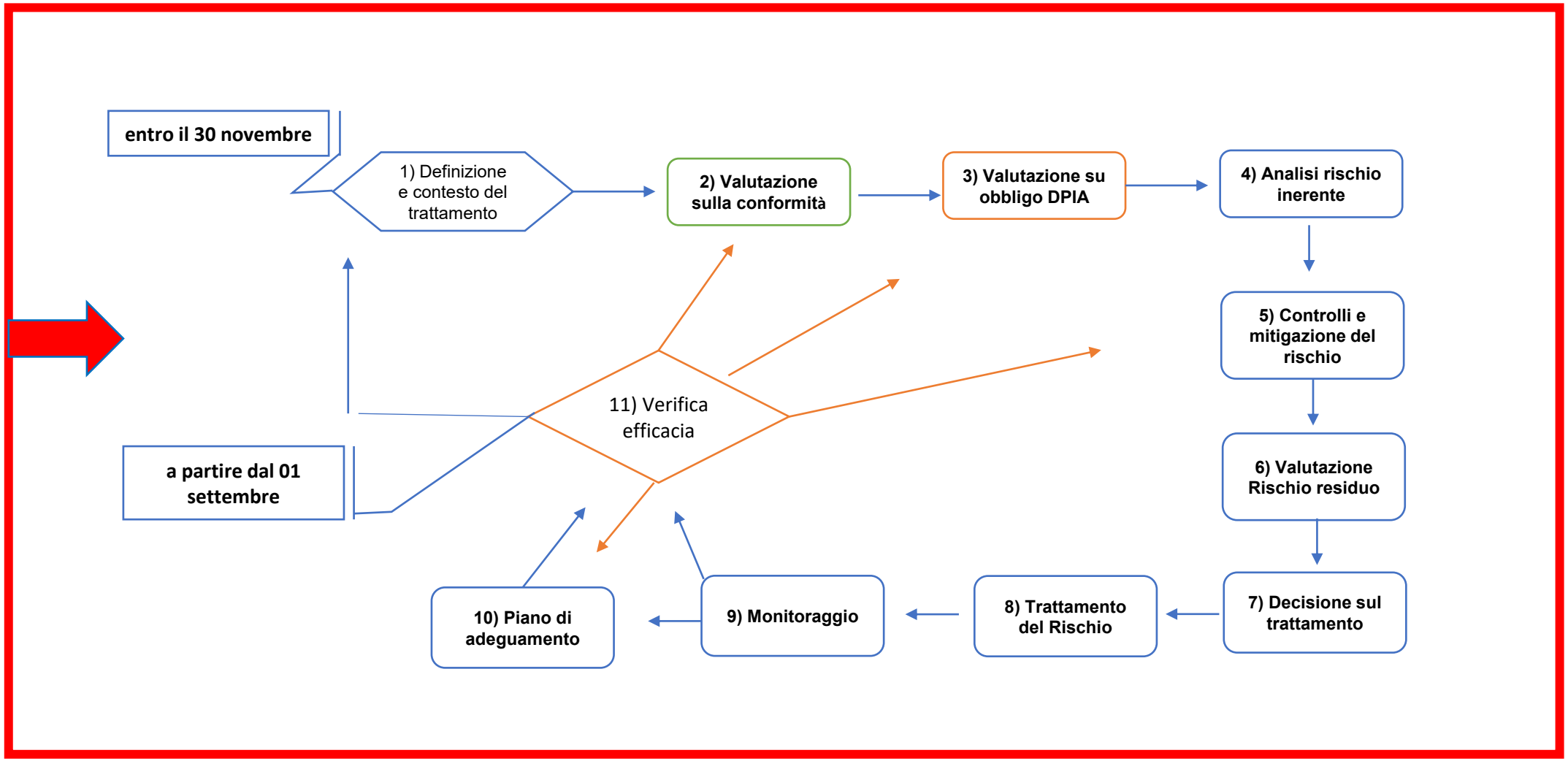
Procedura di gestione dei rischi del trattamento



Procedura di gestione dei rischi del trattamento



Procedura di gestione dei rischi del trattamento



COSA DICE IL GARANTE…

- Provvedimento del Garante in tema di fatturazione elettronica – 20 dicembre 2018 [9069072]

…

..*evitare schemi standard e semplificazioni che rischiano di comprometterne l'efficacia…*

5. La valutazione di impatto sulla protezione dei dati

L'Agenzia delle entrate, con la nota del 17 dicembre u.s., ha trasmesso all'Autorità la valutazione d'impatto relativa al trattamento dei dati relativi al processo di fatturazione elettronica tra privati (B2B e B2C).

Al riguardo, si rappresenta che la valutazione d'impatto sulla protezione dei dati deve in primo luogo tenere conto dei rischi incombenti sui diritti e sulle libertà degli interessati, esaminando, in modo esaustivo, i diversi scenari di rischio e i possibili impatti al fine di individuare misure adeguate ad affrontarli, annullandoli o, quantomeno, riducendoli a un livello accettabile.

La valutazione di impatto effettuata dall'Agenzia risulta, invece, focalizzata su aspetti meramente tecnici del trattamento, risultando prevalentemente, se non esclusivamente, un documento di valutazione del rischio informatico incombente sui dati. Pertanto, tale valutazione appare carente nella parte analitica riferita agli impatti sui diritti e sulle libertà degli interessati derivanti dai diversi scenari di rischio considerati, anche laddove non siano riferibili alla fattispecie degli incidenti informatici.

Pur considerando la recente introduzione di tale adempimento nel nostro ordinamento, la complessità e la portata della fatturazione elettronica, che coinvolge l'intera popolazione, richiedono che la valutazione di impatto sia realizzata evitando di sfruttare schemi standard e semplificazioni che rischiano di comprometterne l'efficacia, fornendo alla stessa un connotato di eccessiva genericità e, quindi, di inadeguatezza, soprattutto in relazione all'analisi dei rischi che ne costituisce il presupposto essenziale.

Inoltre, non risulta che, come previsto dall'art. 35, § 9, del Regolamento, l'Agenzia abbia raccolto, attraverso le modalità ritenute più opportune, e tenuto in considerazione nell'ambito della valutazione di impatto, le opinioni dei soggetti interessati o dei loro rappresentanti, quali le associazioni di categoria o di consumatori. Anche quando avesse ritenuto non appropriato procedere in tal senso, avrebbe dovuto quantomeno documentare, all'interno del documento, i motivi della mancata raccolta delle opinioni degli interessati.

Ciò posto, si ritiene, quindi, necessario ingiungere all'Agenzia delle entrate di comunicare al Garante, entro il 15 aprile 2019, una nuova versione della valutazione di impatto, riesaminando gli elevati rischi connessi al processo di fatturazione elettronica, anche alla luce di quanto emergerà nei primi mesi di operatività del nuovo obbligo.

COSA DICE IL GARANTE…

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Inserire il testo o il doc web | CERCA

I miei diritti | Imprese ed enti

L'Autorità | Temi | Normativa e provvedimenti | News e comunicazione | Amministrazione trasparente

Home / Provvedimenti / Ordinanza ingiunzione o revoca
/ Ordinanza ingiunzione nei confronti di Università Commerciale "Luigi Bocconi" di Milano - 16 settembre 2021 [9703988]

Ordinanza ingiunzione nei confronti di Università Commerciale "Luigi Bocconi" di Milano - 16 settembre 2021 [9703988]

Ascolta | Stampa | PDF | Condividi

[doc. web n. 9703988]

Ordinanza ingiunzione nei confronti di Università Commerciale "Luigi Bocconi" di Milano - 16 settembre 2021

Registro dei provvedimenti
n. 317 del 16 settembre 2021

Scheda

Doc-Web
9703988

Data
16/09/21

Argomenti

Biometria
Trasferimento dati all'estero
Università
Profilazione

Tipologie

positivi/negativi. Peraltro, al par. 7 della valutazione d'impatto, il rischio relativo alla discriminazione è stato valutato come "poco probabile", con potenziale danno "medio", in quanto "non si potrebbe determinare discriminazione alcuna", senza, tuttavia, una previa valutazione sull'affidabilità degli algoritmi utilizzati dal sistema di supervisione. Vengono, peraltro, indicate misure inconferenti per la mitigazione del rischio di discriminazione ("il sistema è costruito in modo da non permettere la conservazione del dato biometrico. Protezione da intrusioni tramite firewall, assenza di esposizione sulla rete e crittografia sul traffico di transito").

#Errori_da_non_fare

- **Non rispettare la metodologia** approvata dall'organizzazione
- mancanza di flessibilità: essere rigidamente vincolati alla struttura della procedura perdendo il **contatto con la realtà operativa** concreta.....
- **trascurare minacce latenti**, non rilevate … ➔ mancata «***percezione*** *del rischio*»….
- **enfatizzare minacce** che nell'applicazione concreta potrebbero risultare **ininfluenti** perché non applicabili al trattamento
- prevedere **misure generiche** che non sono attinenti alle minacce individuate e al contesto
- **trascurare il monitoraggio** dell'effettivo stato di implementazione delle misure programmate
- affidare **l'audit alle stesse persone che effettuano il trattamento**
- utilizzare **criteri di valutazione soggettivi**, **autoreferenziali, non replicabili** e **non verificabili**
- **trascurare di documentare** attraverso strumenti formali che permettano di motivare i passaggi seguiti
- trascurare le situazioni di **non conformità** che di per sé costituiscono un rischio

Chi coinvolgere ?

- Il DPO ? ➔ Si, ... ma non solo
- un TEAM di **designati** ex art. 2-quaterdecies D.Lgs. 2003/196 ? ➔ ... ma non solo ....

.... ogni persona autorizzata al trattamento deve fare la sua parte ....

ATTENZIONE al fattore umano !

- vulnerabilità ....
- Misura di sicurezza ➔ Formazione

Gli incentivi ….

aran
AGENZIA PER LA RAPPRESENTANZA NEGOZIALE DELLE PUBBLICHE AMMINISTRAZIONI

CONTRATTO COLLETTIVO NAZIONALE DI LAVORO

RELATIVO AL PERSONALE DEL COMPARTO FUNZIONI LOCALI

TRIENNIO 2019 - 2021

Il giorno **16 novembre 2022** ha avuto luogo, presso la sede dell'Aran, l'incontro tra l'A.Ra.N e le Organizzazioni e Confederazioni sindacali rappresentative del Comparto Funzioni Locali.

Al termine della riunione, alle ore 11,30, le parti sottoscrivono l'allegato Contratto Collettivo Nazionale di Lavoro relativo al Personale del Comparto Funzioni Locali Triennio 2019/2021.

Per l'A.Ra.N. Presidente **Cons. Antonio Naddeo** Firmato

…occhio all'art. 84 …..

Art. 84
Indennità per specifiche responsabilità

1. Per compensare l'esercizio di un ruolo che, in base all'organizzazione degli enti, comporta l'espletamento di compiti di specifiche responsabilità, attribuite con atto formale, in capo al personale delle aree Operatori, Operatori Esperti, Istruttori e Funzionari ed EQ, che non risulti titolare di incarico di EQ, ai sensi dell'art. 16 del presente CCNL e seguenti, può essere riconosciuta, secondo i criteri generali di cui all'art. 7 comma 4 lett. f) (Contrattazione integrativa), una indennità di importo non superiore a € 3.000 annui lordi, erogabili anche mensilmente, elevabili fino ad un massimo di € 4.000 per il personale inquadrato nell'Area dei Funzionari ed EQ, con relativi oneri a carico del Fondo Risorse decentrate di cui all'art. 79 (Fondo risorse decentrate: costituzione). A titolo esemplificativo e non esaustivo:

- specifiche responsabilità derivanti dall'esercizio di compiti legati ai processi digitalizzazione ed innovazione tecnologica della PA di cui al Codice dell'amministrazione in digitale (D.Lgs 7 marzo 2005, n. 82, e s.m.i - CAD); es: progettazione, realizzazione e lo sviluppo di servizi digitali e sistemi informatici; tenuta del protocollo informatico, gestione dei flussi documentali e degli archivi;

- specifiche responsabilità derivanti dall'esercizio di compiti legati all'attuazione del Regolamento Generale sulla Protezione dei Dati - GDPR (Regolamento Europeo 2016/679);

Grazie per attenzione!

Avv. Salvatore Maugeri

+39 3386209125

avvocato.maugeri.salvatore@gmail.com

Socio Csig Ivrea Torino www.csigivreatorino.it

per approfondimenti: avvocato.maugeri.salvatore@gmail.com

LinkedIn: Salvatore Maugeri
https://www.linkedin.com/feed/