

La conformità regolamentare delle aziende come insieme di sistemi complessi: il ruolo innovativo dello strumento "AI for GDPR Compliance"

Regulatory compliance for companies as a set of complex systems and innovative role of the "AI for GDPR Compliance" tool

Domenico Giovinazzo



International Institute for Global Analyses

Vision & Global Trends. International Institute for Global Analyses
Piazza dei Navigatori 22, 00147 – Rome (Italy)

The views and opinions expressed in this publication are those of the authors and do not represent the views of the Vision & Global Trends. International Institute for Global Analyses unless explicitly stated otherwise.

© 2026 Vision & Global Trends - International Institute for Global Analyses
© 2026 Domenico Giovinazzo

First Edition: May 2026

Analytical Dossier 13/2026 - ISSN 2704-6419

www.vision-gt.eu
info@vision-gt.eu

La conformità regolamentare delle aziende come insieme di sistemi complessi: il ruolo innovativo dello strumento "AI for GDPR Compliance"

Regulatory compliance for companies as a set of complex systems and innovative role of the "AI for GDPR Compliance" tool

Domenico Giovinazzo



Vision & Global Trends – International Institute for Global Analyses

La conformità regolamentare delle aziende come insieme di sistemi complessi: il ruolo innovativo dello strumento “AI for GDPR Compliance”

Domenico Giovinazzo

ABSTRACT - Al giorno d'oggi per ogni azienda è fondamentale avere una *policy privacy* ben definita e conforme al GDPR. Ciò, tuttavia, non è sempre possibile a causa, sostanzialmente, di due fattori: l'assenza di processi dimostrabili e l'ambiguità delle misure tecniche applicate. Lo strumento “AI for GDPR Compliance” si propone di superare queste barriere fornendo - tramite un input descrittivo dei processi aziendali - un framework dettagliato, operativo e funzionale contenente tutta una serie di rischi e irregolarità rilevate. Il framework, inoltre, mostra le varie soluzioni tecniche per rendere le strategie applicative aziendali più semplici. Va sottolineato, altresì, che il sistema non si propone di sostituire le figure professionali coinvolte nel processo, ma soltanto di fornire loro un quadro più ordinato e chiaro su cui poter lavorare.

KEYWORDS: GDPR compliance; privacy governance; artificial intelligence; framework; risk assessment; accountability; ISO/IEC 27001.

INTRODUZIONE

1.1. Il problema delle varie aziende non è solo quello di interpretare la norma, ma anche (e soprattutto) quello di “mettere insieme i pezzi”. Cioè, collegare *policy*, controlli tecnici, ruoli interni e documentazione.

Il risultato attuale è una diffusa *policy privacy* aziendale poco chiara con una conformità non dimostrabile e, quindi, potenzialmente suscettibile di sanzioni.

A ciò si aggiunga anche la circostanza che usualmente i processi aziendali vengono suddivisi tra varie aree (IT, legal, HR e management) con la conseguenza che manca una visione unitaria del settore. Ciò in materia di *privacy* e trattamento dei dati è profondamente deleterio e potenzialmente dannoso in termini sia di individuazione dell'eventuale problema sia di ordine corretto di intervento.

Il vero problema non è l'assenza di regole, ma la difficoltà di trasformarle in interventi coerenti, correttamente ordinati e sostenibili nel tempo.

1.2. Per risolvere questa situazione presente in molte aziende serve un approccio che trasformi la *compliance* da adempimento formale a strumento di *governance*, con delle istruzioni ben precise e divise per ruoli, al fine di armonizzare il processo e di evitare che la *policy privacy* sia poco chiara e difficilmente dimostrabile.

METODO

2.1. Il metodo di cui qui si tratta è suddiviso in quattro fasi. La prima è costituita da un *input* aziendale strutturato, grazie al quale emergerà un profilo aziendale completo; nello specifico, processi, ruoli, fornitori, misure dichiarate e documentazione disponibile.

Successivamente, si procederà confrontando siffatte informazioni con la normativa in materia di *privacy* (GDPR).

Il risultato sarà un report dettagliato, strutturato come un *framework* poichè individua divari, aree poco presidiate e punti critici.

Sarà il medesimo report, poi, che, una volta ordinate le criticità sulla base della loro rilevanza operativa e regolatoria, produrrà una serie di restituzioni (cd. *outputs*) diversi, ma coerenti con quadro di rischio, criticità, azioni correttive e conseguente mappa di esse.

2.2. L'intero processo consentirà di fornire all'azienda un *framework* operativo cd. "multilivello":

a) il primo livello di *output* restituirà una fotografia sintetica dello stato di conformità: rischio complessivo, importanza dei divari e aree che richiedono attenzione immediata. Questo consentirà di capire rapidamente se il tema da affrontare è di semplice consolidamento oppure di intervento urgente;

b) il secondo livello entrerà nel merito delle lacune individuate, interpretandole. Non si limiterà a elencare ciò che manca, ma metterà in evidenza perché quel punto è rilevante, quali funzioni coinvolge e quale effetto potrà avere sulla capacità dell'organizzazione di dimostrare conformità;

c) il terzo livello tradurrà i risultati in azioni: cosa fare subito, cosa consolidare nel breve termine e quali presidi vanno mantenuti nel tempo. In questo passaggio il report smetterà di essere solo informativo e diventerà uno strumento di coordinamento tra management, DPO, area legale e IT.

2.3. Il sistema, inoltre, attribuisce al *framework* una funzione ulteriore, poichè esso accompagna l'azienda verso una più ordinata strutturazione dei controlli necessari per la sicurezza delle informazioni. Anche sotto tale profilo, il processo consentirà di fornire all'azienda un ulteriore livello di utilità operativa:

(i) in primo luogo, permetterà di individuare i principali presidi organizzativi e tecnici che richiedono attenzione, quali *incident response*, controllo degli accessi, cifratura, *logging*, gestione dei fornitori, formazione periodica e attribuzione delle responsabilità;

(ii) in secondo luogo, consentirà di ordinare tali presidi secondo una logica di priorità, così da evidenziare non solo ciò che manca, ma anche ciò che deve essere affrontato prima per rafforzare in modo più efficace l'assetto organizzativo aziendale;

(iii) in terzo luogo, renderà tali elementi maggiormente verificabili, poiché li collegherà a responsabilità, tempi di attuazione ed evidenze, trasformandoli da misure semplicemente dichiarate in controlli più stabili e dimostrabili;

(iv) infine, proprio perché tali presidi risultano rilevanti non solo sotto il profilo *privacy*, ma anche sotto quello della sicurezza delle informazioni, il *framework* potrà costituire per l'azienda una base organizzativa e tecnica utile per intraprendere un percorso credibile verso la certificazione ISO/IEC 27001.

RISULTATO

Il suddetto metodo è stato testato su una azienda non reale (cd. Alfa Retail s.r.l.) restituendo il seguente report:

"Sintesi per il management:

L'analisi di conformità GDPR per Alfa Retail s.r.l. ha identificato 12 criticità e generato 12 azioni correttive raccomandate. Il livello di rischio complessivo è CRITICO (score: 8.2/10). Sono state rilevate 7 criticità ad alta priorità che richiedono intervento immediato. Questo report è generato a fini consultivi e richiede validazione da parte di DPO, area legale e management aziendale prima dell'implementazione.

Criticità rilevate:

- Manca un piano di risposta agli incidenti formalizzato*
- MFA non attivata per accessi critici/amministrativi e accessi remoti*
- Cifratura at-rest non esplicitamente documentata per dati personali (database, backup, storage)*
- Gestione fornitori incompleta: DPA/accordi ex art. 28 non verificati per tutti i vendor. Vendor senza DPA: Email Marketing Platform, IT Managed Service*
- Non risulta effettuata una DPIA (Data Protection Impact Assessment) per trattamenti potenzialmente ad alto rischio*
- Il registro dei trattamenti (art. 30 GDPR) non risulta documentato o aggiornato*
- Non risultano procedure formalizzate per la gestione dei diritti degli interessati (accesso, rettifica, cancellazione, portabilità, opposizione)*
- Programma di formazione e sensibilizzazione privacy/GDPR non esplicitamente documentato*

- *Controllo accessi basato su ruoli (RBAC) e principio del minimo privilegio non documentati*
- *Monitoraggio centralizzato dei log e sistemi di rilevazione anomalie non documentati*
- *Trattamenti basati su consenso presenti ma manca un sistema strutturato di gestione consensi (raccolta, revoca, tracciamento)*
- *Tecniche di pseudonimizzazione/anonimizzazione non esplicitamente adottate per i dati personali*

Piano d'azione

Qui riportiamo solo alcune delle azioni consigliate:

1) Definire e approvare un Incident Response Plan con ruoli, escalation, tempi di notifica e canali di comunicazione.

- *Riferimenti GDPR: art. 32 GDPR, art. 33 GDPR, art. 34 GDPR*
- *Evidenze/documenti da predisporre:*
- *Policy incident response approvata*
- *Runbook operativo*
- *Registro test/esercitazioni*
- *Matrice escalation*

2) Abilitare MFA per tutti gli account privilegiati, accessi remoti (VPN, RDP) e pannelli di amministrazione.

- *Riferimenti GDPR: art. 32(1)(b) GDPR*
- *Evidenze/documenti da predisporre:*
- *Configurazione IAM/IdP*
- *Policy accessi con requisito MFA*
- *Report compliance MFA*
- *Elenco account esclusi con giustificazione*

3) Creare e mantenere aggiornato il registro dei trattamenti ex art. 30 GDPR, includendo basi giuridiche, finalità, categorie di dati e destinatari.

- *Riferimenti GDPR: art. 30 GDPR*
- *Evidenze/documenti da predisporre:*
- *Registro trattamenti compilato*
- *Data ultimo aggiornamento*
- *Responsabili per processo*
- *Mappatura flussi dati*

Altre parti utili del report:

Roadmap

1) Fase Immediata (0-15 gg): Risoluzione criticità alte

- 2) Fase Consolidamento (15-60 gg): Aggiornamento documentale e training
 3) Fase Monitoraggio (60+ gg): Audit periodico e controllo fornitori

Conseguenze se non si interviene:

Aumento significativo del rischio di violazioni, data breach, contestazioni da parte degli interessati e potenziali sanzioni amministrative fino al 4% del fatturato annuo globale (art. 83 GDPR)

Chi deve intervenire:

- Rilevazione e logging (SIEM) → CISO / IT Security Manager (entro 60 giorni)- Controlli di accesso (IAM / PAM) → IT Manager / CISO (entro 45 giorni)- Backup, resilienza e Disaster Recovery → IT Operations Manager / CISO (entro 60 giorni)- Cifratura e gestione chiavi crittografiche → IT Security / CISO (entro 90 giorni)
- Incident Response e Breach Notification → CISO / DPO (entro 30 giorni)
- Vendor Management e conformità art. 28 GDPR → DPO / Procurement / Legal (entro 60 giorni)".

DISCUSSIONE

4.1. Il sistema è una innovazione concreta rispetto agli altri servizi presenti sul mercato poichè migliora il dialogo tra figure diverse creando un linguaggio comune tra chi valuta il rischio e chi deve decidere investimenti e tempi. Ciò fornisce una gestione armonica di processi ed eventuali decisioni da prendere.

Un altro aspetto da considerare è la *compliance* che diventa più concreta perchè il sistema la collega a responsabilità, tempi e azioni.

Infine, aiuta a vedere la conformità non come un documento statico, ma come processo organizzativo da governare.

"L'innovazione del progetto è organizzativa, oltre che tecnologica, perché rende la conformità una base per decidere e non solo un insieme di obblighi da descrivere".

4.2. Tutto il processo è caratterizzato da un approccio dove l'AI è usata come strumento di supporto. Infatti: a) non vi è alcuna autonomia decisionale per essa; b) è essenziale e necessaria la costante supervisione e la finale validazione di un professionista, nel rispetto di quanto previsto dall' AI Act; c) non vi è alcun processo automatizzato senza il permesso di un professionista.

In questa prospettiva, il progetto non si esaurisce nel supporto alla *compliance* GDPR, ma si colloca in un orizzonte più ampio, in cui la lettura dei divari e la loro traduzione in priorità, responsabilità ed evidenze diventano anche il presupposto per accompagnare l'azienda verso la certificazione ISO/IEC 27001. Il valore del *framework*, quindi, risiede anche nella sua capacità di collegare dimensione normativa, controlli tecnici, organizzazione interna e governo degli interventi in un unico percorso coerente di maturazione aziendale.

Va sottolineato, infine, che il sistema non è stato pensato per sostituire il professionista coinvolto normalmente in questi processi, ma semmai per semplificarli il lavoro fornendo un supporto che possa aiutarlo concretamente lungo la catena dei processi di cui è composta la *compliance privacy*.

CONCLUSIONE

Il progetto proposto mostra come la conformità al GDPR possa essere affrontata in modo più operativo superando una visione puramente tecnologica o meramente formale e/o documentale dell'adeguamento normativo. Uno dei principali limiti che molte organizzazioni incontrano non riguarda, infatti, soltanto la comprensione delle regole, ma la capacità di tradurle poi in azioni concrete, priorità chiare e responsabilità definite.

In questo contesto, il contributo del *framework* consiste proprio nel ridurre la distanza tra analisi documentale e intervento operativo, offrendo un supporto utile per trasformare informazioni disperse, controlli dichiarati e criticità rilevate in un percorso strutturato di miglioramento.

Il valore veramente innovativo del progetto non risiede, quindi, nella produzione di un report (così come è per tutti i servizi simili attualmente presenti sul mercato), ma nella capacità di convertire i divari di conformità in un processo di governo degli interventi. Ciò consente di rendere la *compliance* più leggibile per chi deve valutarla, più verificabile per chi deve dimostrarla e più governabile per chi deve prendere decisioni. Attraverso la definizione di priorità, l'associazione delle responsabilità e la costruzione di una mappa di rimedi, il *framework* consente all'azienda di affrontare la conformità non come un insieme statico di obblighi, ma come una attività continua di organizzazione, controllo e miglioramento.

In questa prospettiva, il progetto assume un valore che va oltre il solo ambito tecnico, poiché rafforza il collegamento tra dimensione normativa, processi interni e capacità decisionale, migliorando concretamente la costruzione di un processo unitario e fluido di *governance*, reale sfida e aspirazione per ogni azienda, grande o piccola che sia.

La conformità viene così interpretata non soltanto come obiettivo da raggiungere, ma come elemento di *governance* utile a orientare scelte, investimenti e responsabilità all'interno dell'organizzazione.

Tale approccio ovviamente risulta particolarmente rilevante in contesti aziendali grandi in cui la frammentazione delle informazioni, la complessità dei ruoli e la difficoltà nel definire le priorità rendono più difficile un adeguamento realmente efficace. Tuttavia, risulta altrettanto importante per le medie e piccole imprese poiché è noto come la conformità normativa e regolamentare sia la base per costruire una crescita aziendale veramente duratura.

Gli sviluppi futuri potranno ampliare ulteriormente il valore del progetto, sia attraverso l'applicazione del *framework* a settori differenti, sia mediante l'analisi di un numero maggiore di casi studio, utili a consolidarne la validità e l'adattabilità.

Ulteriori direzioni di evoluzione potranno, inoltre, riguardare il rafforzamento della tracciabilità delle decisioni, la maggiore strutturazione delle evidenze di conformità e il potenziamento del supporto decisionale, così da rendere il sistema ancora più efficace nel collegare valutazione del rischio, priorità operative e governo aziendale.

BIBLIOGRAFIA

1. Carta dei Diritti Fondamentali dell'Unione Europea (CDFUE; 2000)
2. Regolamento UE n. 679/2016 (GDPR)
3. Regolamento UE n. 1689/2024 (AI Act)
4. Comitato europeo per la protezione dei dati (EDPB), *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a right risk" for the purposes of Regulation 2016/679 (WP248 rev.01)*, adottate il 4 aprile 2017
5. Comitato europeo per la protezione dei dati (EDPB), *Guidelines 05/2020 on consent under Regulation 2016/679*, vers. 1.1, adottate il 4 maggio 2020
6. Comitato Europeo per la Protezione dei Dati (EDPB), *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, vers. 2.0, adottate il 20 ottobre 2020
7. Comitato Europeo per la Protezione dei Dati (EDPB), *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, vers. 2.1, adottate il 7 luglio 2021
8. Comitato europeo per la protezione dei dati (EDPB), *Guidelines 9/2022 on personal data breach notification under GDPR*, vers. 2, adottate il 4 aprile 2023
9. Comitato europeo per la protezione dei dati (EDPB), *Guidelines 01/2022 on data subject rights – Right of access*, vers. 2.1, adottate il 17 aprile 2023

* * *

Domenico Giovinazzo studia attualmente presso la Fondazione M.A.SK. ITS Academy di San Ferdinando (RC), dove frequenta il corso di Tecnico Superiore in Governance e Compliance. Tecnico Informatico di formazione, ha sviluppato competenze di base in programmazione e sistemi di rete, orientando progressivamente il proprio interesse verso il tema della privacy e del trattamento dei dati. È particolarmente incuriosito da ciò che può nascere integrando alta tecnologia e profili regolamentari in una prospettiva operativa di supporto alla governance aziendale.



Vision & Global Trends - International Institute for Global Analyses

www.vision-gt.eu

info@vision-gt.eu