TRATTAMENTI EFFETTUATI IN OUTSOURCING: COME MANTENERE IL CONTROLLO DEL PERIMETRO DEI DATI IN CONFORMITÀ AL GDPR?

Navigare la Convergenza Normativa tra GDPR, NIS2, DGA e Cyber Resilience Act

6 giugno 2025

PRIVACYDAY
INNOVAZIONE RESPONSABILE E COMPLIANCE PER LA SOSTENIBILITA' DELLA TRASFORMAZIONE DIGITALE
Arezzo Fiere & Congressi, venerdì 6 Giugno 2025

Un Possibile Percorso: L'Approccio Olistico

L'Approccio Olistico e la Convergenza Normativa

Il principio fondamentale da cui partire è quello della responsabilizzazione (Accountability), sancito dall'articolo 5, paragrafo 2 del Regolamento (UE) 2016/679 (GDPR), secondo cui:

"Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo."

L'Unione Europea ha introdotto una serie di normative strategiche per regolamentare il mondo digitale, con l'obiettivo di proteggere i cittadini, rafforzare la sicurezza e promuovere un mercato unico digitale equo e competitivo.

Outsourcing nell'Era della Convergenza Normativa

Protezione dei Dati Personali e della Privacy:

- ❑ Regolamento Generale sulla Protezione dei Dati (GDPR - Regolamento UE 2016/679)
- ❑ Direttiva ePrivacy (Direttiva 2002/58/CE, modificata dalla Direttiva 2009/136/CE)

Cybersecurity e Sicurezza delle Reti e dei Sistemi:

- ❑ Direttiva NIS2 (Direttiva UE 2022/2555 - Network and Information Security 2)
- ❑ Regolamento sulla Cibersicurezza (Cybersecurity Act - Regolamento UE 2019/881)
- ❑ DORA (Digital Operational Resilience Act - Regolamento UE 2022/2554)
- ❑ Cyber Resilience Act (CRA - Proposta di Regolamento, approvata dal Consiglio e dal Parlamento, in attesa di pubblicazione in Gazzetta Ufficiale)

Intelligenza Artificiale e Dati (non personali):

- ❑ AI Act (Artificial Intelligence Act - Regolamento UE 2024/1689)
- ❑ Data Governance Act (DGA - Regolamento UE 2022/868)
- ❑ Data Act (Proposta di Regolamento, approvata dal Consiglio e dal Parlamento, in attesa di pubblicazione in Gazzetta Ufficiale)

Servizi Digitali e Piattaforme Online:

- ❑ Digital Services Act (DSA - Regolamento UE 2022/2065)
- ❑ Digital Markets Act (DMA - Regolamento UE 2022/1925)

Identità Digitale:

- ❑ Regolamento eIDAS2 (Regolamento UE 2024/1183 - Electronic Identification, Authentication and Trust Services 2)

I 4 Pilastri della Compliance Digitale (e non solo)

GDPR

PERSONA

Norma: Reg. (UE) 2016/679 | D.Lgs. 101/2018
Obiettivo: Proteggere i dati e i diritti fondamentali delle persone fisiche.
Ambito: Qualsiasi entità che tratta dati personali di persone nell'UE.

NIS2

SERVIZIO

Norma: Dir. (UE) 2022/2555 | Recepimento italiano in corso
Obiettivo: Garantire un livello comune elevato di cybersicurezza per i servizi essenziali.
Ambito: Soggetti "essenziali" e "importanti" in settori critici e la loro supply chain.

DGA

CONDIVISIONE

Norma: Reg. (UE) 2022/868 | Attuazione italiana in corso
Obiettivo: Facilitare la condivisione sicura di dati (anche industriali) e creare fiducia.
Ambito: Organismi pubblici, intermediari di dati, organizzazioni per l'altruismo dei dati.

CRA

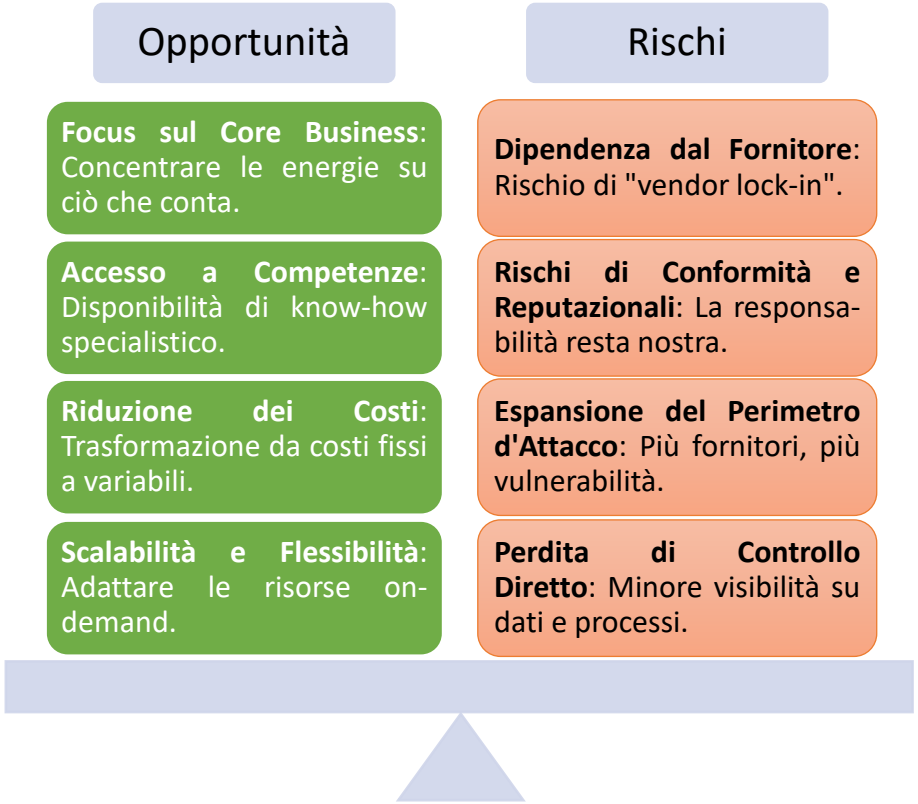
PRODOTTO

Norma: Regolamento in fase di approvazione finale
Obiettivo: Imporre requisiti di cybersicurezza per i prodotti con elementi digitali.
Ambito: Produttori, importatori e distributori di prodotti hardware e software.

Efficienza vs. Rischio: Il Paradosso dell'Outsourcing

L'esternalizzazione è una leva strategica fondamentale per la crescita, ma introduce nuove complessità. È cruciale comprendere entrambe le facce della medaglia.

La scelta di esternalizzare è strategica e irreversibile. Il nostro compito non è fermarla, ma governarla. La perdita di controllo diretto è il rischio principale, un rischio che oggi non è solo '**di privacy**', ma anche '**di sicurezza**', '**operativo**' e '**di conformità del prodotto**'.



Un Fornitore, Molteplici Obblighi

Scenario Pratico: Utilizziamo un software gestionale in cloud fornito da un'azienda esterna.Questo singolo fornitore, a seconda del contesto, assume molteplici ruoli e obblighi:

- **Per il GDPR, è un Responsabile del Trattamento** Tratta i dati personali dei nostri dipendenti e clienti per nostro conto e su nostra istruzione.
- **Per la NIS2, è parte della nostra Supply Chain** Se operiamo in un settore critico (es. sanità, energia, finanza), la sua sicurezza e resilienza impattano direttamente sulla nostra capacità di erogare il servizio.
- **Per il CRA (Cyber Resilience Act), il suo software è un Prodotto Digitale** Dovrà essere immesso sul mercato con requisiti di sicurezza "by design" e il fornitore avrà obblighi continuativi sulla gestione delle vulnerabilità.
- **Per il DGA (Data Governance Act), potrebbe essere un Intermediario di Dati** Se offre servizi avanzati di analisi aggregata o di condivisione di dati (anche anonimi) con terze parti, potrebbero applicarsi le regole sulla neutralità e trasparenza.

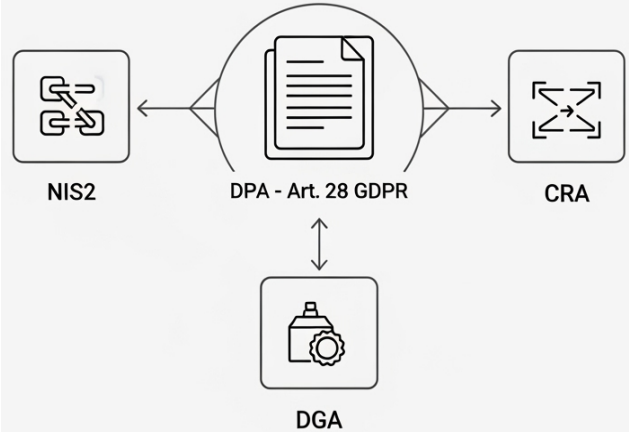
Dalla Nomina a Responsabile alla Governance Integrata del Fornitore

Il **DPA (Art. 28 GDPR)** rimane la base fondamentale per i dati personali. Ma se vogliamo adottare una modalità di gestione olistica dobbiamo integrarlo, seguendo il precedente esempio, Il nostro contratto deve considerare anche:

Clausole sulla Sicurezza della Supply Chain (Art. 21 NIS2): Obblighi di notifica degli incidenti che impattano il nostro servizio, requisiti minimi di sicurezza, diritto di audit esteso alla resilienza operativa.

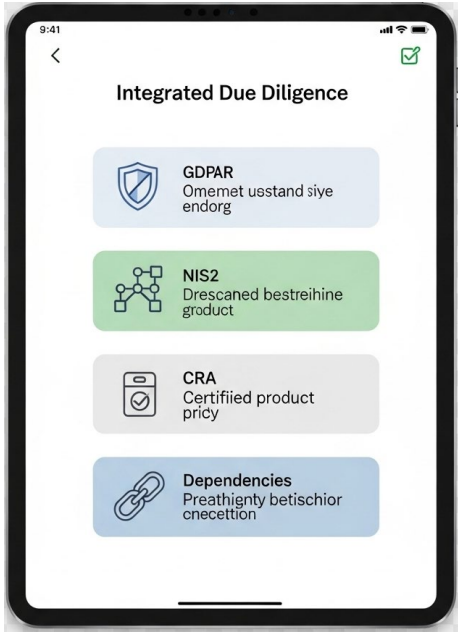
Requisiti di Conformità del Prodotto (CRA): Obbligo per il fornitore di mantenere il software sicuro, gestire le vulnerabilità e fornire dichiarazioni di conformità CE.

Obblighi specifici per l'Intermediazione (DGA): Se applicabile, clausole che garantiscano neutralità e trasparenza.



Checklist di Valutazione Precontrattuale 2.0 (1)

La valutazione di un fornitore oggi richiede uno sguardo a 360 gradi. Oltre alle garanzie fondamentali del GDPR, la nostra analisi deve includere:



Verifica Trattamento Dati (GDPR):

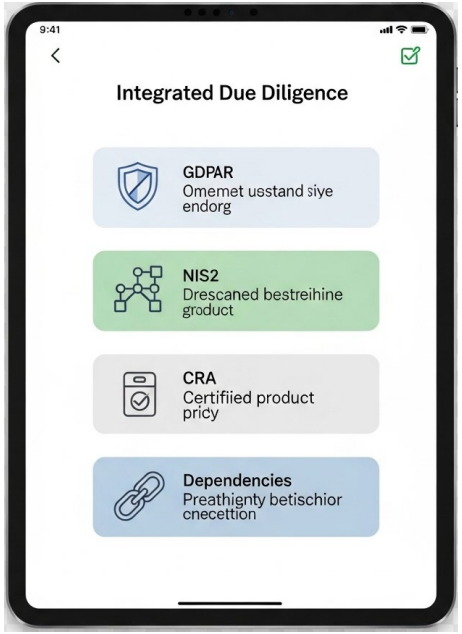
- Il fornitore offre un DPA (Art. 28 GDPR) completo e non generico?Le misure di sicurezza tecniche e organizzative descritte sono adeguate al rischio? (es. cifratura, pseudonimizzazione).
- Viene garantita la trasparenza sulla nomina di eventuali sub-responsabili?
- Sono definiti i processi per la gestione dei data breach e per l'esercizio dei diritti degli interessati?

Verifica di Resilienza (NIS2):

- Qual è lo status del fornitore (soggetto essenziale/importante)?
- Esistono e sono adeguate le sue policy di gestione del rischio della supply chain?

Checklist di Valutazione Precontrattuale 2.0 (2)

La valutazione di un fornitore oggi richiede uno sguardo a 360 gradi. Oltre alle garanzie fondamentali del GDPR, la nostra analisi deve includere:



Verifica Sicurezza del Prodotto (CRA):

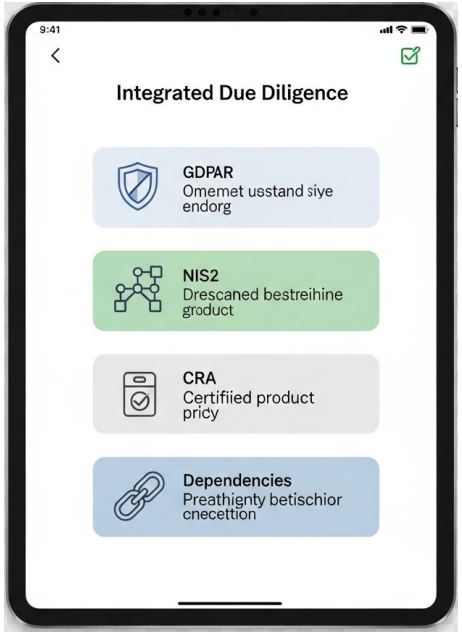
- Il software (prodotto digitale) possiede i requisiti di sicurezza "by design"?
- Il fornitore ha un processo documentato per la gestione delle vulnerabilità e il rilascio di patch di sicurezza?
- È in grado di fornire una dichiarazione di conformità CE per il prodotto, come previsto dal CRA?

Verifica delle Dipendenze (Supply Chain):

- Quali sono i sub-fornitori critici da cui dipende il nostro fornitore?
- È garantita la trasparenza e il controllo lungo tutta la catena?

Checklist di Valutazione Precontrattuale 2.0 (3)

La valutazione di un fornitore oggi richiede uno sguardo a 360 gradi. Oltre alle garanzie fondamentali del GDPR, la nostra analisi deve includere:



Verifica Intermediazione Dati (DGA):

- Il servizio offerto dal fornitore si qualifica come "servizio di intermediazione di dati"?
- In caso affermativo, sono presenti clausole contrattuali che ne garantiscano la neutralità e la trasparenza, come richiesto dal DGA?

Verifica Affidabilità e Certificazioni:

- Il fornitore possiede certificazioni riconosciute (es. ISO/IEC 27001) e ne fornisce evidenza?
- È disponibile a condividere report di audit recenti (es. SOC 2) per una valutazione indipendente dei controlli?

Costruire un Accordo a Prova di Futuro

Il contratto moderno è una piattaforma flessibile, non un blocco di cemento. La struttura vincente si basa su:

- ❑ **Master Service Agreement (MSA):** Il "contenitore" con le condizioni legali e commerciali generali.
- ❑ **Clausola di Revisione Normativa:** Un meccanismo per adeguare l'accordo alle nuove leggi senza rinegoziare tutto da capo.
- ❑ **SLA di Sicurezza:** Accordi sul livello di servizio che misurano le performance di sicurezza (es. tempo massimo per applicare una patch critica).
- ❑ **Allegati Modulari (Add-on):**
  - **DPA (GDPR):** Per il trattamento dei dati personali.
  - **Allegato Sicurezza (NIS2):** Per le misure di resilienza e la gestione degli incidenti.
  - **Allegato Conformità (CRA):** Per gli obblighi di sicurezza del prodotto.

Dalla Conformità Puntuale alla Fiducia Continua

La fiducia non si basa su un controllo annuale, ma su un flusso costante di informazioni. Il nostro cruscotto di monitoraggio deve integrare diverse fonti per avere una visione completa:

- **Report di Audit (SOC 2):** Per una valutazione indipendente e periodica dei controlli.
- **Stato Certificazioni (ISO 27001):** Per la conferma di un sistema di gestione maturo.
- **Bollettini di Sicurezza (CRA):** Per il monitoraggio proattivo delle vulnerabilità di prodotto.
- **Notifiche di Incidenti (NIS2):** Per la gestione tempestiva degli eventi che impattano la resilienza.

Rompere i Silos: Un Framework, Molteplici Risposte

L'approccio vincente è adottare un **Sistema di Gestione della Sicurezza delle Informazioni (SGSI)** basato su standard internazionali o propri Modelli Organizzativi.

ISO/IEC 27001:2022 è un buon esempio.

Un unico **processo di analisi del rischio** può identificare i rischi relativi a dati personali (GDPR), continuità operativa (NIS2) e sicurezza del prodotto (CRA).

Un unico **framework di controlli** (es. l'Annex A della ISO 27001) può essere mappato per rispondere ai requisiti di tutte le normative.

Questa è la chiave per ridurre la complessità. Invece di avere quattro checklist e quattro team che fanno lo stesso lavoro, creiamo un unico motore di compliance. L'analisi del rischio e la gestione dei fornitori diventano processi centralizzati che 'alimentano' la conformità a tutte le normative applicabili.

Da Centro di Costo a Vantaggio Competitivo

Adottare un framework integrato, non è solo una questione di conformità normativa, è soprattutto una decisione strategica che trasforma il modo in cui gestiamo i fornitori, ottimizzando l'intero ciclo di vita e generando valore tangibile.

Efficienza Operativa e Riduzione dei Costi: Un unico processo di valutazione semplifica e accelera la qualifica (onboarding) di nuovi fornitori, riducendo i tempi e i costi amministrativi.

Visione Strategica del Rischio di Terze Parti: La gestione continua del fornitore avviene tramite un unico cruscotto di controllo, offrendo al management una visione chiara e aggregata del rischio, non più frammentata per singola normativa.

Maggiore Resilienza e Tutela: Un processo di uscita (offboarding) strutturato e basato su controlli integrati garantisce la sicura cancellazione o restituzione dei dati e la chiusura di tutte le vulnerabilità, proteggendo l'azienda anche al termine del rapporto.

Vantaggio Competitivo e Fiducia del Mercato: Dimostrare un processo di governance dei fornitori maturo e integrato non solo ci rende più resilienti, ma ci qualifica come un partner più affidabile agli occhi dei clienti e del mercato.

Le Azioni Chiave da Portare a Casa

PENSA in modo integrato:
Valuta i fornitori non solo per il GDPR, ma anche per la resilienza (NIS2) e la sicurezza dei prodotti (CRA) e altro nelle tue valutazioni.

VALUTA in modo olistico (Due Diligence 2.0):
La checklist di conformità precontrattuale del fornitore deve coprire tutti gli angoli normativi.

CONTRATTUALIZZA in modo robusto (Contratto Modulare):
L'Art. 28 è solo l'inizio. Supera il DPA - Integra il contratto con allegati modulari per coprire la sicurezza della supply chain e la conformità del prodotto.

GOVERNA ciclo di vita del fornitore con un sistema (SGSI): Adotta, o meglio costruisci, un tuo framework (personalizzando e integrando ad es. la ISO 27001) per gestire la complessità in modo efficiente e sostenibile.

Grazie della vostra attenzione

Domande e Risposte

Felice Amelia
Responsabile Privacy E.S.TR.A SpA
famelia@estraspa.it