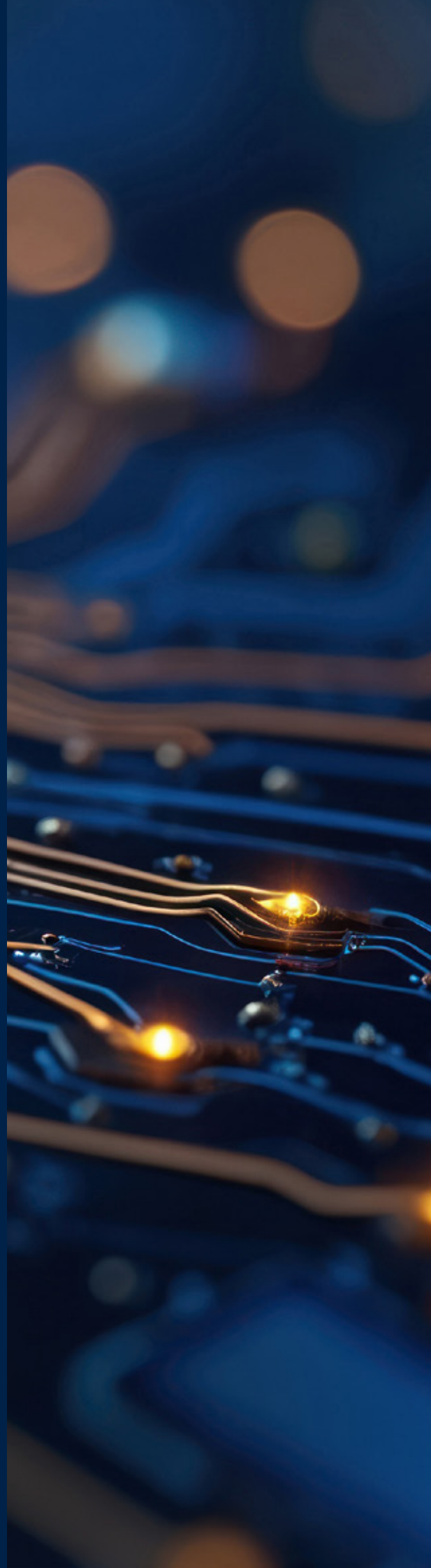


**Garantire la
capacità d'azione:**
*guida alla
sovranità digitale*

BEST PRACTICE GUIDE

Opportunità e dipendenze: Il percorso verso la sovranità digitale	03
Sette misure per l'indipendenza digitale aziendale:	04
1. Alternative open source	04
2. Tecnologia made in UE	05
3. Gestione dei dati nel cloud	06
4. On-premise invece del cloud	07
5. Responsabilizzazione dei partner	08
6. Sviluppare strategie di uscita	09
7. Co-management e diversificazione	10
Conclusioni e prospettive	11
Contattaci	13



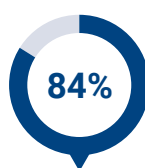
Opportunità e dipendenze: Il percorso verso la sovranità digitale

Nel nostro mondo interconnesso e basato sui dati, la sovranità digitale è passata da semplice parola d'ordine a fattore strategico di successo per le aziende. L'integrazione con i partner commerciali, l'utilizzo di servizi cloud e i modelli di business data-driven offrono enormi opportunità. Tuttavia, questi aspetti richiedono un'analisi critica:



Dipendenza dall'estero

Il 96% delle aziende UE dipende da tecnologie e servizi digitali esteri, principalmente da Stati Uniti e Cina.



Sostenitori

L'84,4% dei responsabili delle decisioni IT preferisce prodotti digitali europei per le infrastrutture critiche, ma solo il 20% sta effettuando il passaggio.



Strategia concreta

Solo il 21% delle aziende ha sviluppato una strategia concreta per la sovranità digitale.



Obiettivo strategico

L'87% delle aziende considera l'indipendenza digitale un obiettivo strategico, tuttavia il 79% dipende criticamente da pochi fornitori, prevalentemente non europei.

La sovranità digitale assume importanza crescente, soprattutto in periodi di incertezza globale, crescenti minacce informatiche e requisiti normativi complessi. Mantenere il controllo su informazioni, infrastrutture e processi digitali è fondamentale per evitare dipendenze da fornitori terzi, piattaforme esterne o interessi geopolitici. L'obiettivo è garantire autonomia operativa, minimizzare i rischi e mantenere la competitività a lungo termine.



Secondo uno studio condotto da adesso e dall'Handelsblatt Research Institute, la carenza di competenze specializzate e i costi elevati continuano a rallentare l'espansione della sovranità digitale in molte realtà aziendali.

Sette misure per l'indipendenza digitale aziendale:

1. Alternative open source

La maggior parte del software utilizzato quotidianamente negli uffici proviene da grandi aziende con modelli di licenza spesso unilaterali e restrittivi. Chi si affida completamente a singoli ecosistemi chiusi (walled garden) rischia di subire pressioni da questi fornitori. L'utilizzo di software open source gratuito permette di evitare questa problematica:

- ✓ **Eliminazione dei costi di licenza**
- ✓ **Indipendenza da singoli produttori**
- ✓ **Maggiore sicurezza grazie alla revisione continua del codice e alla tracciabilità**
- ✓ **Supporto di ampie comunità online**

ESEMPI SIGNIFICATIVI

di soluzioni open source professionali includono LibreOffice, l'editor di immagini GIMP, il sistema operativo Linux, il browser Mozilla Firefox e il client di posta Thunderbird.

2. Tecnologia made in UE

La sovranità dei dati dipende dalla giurisdizione del partner tecnologico. Se un partner è obbligato dal proprio governo a cedere dati, nessun accordo contrattuale può offrire protezione. La scelta del fornitore giusto è quindi essenziale.

L'UE e i suoi Stati membri vantano le normative più rigorose al mondo in materia di:

- **Protezione dei dati**
(GDPR, TISAX, DORA)
- **Tutela dei consumatori**
(Digital Fairness Act, Digital Services Act)
- **Obblighi di due diligence**
(EU Data Act, EU Supply Chain Act)

Software e servizi provenienti dai paesi UE rappresentano quindi un investimento sicuro per proteggere dati e infrastrutture in termini di certezza giuridica e tutela legale. Questo aspetto è particolarmente rilevante nella scelta di fornitori cloud. Anche se i data center si trovano nell'UE, **la sede legale dell'azienda rimane un fattore determinante.**



3. Gestione dei dati nel cloud

L'archiviazione cloud non dovrebbe basarsi esclusivamente sulla sicurezza garantita dal fornitore. Anche utilizzando servizi cloud all'interno dell'UE, con le sue rigorose norme sulla protezione dei dati, è necessario considerare:

Crittografia

La sicurezza richiede che neanche il fornitore cloud abbia accesso ai dati in chiaro. Le aziende che crittografano i propri dati dimostrano responsabilità e rafforzano la fiducia nei processi digitali.

Procedure di cancellazione

Dopo la risoluzione contrattuale, è necessario garantire l'effettiva eliminazione dei dati.

Gestione delle autorizzazioni

L'utilizzo dei servizi cloud richiede sistemi di autorizzazione affidabili e ben strutturati. Vale il principio „quanto necessario, il minimo possibile“.



Queste misure consentono di raggiungere un adeguato livello di sicurezza e indipendenza.



4. On-premise invece del cloud

I servizi cloud attraggono per praticità e scalabilità. Tuttavia, il loro utilizzo implica l'affidamento dei propri dati a terzi. Per chi preferisce evitarlo, il ritorno all'on-premise offre vantaggi significativi:

- ✓ **Nessun accesso di terzi a risorse digitali sensibili**
- ✓ **Soluzione spesso più economica nel lungo periodo**
- ✓ **Risoluzione più rapida dei problemi tramite personale interno**



Per il successo delle soluzioni on-premise, le aziende devono investire tempestivamente in competenze e attrezzature tecniche interne.

5. Responsabilizzazione dei partner

La sovranità digitale si raggiunge solo proteggendo i propri processi e sistemi interni e responsabilizzando costantemente i partner aziendali. I partner tecnologici e di servizio svolgono un ruolo cruciale nel trattamento dei dati sensibili e nella fornitura di infrastrutture digitali. È essenziale stabilire chiare norme contrattuali su trattamento e archiviazione dei dati, oltre a standard di sicurezza.



Trasparenza

Esigi massima trasparenza dai tuoi partner.



Divulgazione

Richiedi la divulgazione di subappaltatori e loro sedi per identificare rischi potenziali derivanti da accessi legali stranieri (CLOUD Act o normative simili).



Protezione

Assicurati che gli accordi contrattuali regolino esplicitamente la protezione contro accessi non autorizzati e stabiliscano meccanismi vincolanti per la sicurezza delle informazioni.



Verifica

Conferma contrattualmente audit e certificazioni regolari (es. ISO 27001) per verificare la conformità agli standard promessi.



6. Sviluppare strategie di uscita

Le aziende evolvono e i partner tecnologici potrebbero non soddisfare più i requisiti di sicurezza e conformità. Le ragioni possono essere molteplici: modelli di business modificati, incidenti di sicurezza, mancanza di trasparenza o sviluppi geopolitici. Per poter agire tempestivamente, è consigliabile identificare alternative per tutti i sistemi critici e sviluppare strategie di uscita.

La strategia dovrebbe includere processi e responsabilità chiari per attuare il cambiamento in modo strutturato e con minimo impatto.



Compito 1

Effetua inventari regolari per verificare quali servizi utilizzate e quali alternative sono disponibili

Compito 2

Crea un processo che definisca procedure per il cambio di servizio/ tecnologia e relative responsabilità

Compito 3

Stabilisci scadenze per la cancellazione dei dati dal precedente partner e richiedi prova dell'eliminazione completa.

7. Co-management e diversificazione

La sovranità digitale significa operare indipendentemente da singole soluzioni software. Le aziende non dovrebbero dipendere da un unico fornitore, ma puntare sulla diversificazione. L'utilizzo simultaneo di sistemi compatibili aumenta l'affidabilità e consente di rimanere operativi in caso di interruzioni.

Il co-management supporta questo approccio attraverso:

- **Gestione simultanea su piattaforme diverse**
- **Flessibilità nell'infrastruttura IT secondo il principio „best of breed“**
- **Prevenzione degli effetti di lock-in**

Combinando diversificazione e co-management, le aziende mantengono il controllo sui processi digitali e possono rispondere più rapidamente ai cambiamenti tecnici, economici o normativi.



Conclusioni e prospettive

La sovranità digitale non è un progetto singolo, ma un processo continuo che richiede pensiero strategico, competenza tecnologica e chiarezza organizzativa. Le aziende che oggi impostano la rotta corretta si assicureranno l'indipendenza e la flessibilità necessarie per rispondere con sicurezza alle sfide future.



Esamina le tue attuali dipendenze digitali, definisci obiettivi chiari per una maggiore autodeterminazione digitale e implementateli con coerenza.

**È il momento
*di agire.***

Informazioni su baramundi software GmbH

baramundi software sviluppa soluzioni di gestione unificata degli endpoint per l'amministrazione centralizzata di PC, dispositivi mobili e server. Automatizza la distribuzione del software, semplifica la gestione delle patch e crea trasparenza nella rete. baramundi contribuisce in modo significativo alla sicurezza IT e libera risorse.



Hai domande?

Non esita a fissare un appuntamento con noi.

Durante un incontro personale ti spiegheremo come il software baramundi può aiutarti a raggiungere una maggiore indipendenza digitale con la soluzione di gestione unificata degli endpoint.



Contattaci.

*Non vediamo l'ora
di incontrarti!*



Making IT Admins Smile



baramundi software GmbH
Forschungsallee 3
86159 Augsburg, Germany
+49 821 56708-380
request@baramundi.com



+43 1 928 0136 0010
request@baramundi.com



+41 77 280 49 79
request@baramundi.com



+39 340 8861886
request-italia@baramundi.com



+48 735 91 44 54
request@baramundi.com



+44 2071 93 28 77
request@baramundi.com



baramundi software USA, Inc.
30 Speen St, Suite 501
Framingham, MA 01701, USA
+1 508 861 7561
requestUSA@baramundi.com



+49 821 56708-390
request@baramundi.com