Microsoft

Adeguamento al GDPR: come un modello IaaS può semplificare il tuo percorso

Le aziende in tutto il mondo sono alle prese con l'adeguamento al Regolamento generale sulla protezione dei dati (GDPR) dell'Unione europea.

Procedi nella direzione giusta per l'adeguamento al GDPR con IaaS di Azure

Come evitare malintesi riguardo al GDPR

FALSO Il GDPR non si applica alle aziende che non svolgono attività nell'Unione europea.

VERO Il GDPR si applica a qualsiasi azienda che archivi informazioni personali di un cittadino dell'Unione europea, indipendentemente da dove si trovi.

FALSO L'adeguamento al GDPR è semplice come acquistare la soluzione giusta.

VERO Non esistono soluzioni sul mercato in grado di "rendere" un'azienda adeguata al GDPR. Si tratta di un grande onere, che richiede un impegno costante da parte dell'azienda.

FALSO La classificazione dei dati è responsabilità della parte che digitalizza e archivia i dati (in questo caso, il service provider di soluzioni cloud).

VERO Le aziende che raccolgono dati sono responsabili esclusivamente della loro governance, la quale include la classificazione e l'identificazione dei dati che rientrano nell'ambito delle nuove definizioni del GDPR.

FALSO Il GDPR prevede che i dati personali debbano rimanere all'interno dell'Unione europea.

VERO Ai sensi del GDPR, le aziende possono archiviare i dati personali di un cittadino dell'Unione europea all'esterno dell'UE, ma solo conformemente a quanto stabilito dal GDPR.

Responsabilità condivise

Se lavori con un modello interamente locale, i problemi di sicurezza ricadono tutti su di te. Se utilizzi un modello IaaS, il provider di servizi cloud è responsabile di elementi quali i server e l'hardware di rete. Sebbene la configurazione della rete, la gestione di accessi e identità e la protezione degli endpoint rimangano di tua responsabilità, condivisa o esclusiva, Azure offre servizi che consentono quanto segue:

Requisito GDPR	Le aziende devono identificare e individuare i dati personali che rientrano nella giurisdizione del GDPR.	Le aziende devono segnalare tempestivamente eventuali violazioni di dati personali.	Le aziende devono rispettare le obiezioni di un utente al trattamento dei suoi dati.
Contributo di Azure	La capacità di elaborazione DSR (Data Subject Request), integrata nel portale di Azure, consente di gestire le richieste dei dati personali.	Il Centro sicurezza consente di monitorare automaticamente minacce e violazioni della sicurezza.	Grazie al controllo degli accessi in base al ruolo è possibile revocare in qualsiasi momento l'accesso ai dati.

Imposta una rotta per il futuro

IaaS di Azure offre una soluzione efficiente ed economica per gestire i dati personali ai sensi del GDPR e garantisce scalabilità futura con:

- Una struttura dei costi flessibile per garantire il pagamento dei soli servizi utilizzati.
- Capacità elastica del server che si espande e comprime in base alle esigenze.
- Servizi gestiti per rimanere concentrati sul business.

Domande frequenti sul GDPR

Contributo di Microsoft Azure

Scopri di più su Azure

Microsoft Azure