AUTONOME PROVINZ BOZEN - SÜDTIROL
Deutsche Bildungsdirektion
Abteilung 16 Bildungsverwaltung
Beschaffungsamt

PROVINCIA AUTONOMA DI BOLZANO - ALTO ADIGE
Direzione Istruzione e Formazione tedesca
Ripartizione 16 Amministrazione istruzione e formazione
Ufficio Acquisti

Al sig.
[redacted]

Bolzano, 07.01.2021

Redatto da:
Johann Parigger
Tel. 0471 417600
Bildungsverwaltung@provincia.bz.it

Per conoscenza: All'Ufficio Organizzazione

Richiesta di accesso civico generalizzato del 9/12/2020

Gentile sig. [redacted]
in ordine alla richiesta di accesso civico generalizzato del 9/12/2020 si trasmettono i seguenti documenti:

- Decreto 16908/2020
- Informazioni da parte di Microsoft

Per quanto concerne la valutazione comparativa prevista dall'art. 68 del Codice dell'amministrazione digitale (CAD) si fa presente che la decisione di stipulare il contratto *"Enrollment for Education Solutions"* persegue due obiettivi distinti:

1) Il primo obiettivo è quello di mettere a disposizione del personale delle scuole, compreso il personale insegnante, un pacchetto office per il lavoro amministrativo. Il decreto 16908/2020 motiva la scelta dei prodotti di Microsoft con un rinvio alla decisione della Giunta Provinciale n. 388/2016 che prevede la migrazione della suite Office allora in uso verso Microsoft Office 365 in tutte le pubbliche amministrazioni dell'Alto Adige. Quindi questa decisione vale anche per l'attività amministrativa delle scuole. Si fa inoltre presente che si acquistano le licenze per le scuole con un contratto separato da quello dell'amministrazione centrale perché il contratto EES è economicamente molto più conveniente rispetto a quello per l'amministrazione. Poiché il decreto 16908/2020 si basa sulla decisione di massima della Giunta Provinciale n. 388/2016 e mette in atto questa deliberazione, si ritiene che non serva un'ulteriore valutazione comparativa.
2) Il secondo obiettivo della stipula del contratto Microsoft è quello di mettere a disposizione i prodotti Microsoft per l'uso didattico. Si fa presente che le scuole in base all'autonomia scelgono il software da utilizzare per l'insegnamento in base alle disposizioni dell'ordinamento scolastico, quindi per il primo ciclo la legge provinciale 5/2008 e per il secondo ciclo la legge provinciale 11/2010 e, inoltre, in base alle singole indicazioni provinciali e al piano triennale dell'offerta formativa adottato dalle singole scuole. Quindi la decisione di utilizzare i prodotti Microsoft anche nella didattica spetta solo ed esclusivamente alla singola scuola autonoma e non all'amministrazione provinciale. Per questo motivo la stipula del contratto EES da parte della Direzione Istruzione e Formazione anche per la didattica si basa sul comma 12 dell'articolo 12 della legge provinciale 12/2000, recante "Autonomia delle scuole". La stipula del contratto centralizzato comporta un vantaggio economico di oltre il 40% per ogni licenza e nella rilevazione delle scuole interessate alla conclusione del contratto Microsoft ca. il 90% delle scuole ha indicato di utilizzare i prodotti Microsoft. Siccome il contratto centralizzato per l'utilizzo dei prodotti per la didattica è solo un'offerta contrattuale e non obbliga la singola scuola ad utilizzare i prodotti Microsoft, una valutazione compartiva non può essere effettuata dall'amministrazione centrale. Per la combinazione

di questi due obiettivi i costi per la didattica non sono più rilevanti perché le licenze per gli studenti sono tutti senza costi.

I documenti di riferimento per la decisione sono quindi il decreto 16809/2020 e la deliberazione della Giunta Provinciale n. 388/2016 che si allegano.

Per quanto riguarda la valutazione e la documentazione relative alle misure conforme alla sentenza "Schrems II" si fa presente che si tratta di una problematica che viene discussa dagli esperti in modo divergente e contraddittorio anche nei confronti del cloud di Microsoft 365. Come si evince dalle informazioni fornite da parte di Microsoft sulla protezione dei dati, la ditta Microsoft si adegua alla normativa europea rispettando la suddetta sentenza, e dimostra che i dati vengono tenuti su server situati in Europa evitando il trasferimento di dati verso paesi diversi dall'Unione europea. Si ritiene che la sicurezza dei dati nel cloud di Microsoft 365 sia sufficiente e conforme e che serva un intervento normativo su livello europeo per risolvere la valutazione divergente del trattamento di dati da parte di gruppi multinazionali.

Con riguardo alle attuali disposizioni di usare la didattica a distanza per l'insegnamento nelle scuole, si ritiene che il rischio residuo sia di minore entità; anche il Ministero dell'Istruzione per questo motivo promuove nel suo sito (link: https://www.istruzione.it/coronavirus/didattica-a-distanza.html) le piattaforme di Google, Microsoft e Wescool.

In concreto, anche in questo tema si devono distinguere i due obiettivi, cioè l'amministrazione e la didattica, per i quali vengono utilizzati anche due *tennants* distinti con livelli di sicurezza differenti. Si ritiene conforme alle indicazioni dell'AGID il *tennant* dell'amministrazione provinciale per il quale è competente la ripartizione informatica. Per questo motivo le scuole sono state informate di non usare il *tennat* della didattica per trattare dati amministrativi e di prestare particolare attenzione nell'utilizzo di dati personali nell'ambito della didattica a distanza. Un gruppo di lavoro sta elaborando ulteriori indicazioni e informazioni sull'utilizzo dei due *tennat*.

Cordiali saluti

Il Direttore di Ripartizione
Stephan Tschigg
(sottoscritto con firma digitale)

Allegati:
- Decreto 16908/2020
- Deliberazione 388/2016
- Informazioni da parte di Microsoft

Informazione da parte Microsoft sulla protezione dei dati
FONTE: https://docs.microsoft.com/it-it/microsoft-365/enterprise/eu-data-storage-locations?view=o365-worldwide

Posizioni dei dati per l'Unione europea

I dati dei clienti sono fondamentali

Microsoft riconosce l'importanza di mantenere la privacy e la riservatezza dei dati aziendali. I dati appartengono all'utente, che può accedervi, modificarli o eliminarli in qualsiasi momento. Microsoft non userà i dati senza il consenso dell'utente e, dopo il consenso, userà i dati solo per fornire i servizi che si sono scelti. Se l'utente lascia uno dei servizi, si garantisce la conservazione dei dati personali da parte dell'utente attraverso la rimozione dei dati dai sistemi secondo rigorosi standard e processi.

Nota

I dati dei clienti, noti anche come "dati" o "dati commerciali", includono tutti i dati, tra cui testo, audio, video o file di immagine e il software fornito direttamente dall'utente o per conto dell'utente a Microsoft usando i servizi Microsoft Enterprise online, esclusi Microsoft Professional Services. Include il contenuto dei clienti, ossia i dati caricati per la risorsa di archiviazione o l'elaborazione e le app caricate per la distribuzione tramite un servizio cloud Microsoft aziendale. Ad esempio, il contenuto dei cliente includi la posta elettronica e gli allegati di Exchange Online, il contenuto del sito di Microsoft SharePoint Online* o una conversazione di messaggistica istantanea

Archiviazione ed elaborazione dei dati

Se si usano i servizi di Microsoft 365, si inizia con il presupposto che i clienti aziendali vorrebbero che i propri dati commerciali venissero archiviati ed elaborati poco lontano.When you use Microsoft 365 services, we start with the assumption that our enterprise customers would like to have their business data stored and processed close to home. Se possibile, si procede in questo modo.Wherever possible, we do just that. Per mantenere i dati nei data center più vicini, archiviare i dati in base alla sede aziendale fornita durante la creazione del tenant.To keep your data in datacenters nearest to you, we store your data based on the business location you provide when you create your tenant. Per scegliere le posizioni di archiviazione importanti per le attività dell'organizzazione, è possibile creare un numero illimitato di tenant per l'organizzazione

Dove vengono archiviati i dati UE dei clienti

Il data center GEOS è disponibile in Germania e in Francia e consente di archiviare i dati nel proprio paese, se ivi è ubicata l'azienda. I data center dell'Unione europea si trovano in Austria, Finlandia, Francia, Irlanda e Paesi Bassi. I dati dei servizi seguenti verranno ospitati nelle posizioni seguenti in base all'indirizzo di fatturazione scelto:

Dove vengono archiviati i dati UE dei clienti

Nome del servizio	Posizione dei tenant creati con un indirizzo di fatturazione in Francia	Posizione dei tenant creati con un indirizzo di fatturazione in Germania	Posizione dei tenant creati con un indirizzo di fatturazione in altri paesi
Exchange Online	Francia	Germania	Unione Europea
OneDrive for Business	Francia	Germania	Unione Europea
SharePoint Online	Francia	Germania	Unione Europea
Skype for Business	Unione Europea	Unione Europea	Unione Europea
Microsoft Teams	Francia	Germania	Unione Europea
Office Online e Mobile	Francia	Germania	Unione Europea
Exchange Online Protection	Francia	Germania	Unione Europea
Intune	Unione Europea	Unione Europea	Unione Europea
MyAnalytics	Francia	Germania	Unione Europea
Planner	Unione Europea	Unione Europea	Unione Europea
Yammer	Unione Europea	Unione Europea	Unione Europea
Servizi di OneNote	Francia	Germania	Unione Europea
Stream	Unione Europea	Unione Europea	Unione Europea
Whiteboard	Unione Europea	Unione Europea	Unione Europea
Forms	Unione Europea	Unione Europea	Unione Europea

In che modo Microsoft protegge i dati

Misure di protezione

Microsoft protegge i dati usando più livelli di protocolli di sicurezza e crittografia. Ottenere una panoramica delle funzionalità di sicurezza dei dati Microsoft nell'articolo Crittografia di Microsoft 365.

Per impostazione predefinita, le chiavi gestite di Microsoft proteggono i dati dei clienti. I dati che rimangono permanenti su qualsiasi supporto fisico sono sempre crittografati con protocolli di crittografia conformi a FIPS 140-2. È anche possibile usare le chiavi gestite dal cliente (CMK), Doppia crittografiae/o i moduli di sicurezza hardware (HSM) per una maggiore protezione dei dati.

Tutto il traffico dei dati tra i data center è protetto anche con gli standard di sicurezza IEEE 802.1 AE MAC, evitando gli attacchi fisici "Man-in-the-Middle".

Per impedire l'accesso fisico non autorizzato ai data center, vengono impiegati controlli e processi operativi rigorosi che includono videocontrolli continui, personale di sicurezza addestrato e processi specifici, nonché controlli di accesso multifattoriali come smart card o biometrici. Al termine del ciclo vitale, i dischi dati vengono eliminati e distrutti. Se un'unità disco usata per la risorsa di archiviazione subisce un errore hardware o raggiunge la fine del ciclo vitale, viene cancellata o eliminata in tutta sicurezza. I dati nell'unità vengono completamente sovrascritti per assicurare che non sia possibile recuperare i dati con alcun mezzo. Quando tali dispositivi vengono eliminati, vengono triturati e distrutti in linea con il NIST SP 800-88 R1, linee guida per la sanificazione dei supporti. Le registrazioni dell'avvenuta distruzione vengono conservate e riviste nell'ambito del processo di controllo e conformità Microsoft. Tutti i servizi di Microsoft 365 usano i servizi di gestione delle risorse di archiviazione e smaltimento di supporti approvati.

Controlli tecnici

Oltre alle protezioni fisiche e tecnologiche, Microsoft adotta misure efficaci per proteggere i dati dei clienti da accessi non autorizzati da parte del personale e dei subappaltatori Microsoft. L'accesso ai dati dei clienti tramite le operazioni Microsoft e il personale di supporto viene negato per impostazione predefinita. Quasi tutte le operazioni di servizio eseguite da Microsoft sono completamente automatizzate e la partecipazione umana è estremamente controllata ed eliminata dai dati dei clienti.

Solo in rari casi un tecnico Microsoft deve avere accesso ai dati dei clienti. In genere questa operazione è necessaria solo se si richiede assistenza di Microsoft per risolvere un problema del cliente. L'accesso ai dati dei clienti è estremamente limitato dai controlli di accesso basato sui ruoli, dall'autenticazione a più fattori, dalla riduzione al minimo dei dati e da altri controlli. Tutti gli accessi ai dati dei clienti sono registrati in modo rigoroso e Microsoft e terze parti eseguono verifiche regolari, nonché controlli a campione, per attestare che l'accesso è appropriato.

I clienti possono usare le chiavi gestite dai clienti per evitare che i dati siano leggibili in caso di accesso non autorizzato. Sia la crittografia lato server sia quella lato client possono contare sulle chiavi gestite dal cliente o sulle chiavi fornite dai clienti. In entrambi i casi, Microsoft non è in grado di accedere alle chiavi di crittografia e non può decrittografare i dati. Controllo SOC di un revisore accreditato di AICPA due volte all'anno per verificare l'efficacia dei controlli di sicurezza nell'ambito di controllo. Il report di attestazione del SOC 2 di tipo 2 pubblicato dal revisore spiega in quali casi può verificarsi l'accesso ai dati dei clienti e come.

Oltre a archiviare ed elaborare i dati quando si usa il servizio online, Microsoft genera i dati di servizio per monitorare l'integrità del sistema e per eseguire operazioni di servizio come la risoluzione dei problemi. Come misura di protezione della privacy, Microsoft genera e si basa su identificatori pseudonimi in questo servizio di dati generati per poter distinguere un utente da un altro senza identificare gli utenti effettivi. Gli identificatori pseudonimi non identificano direttamente una persona e le informazioni che consentono di eseguire il mapping degli identificatori pseudonimi agli utenti effettivi sono protette come parte dei dati.

Come Microsoft gestisce le richieste di enti pubblici

Se un ente pubblico vuole accedere ai dati di un cliente, deve seguire i processi legali applicabili. La richiesta deve essere inviata a Microsoft con un mandato, un ordine del tribunale, una citazione per informazioni sull'abbonato o altri dati non relativi al contenuto.
•Tutte le richieste devono essere indirizzate ad account e identificatori specifici.
•Il team addetto alla conformità legale Microsoft esamina tutte le richieste per assicurarsi che siano valide, rifiuta quelle non valide e fornisce solo i dati specificati.
•Se Microsoft è costretto per legge a divulgare i dati dei clienti, l'utente riceverà subito una notifica e riceverà una copia della richiesta, a meno che non sia legalmente vietato a Microsoft.
•Microsoft effettua una revisione legale locale di ogni richiesta ricevuta secondo le leggi e gli standard locali. Microsoft controlla inoltre periodicamente i processi di selezione in tutto il mondo per assicurare che vengano seguite le procedure giudiziarie locali e che venga applicata la relativa istruzione di esecuzione globale per i diritti umani.

Per altre informazioni sull'impegno di Microsoft per contestare gli ordini in linea con il GDPR dell'UE, vedere Nuovi passaggi per difendere i dati.

Quando i governi o le autorità delegate all'applicazione della legge inviano una richiesta legale relativa ai dati dei clienti, Microsoft si impegna a garantire la trasparenza e limita il contenuto accessibile. Due volte all'anno Microsoft pubblica il numero di richieste legali relative ai dati dei clienti ricevute dalle autorità delegate all'applicazione della legge. Vedere Report sulle richieste di applicazione della legge. Questo report non divulga le specifiche di una particolare domanda, incluso il cliente in questione. Due volte all'anno pubblichiamo anche i dati sulle richieste legali ricevute dal governo degli Stati Uniti. Vedere Report sugli ordini di sicurezza nazionale negli Stati Uniti per il report più recente.

Per altre informazioni, vedere Domande frequenti relative alle richieste del governo e delle autorità delegate all'applicazione della legge, incluse le domande sul CLOUD act.

Clausole del modello dell'Unione europea - 02/12/2020
Fonte https://docs.microsoft.com/it-it/compliance/regulatory/offering-EU-Model-Clauses

Panoramica delle clausole del modello dell'Unione europea

La legge sulla protezione dei dati dell'Unione europea (UE) regola il trasferimento dei dati personali dei clienti UE in paesi al di fuori dell'Area Economica Europea (AEE) che include tutti i paesi dell'Unione europea, Islanda, Liechtenstein e Norvegia. Le clausole del modello UE sono clausole contrattuali standard usate negli accordi tra provider di servizi (quale Microsoft) e i loro clienti per garantire che l'eventuale trasferimento di dati personali al di fuori dell'AEE sia adeguato alla legge sulla protezione dei dati europea e soddisfi i requisiti della Direttiva europea sulla protezione dei dati 95/46/EC.

A livello pratico, la conformità alle leggi sulla protezione dei dati europea significa anche che i clienti hanno bisogno di meno autorizzazioni da parte delle singole autorità per trasferire i dati personali al di fuori dell'UE, poiché la maggior parte degli Stati membri dell'UE non richiede un'autorizzazione aggiuntiva se il trasferimento si basa su un accordo conforme alle clausole del modello.

Microsoft e le clausole del modello dell'Unione europea

Microsoft ha investito nei processi operativi necessari per soddisfare i requisiti specifici delle clausole del modello per il trasferimento di dati personali ai responsabili del trattamento. Microsoft offre ai clienti clausole del modello, denominate clausole contrattuali standard, per offrire garanzie specifiche relativamente ai trasferimenti di dati personali per i servizi Microsoft interni all'ambito. In questo modo, i clienti Microsoft possono spostare liberamente dati nel cloud Microsoft dall'AEE al resto del mondo.

Tuttavia, i clienti aziendali di Microsoft, che detengono il controllo dei dati personali, hanno l'obbligo primario di proteggere tali dati. Ciò significa che i clienti aziendali dell'AEE hanno un forte interesse nell'assicurarsi che il loro provider di servizi rispetti le leggi sulla protezione dei dati dell'Unione europea, in caso contrario potrebbero essere ritenuti responsabili e subire il blocco del servizio.

Microsoft ha sottoposto le sue clausole contrattuali standard al Gruppo di lavoro articolo 29 dell'Unione europea affinché vengano riviste e approvate. Il Gruppo di lavoro articolo 29 include rappresentanti del Garante europeo della protezione dei dati, della Commissione europea e di ognuna delle 28 autorità per la protezione dei dati dell'Unione europea (DPA).

Il gruppo ha stabilito che l'implementazione delle disposizioni negli accordi Microsoft era conforme ai loro rigidi requisiti (Microsoft è stato il primo provider di servizi cloud a ricevere una lettera di approvazione da parte del gruppo). L'approvazione riguardava gli impegni riportati nelle clausole del modello 2010/87/EU ma non nelle appendici, che descrivono i trasferimenti di dati e le misure di sicurezza implementati dalla persona incaricata a importare i dati. Le appendici possono essere analizzate separatamente dalla DPA.