Informativa sul trasferimento dei dati e compatibilità con il General Data Protection Regulation (GDPR) dell'Unione Europea

Per il trasferimento dei dati tra l'Unione europea e gli Stati Uniti, Microsoft si basa da tempo due strumenti di riferimento: le Clausole Contrattuali Tipo e lo Scudo UE-USA per la privacy (EU-US Privacy Shield). Microsoft continua a basarsi sulle Clausole Contrattuali Tipo, che rimangono il meccanismo di trasferimento dei dati in vigore, e ha aggiornato l'Addendum relativo alla Protezione dei Dati Personali dei Servizi Online Microsoft (Addendum) per riflettere le obbligazioni che regolano il trasferimento dei Dati della Società, dei Dati dei Servizi Professionali e dei Dati Personali (che, ai sensi dell'Addendum, includono anche i Dati Personali compresi nei Dati di Diagnostica e nei Dati Generati dai Servizi) fuori dall'Unione Europea, dallo Spazio Economico Europeo, dal Regno Unito e dalla Svizzera in relazione all'erogazione dei Servizi Online e disciplinati dalle Clausole Contrattuali Tipo esistenti (titolare del trattamento-responsabile del trattamento) tra i clienti e Microsoft Corporation.

Lo strumento giuridico di principale rilevanza per il trattamento dei dati è il Regolamento Generale sulla Protezione dei Dati (GDPR) dell'UE. Sebbene il GDPR non imponga limiti assoluti rispetto alla conformità di Microsoft Ireland Operations Limited (MIOL) in relazione alle richieste provenienti da autorità statunitensi, impone tuttavia obbligazioni relative alla conformità delle attività correlate al trattamento e alla protezione dei Dati Personali da parte di MIOL. Ad esempio, ai sensi del GDPR, il trasferimento dei Dati Personali dall'Unione Europea verso paesi terzi devono essere in linea con i termini stabiliti dal Capo V del GDPR.

La misura in cui Microsoft viene considerata un "fornitore di servizi di comunicazione elettronica" ai sensi della Sezione 702 del Foreign Intelligence Surveillance Act (FISA) dipende da diversi fattori, tra cui, in particolare, il servizio Microsoft specifico in questione. Come indicato di seguito, in base ai termini dell'Electronic Communication Privacy Act del 1986 ("ECPA"), alcuni servizi Microsoft sono da considerarsi come servizi di comunicazione elettronica e/o servizi di elaborazione remota e rientrano pertanto nell'ambito di definizione dei "fornitori di servizi di comunicazione elettronica" ai fini dell'applicabilità della Sezione 702 del FISA. Ulteriori informazioni relative all'applicazione delle leggi sulla sicurezza nazionale degli Stati Uniti ai servizi Microsoft sono disponibili nel rapporto sul numero di ordini richiesti dalla sicurezza nazionale degli Stati Uniti: U.S. National Security Orders Report. Da sempre, Microsoft si impegna per garantire una maggiore trasparenza nelle pratiche di sorveglianza del governo degli Stati Uniti e la divulgazione dei rapporti sopra citati è il risultato di una controversia intentata da Microsoft contro il governo degli Stati Uniti nel 2013, come descritto in dettaglio in questo post di blog.

Il fatto che Microsoft rientri nell'ambito legislativo del FISA, della Sezione 702 del FISA o del Cloud Act dipende dal servizio specifico in esame. Le informazioni sul numero di richieste legali che Microsoft ha ricevuto dal governo degli Stati Uniti ai sensi delle norme in materia di sicurezza nazionale vengono divulgate tramite il rapporto sul numero di ordini richiesti dalla sicurezza nazionale degli Stati Uniti. Da sempre, Microsoft si impegna per garantire una maggiore trasparenza nelle pratiche di sorveglianza del governo degli Stati Uniti e la divulgazione dei rapporti sopra citati è il risultato di una controversia intentata da Microsoft contro il governo degli Stati Uniti nel 2013.

Per quanto riguarda la protezione dei Dati Personali ai sensi dell'articolo 44 del GDPR, Microsoft è conforme agli impegni e alle obbligazioni dell'importatore come definiti dal Comitato scientifico della sicurezza dei consumatori (CSSC) in relazione al trattamento da parte di Microsoft di tutti i dati personali correlati alla fornitura dei Servizi Online e dei Servizi Professionali. Ciò include l'accettazione delle obbligazioni dei subincaricati del trattamento, dei diritti del terzo beneficiario da parte degli interessati, dei diritti di controllo nonché della cooperazione con le autorità di vigilanza. In attesa di ulteriori indicazioni da parte del Comitato Europeo per la Protezione dei Dati (European Data Protection Board, EDPB), Microsoft ritiene che il proprio impegno sia conforme alle indicazioni del Comitato scientifico della sicurezza dei consumatori (CSSC), insieme alle garanzie fornite nelle misure supplementari sopra descritte, e che contribuisca a garantire un livello adeguato per la protezione dei dati. Gli accordi di Microsoft con i subincaricati del trattamento con accesso

ai dati personali prevedono che non venga effettuato alcun trasferimento internazionale dei Dati Personali in mancanza di previa approvazione scritta di Microsoft e che vengano rispettate le norme di protezione dei dati di eventuali Clausole Contrattuali Tipo, regole aziendali vincolanti o di altri sistemi approvati da qualsiasi autorità per la protezione dei dati, quali il Comitato europeo per la protezione dei dati o la Commissione Europea, come adottate o approvate da Microsoft. Questi sono i requisiti di base per tutti i fornitori di Microsoft con accesso ai Dati Personali.

Inoltre, Microsoft ha predisposto addenda contrattuali specifici che incorporano il testo completo delle clausole per i fornitori con accesso ai Dati Personali inclusi nei Dati della Società e aggiungono tali clausole per tutti i fornitori con accesso ai Dati Personali dei Servizi Online diversi da quelli contenuti nei Dati della Società, al fine di garantire che i fornitori abbiano una visione completa di tutte le clausole previste. Tali addenda incorporeranno automaticamente eventuali clausole aggiuntive adottate o approvate dalla Commissione Europea a cui Microsoft aderisce.

L'ordinanza esecutiva 12.333 riguarda le attività di sorveglianza unilaterali del governo degli Stati Uniti condotte al di fuori degli Stati Uniti senza l'assistenza o la partecipazione dei fornitori di servizi statunitensi. Come dichiarato pubblicamente da Microsoft in precedenza, la società non fornisce dati dei clienti su base volontaria.

Microsoft utilizza protocolli di crittografia avanzati come barriera contro l'accesso non autorizzato ai dati dei clienti del settore pubblico e commerciale. L'utilizzo della crittografia da parte di Microsoft in relazione ai Servizi Online include:

- Crittografia dei Dati della Società per impostazione predefinita (inclusi eventuali Dati personali in essi contenuti) in transito su reti pubbliche tra il Cliente e Microsoft o tra i data center Microsoft.
- Crittografia dei Dati della Società archiviati a riposo nei Servizi Online.
- Nel caso di Servizi Online in cui il Cliente o una terza parte che agisce per conto del Cliente può creare applicazioni (ad esempio, alcuni servizi Azure), la crittografia dei dati archiviati in tali applicazioni può essere impiegata a discrezione del Cliente, utilizzando funzionalità fornite da Microsoft oppure ottenute dal Cliente tramite terze parti.

La corretta gestione delle chiavi è un altro elemento essenziale delle best practice di crittografia, Microsoft si impegna per garantire che tutte le chiavi di crittografia gestite da Microsoft siano adeguatamente protette. Nel Centro protezione Microsoft, vengono inoltre pubblicate informazioni di supporto rivolte ai clienti per consentire di gestire in autonomia valutazioni e pratiche di sicurezza.

Lo standard FIPS 140-2 e il successivo FIPS 140-3, anche noto come ISO/IEC 19790, specificano i requisiti di sicurezza per i moduli crittografici. I fornitori di prodotti ICT, tra cui Microsoft, includono moduli crittografici per la protezione dei dati degli utenti mediante crittografia avanzata. Questi moduli vengono convalidati da laboratori di terze parti indipendenti ai fini della conformità agli standard FIPS 140-2. Le nostre offerte cloud si basano su sistemi operativi sviluppati da Microsoft che contengono moduli di crittografia convalidati.

Per informazioni su Azure, vedi la pagina dedicata alle nozioni fondamentali sulla sicurezza di Azure. Leggi le pagine da 12 a 15 del documento sulla sicurezza di Azure per l'adozione del cloud del settore pubblico e trova informazioni più dettagliate nella pagina dedicata alla gestione delle chiavi di crittografia dei dati, alla crittografia dei dati in transito e a riposo. Per informazioni su Office 365, vedi la documentazione sulla crittografia di Office 365.

Di seguito vengono forniti maggiori dettagli su alcuni argomenti correlati alla crittografia.

Gestione delle chiavi di crittografia dei dati

Azure Key Vault offre funzionalità efficaci per il controllo della gestione dell'accesso ai dati. Azure Key Vault può essere usato per un'archiviazione sicura e un controllo rigoroso dell'accesso a token, password, certificati, chiavi API, chiavi di crittografia e altri segreti. Un segreto è una coppia costituita da identificatore-valore. Azure Key Vault consente di archiviare i segreti con il supporto di moduli di protezione hardware (HSM). I segreti e le chiavi possono essere protetti tramite software o HSM convalidati in base agli standard FIPS 140-2 Livello 2.

La centralizzazione dell'archiviazione dei segreti dell'applicazione in Azure Key Vault consente alle organizzazioni di controllarne la distribuzione. Key Vault riduce notevolmente le possibilità che i segreti possano essere divulgati accidentalmente. L'accesso a un insieme di credenziali delle chiavi richiede autenticazioni e autorizzazioni appropriate prima che un chiamante (utente o applicazione) possa ottenere l'accesso. L'autenticazione stabilisce l'identità del chiamante, l'autorizzazione determina le operazioni che è consentito eseguire. Per ulteriori informazioni sulle funzionalità di Azure Key Vault, è possibile consultare la documentazione del prodotto.

Crittografia in transito

La crittografia del trasporto riguarda la crittografia delle pipe di dati virtuali attraverso le quali transitano i messaggi e le informazioni tra un endpoint e i servizi Microsoft su reti private o Internet pubbliche. Una trasmissione senza crittografia del trasporto si può paragonare a una lettera imbucata nella cassetta della posta senza la protezione di una busta sigillata. La crittografia del trasporto viene implementata tramite standard internazionali consolidati. È importante che i clienti sostituiscano le versioni precedenti obsolete (TLS 1.0) con versioni più moderne (TLS 1.2+). Ulteriori informazioni sono disponibili nella documentazione di ingegneria della sicurezza Microsoft. Microsoft inoltre si impegna al massimo sfruttando funzionalità di analisi della sicurezza per garantire che venga utilizzata la "doppia crittografia in transito", un secondo livello di crittografia avanzata che interessa tutto il traffico che transita attraverso spazi di rete "non attendibili", ad esempio attraverso l'infrastruttura di rete pubblica. Grazie a questa funzionalità, nel caso sia presente una vulnerabilità nel "wrapper" esterno o si verifichi un'intercettazione, i singoli flussi non vengono compromessi.

Crittografia a riposo

Microsoft è conforme alle migliori pratiche del settore. La crittografia del disco consente di proteggere l'archiviazione dei dati nei data center cloud di Microsoft. In questo modo ci si può difendere dalla possibilità altamente improbabile che qualcuno ottenga l'accesso fisico a un dispositivo di archiviazione dati in un data center sicuro e acceda ai dati. Microsoft protegge i dati dei clienti abilitando almeno due livelli di crittografia. La doppia crittografia dei dati a riposo è mirata alla protezione dalle minacce interne provenienti dall'organizzazione del cliente o dal fornitore di servizi cloud. Azure consente di affrontare queste minacce attraverso controlli e livelli indipendenti di crittografia che assicurano la protezione dalla compromissione di qualsiasi livello di crittografia. L'approccio di Microsoft alla doppia crittografia a riposo è costituito da due livelli separati e distinti.

Il primo livello corrisponde alla crittografia a livello di infrastruttura in cui Microsoft fornisce e controlla le chiavi. La crittografia dell'infrastruttura viene implementata il più vicino possibile al dispositivo di archiviazione e/o al dispositivo di rete. Ciò garantisce che nessun dato venga mai archiviato o trasmesso in chiaro, proteggendo i dati da errori di implementazione, del cliente o dell'operatore ai livelli più alti dello stack di sistema.
Il secondo livello è costituito dalla crittografia a livello di servizio. Questo tipo di crittografia utilizza un proprio set di chiavi e si colloca tra la crittografia del disco e la crittografia di singoli documenti o e-mail. La crittografia a livello di servizio offre un ulteriore livello di sicurezza e conformità assicurando

che gli amministratori del sistema, con accesso ai volumi di archiviazione dei dati nel cloud che contengono anche i dati dei clienti, non abbiano accesso anche ai dati dell'applicazione stessa archiviati su quei volumi (ad esempio Exchange Online o SharePoint Online, due dei componenti chiave di Office 365). La crittografia a livello di servizio funziona solo sui dati a riposo, non in transito. Per crittografare singoli messaggi o file in transito oltre il TLS predefinito, i clienti possono scegliere un'opzione aggiuntiva come Azure Information Protection oppure Office Message Encryption.

Accesso ai dati

Microsoft utilizza meccanismi di accesso con privilegi minimi per controllare l'accesso ai Dati della Società (inclusi i Dati Personali in essi contenuti). I controlli di accesso basati sui ruoli vengono utilizzati per garantire che l'accesso ai Dati della Società richiesto per le operazioni di servizio sia per uno scopo appropriato, per un tempo limitato e approvato con la supervisione della direzione.

Rapporti sulla trasparenza

A dimostrazione del proprio impegno, Microsoft divulga un rapporto sulla trasparenza che include sia informazioni sulle richieste delle forze dell'ordine sia dati specifici sulle richieste delle autorità di sicurezza nazionali degli Stati Uniti. La legge degli Stati Uniti impone delle limitazioni rispetto alle informazioni che Microsoft è autorizzata a fornire sull'argomento, ma Microsoft rispetta rigorosamente tutte le normative relative alle richieste del governo correlate ai dati dei clienti. Microsoft è ricorsa cinque volte alle vie legali contro il governo degli Stati Uniti per contestare gli ordini che richiedevano l'accesso ai dati delle persone o per proteggere la nostra capacità di informare gli utenti sulle richieste pendenti, portando il caso alla Corte Suprema degli Stati Uniti. Grazie alle nostre azioni, abbiamo garantito maggiore trasparenza per i nostri Clienti, attraverso un accordo che ci ha permesso di divulgare i rapporti sul numero di ordini richiesti dalla sicurezza nazionale degli Stati Uniti. Oltre a stabilire nuove politiche all'interno del governo degli Stati Uniti che limitano l'uso di ordini di segretezza.

Portata delle politiche

Oltre al supporto continuo per i clienti che necessitano del flusso di dati attraverso l'Atlantico, Microsoft collaborerà in modo proattivo con la Commissione Europea, le autorità per la protezione dei dati e il governo degli Stati Uniti per affrontare le questioni sollevate dalla sentenza. Microsoft riconosce che la Corte di giustizia dell'Unione europea ha sollevato argomenti importanti che i governi devono tenere in considerazione nella definizione delle politiche correlate al trasferimento dei dati oltre confine. Microsoft si impegna a contribuire, come fatto finora, collaborando con governi e autorità di regolamentazione su entrambe le sponde dell'Atlantico per offrire un supporto concreto. Siamo consapevoli che i responsabili politici dell'UE e degli Stati Uniti stanno dedicando la massima attenzione alla risoluzione di questi problemi e apprezziamo che siano attivamente coinvolti.

È possibile trovare altre risorse sul GDPR nel Centro protezione, nonché report di controllo, informazioni dettagliate sulla sicurezza e altre informazioni correlate alla conformità nel Service Trust Portal.

Il team per la privacy di Microsoft (15/10/2020)