Gestione della conformità con i requisiti sul trasferimento dei dati dell'UE

7 settembre 2021

Avvisi

I clienti sono responsabili della propria valutazione autonoma delle informazioni contenute nel presente documento, il quale: (a) è solo a scopo informativo, (b) illustra le offerte e le pratiche attuali dei prodotti AWS soggette a modifiche senza preavviso, e (c) non crea alcun impegno o garanzia da parte di AWS e dei suoi affiliati, fornitori o licenziatari. I prodotti o servizi AWS sono forniti "così come sono" senza garanzie, dichiarazioni o condizioni di alcun tipo, sia esplicite che implicite. Le responsabilità e gli obblighi di AWS verso i propri clienti sono disciplinati dagli accordi AWS e il presente documento non costituisce né modifica alcun accordo tra AWS e i suoi clienti.

Sommario

Riassunto

Il presente documento fornisce informazioni riguardanti i servizi e le risorse che Amazon Web Services (AWS) offre ai clienti per aiutarli a condurre valutazioni sul trasferimento dei dati alla luce della sentenza "Schrems II" sui trasferimenti di dati personali disciplinati dal Regolamento generale sulla protezione dei dati e delle successive raccomandazioni del Comitato Europeo per la Protezione dei Dati. Il presente documento descrive inoltre le misure chiave supplementari adottate da AWS e messe a disposizione da AWS per proteggere i dati dei clienti.

Introduzione

AWS si impegna a far sì che i clienti usino tutti i servizi AWS in conformità con le regole sulla protezione dei dati dell'UE, tra cui il regolamento generale sulla protezione dei dati (General Data Protection Regulation - GDPR). Il presente documento descrive come i clienti AWS possono continuare a usare i servizi AWS in conformità con lo scenario in rapida evoluzione della protezione dei dati nell'UE in seguito alla sentenza Schrems II e alle successive raccomandazioni emesse dal Comitato Europeo per la Protezione dei Dati (CEPD). Le fasi esposte nel documento delineano la modalità con cui i clienti possono condurre valutazioni circa il proprio uso dei servizi AWS in conformità con la sentenza Schrems II e le raccomandazioni del CEPD e, di conseguenza, permettono ai clienti di adempiere alle regole sulla protezione dei dati prevista dall'UE.

Panoramica della sentenza Schrems II

Il 16 luglio 2020 la Corte di Giustizia dell'Unione Europea (CGUE) ha emesso una sentenza (denominata "Schrems II") circa il trasferimento dei dati personali disciplinati dal GDPR al di fuori dello Spazio Economico Europeo (SEE). Nella sentenza Schrems II, la CGUE ha stabilito che lo Scudo UE-USA per la privacy non rappresentava più un meccanismo valido per il trasferimento dei dati personali dal SEE agli Stati Uniti.

Tuttavia, nella medesima sentenza, la CGUE ha confermato che le organizzazioni possono (a patto di rispettare determinate condizioni riepilogate di seguito) continuare a usare le Clausole Contrattuali Standard (CCS) come meccanismo valido per il trasferimento dei dati personali al di fuori del SEE. La CGUE ha confermato che le organizzazioni che trasferiscono dati personali al di fuori del SEE (esportatori di dati) devono, in collaborazione con i destinatari di tali dati personali (importatori di dati), appurare se è presente un livello di protezione dei dati personali trasferiti essenzialmente equivalente a quello garantito nel SEE dal GDPR.

Gli esportatori di dati devono condurre tali valutazioni anche quando gli esportatori e gli importatori di dati usano le CCS come base per il trasferimento. Quando trasferiscono dati personali caricati nei servizi AWS dei loro account AWS (dati dei clienti) all'infuori del SEE, i clienti sono esportatori di dati e AWS è l'importatore di dati.

Con la sentenza Schrems II, la CGUE ha inoltre confermato che, a seconda della valutazione di cui sopra, AWS e i suoi clienti potrebbero dover adottare "misure supplementari" (oltre all'implementazione delle CCS) per garantire che vi sia un livello di protezione essenzialmente equivalente per i dati personali trasferiti verso paesi esterni al SEE.

Panoramica delle raccomandazioni del CEPD

Il CEPD, un ente che include rappresentanti delle autorità di protezione dei dati di tutti gli stati membri dell'UE, ha fornito esempi delle misure supplementari nel documento "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data" (Raccomandazioni del CEPD).

Le raccomandazioni del CEPD forniscono anche una guida per valutare se è presente un livello di protezione essenzialmente equivalente per i trasferimenti di dati al di fuori del SEE in seguito alla sentenza Schrems II. Le raccomandazioni del CEPD prevedono che gli esportatori di dati eseguano la seguente valutazione del trasferimento dei dati in sei fasi (la valutazione del trasferimento dei dati del CEPD):

- **Fase 1:** Eseguire una mappatura dei trasferimenti di dati internazionali e valutare se i dati trasferiti sono adeguati e limitati a quanto strettamente necessario.
- **Fase 2:** Verificare lo strumento usato per il trasferimento (per esempio i clienti si appoggiano alle CCS per trasferire i dati dei clienti).
- **Fase 3:** Esaminare le leggi o le prassi dei paesi terzi che possono ledere l'efficacia delle salvaguardie appropriate dello strumento di trasferimento, usando le Raccomandazioni 02/2020 relative alle garanzie essenziali europee per le misure di sorveglianza.
- **Fase 4:** Se dalla valutazione dell'esportatore di dati emerge che l'uso dello strumento di trasferimento da solo non fornirebbe un livello di protezione essenzialmente equivalente, identificare le misure contrattuali, tecniche o organizzative supplementari che sono necessarie per portare il livello di protezione dei dati trasferiti in modo sostanzialmente equivalente allo standard SEE.
- **Fase 5:** Adottare qualsiasi fase procedurale formale che possa essere richiesta da una o più delle misure supplementari.
- **Fase 6:** Rivalutare, a intervalli adeguati, il livello di protezione garantito ai dati che l'esportatore di dati trasferisce verso Paesi terzi e monitorare se vi sono stati o vi saranno sviluppi che possono condizionarlo.

Impatto della sentenza Schrems II e delle raccomandazioni del CEPD sull'uso dei servizi AWS

I clienti AWS possono continuare a usare i servizi AWS per il trasferimento dei dati dei clienti al di fuori del SEE in conformità con le leggi sulla protezione dei dati (incluso il

GDPR). AWS incorpora l'AWS GDPR Data Processing Addendum (AWS GDPR DPA) nelle condizioni del servizio AWS: ciò significa che l'AWS GDPR DPA viene applicato automaticamente a tutti i clienti che usano i servizi AWS per trattare i dati dei clienti soggetti al GDPR dove AWS è il responsabile del trattamento (come definito nel GDPR) di questi dati dei clienti.

La priorità assoluta di AWS è mettere in sicurezza i dati dei clienti. AWS implementa misure tecniche e organizzative rigorose per proteggerne la riservatezza, l'integrità e la disponibilità, a prescindere dalla regione AWS che il cliente ha selezionato.

AWS fornisce servizi e strumenti di cifratura avanzati che i clienti AWS possono usare per proteggere i dati dei clienti. I clienti AWS possono gestire le loro chiavi di cifratura attraverso una serie di soluzioni di cifratura native di AWS o di terza parte. AWS segue policy rigide quando si tratta di gestire le richieste di divulgazione da parte delle autorità e attraverso condizioni contrattuali rigorose si impegna a proteggere i dati dei clienti, come esposto in maggior dettaglio nella sezione Misure contrattuali del presente whitepaper.

AWS continuerà ad aggiornare le sue pratiche per soddisfare l'evolversi delle esigenze e delle aspettative di clienti e organi di regolamentazione, così come per ottemperare appieno a tutte le leggi vigenti in ogni Paese in cui opera.

Per maggiori informazioni si rimanda ai blog Customer update on the EU-US Privacy Shield e Customer update on strengthened commitments to protect customer data.

In caso di domande sul trasferimento di dati dei clienti verso e dal Regno Unito post-Brexit, consultare la pagina Web AWS and Brexit.

Mappatura dei trasferimenti dei dati dei clienti

La presente sezione aiuta a soddisfare la fase 1 della valutazione sul trasferimento dei dati del CEPD.

> **Fase 1:** Eseguire una mappatura dei trasferimenti di dati internazionali e valutare se i dati trasferiti sono adeguati e limitati a quanto strettamente necessario.

Parte contraente di AWS

Come descritto nel Contratto clienti AWS che disciplina l'uso dei servizi AWS da parte dei clienti AWS, la società europea AWS erogatrice di servizi (Amazon Web Services EMEA SARL), con sede in Lussemburgo, è la parte contraente di AWS che fornisce i servizi AWS ai clienti situati in Europa, nel Medio Oriente e in Africa (ad eccezione del

Sudafrica). In conformità con il Contratto clienti AWS, altri affiliati AWS forniscono i servizi AWS ai clienti situati fuori dall'Europa, dal Medio Oriente e dall'Africa.

Come i clienti possono trasferire i propri dati

In base all'AWS GDPR DPA, i clienti selezionano la regione AWS in cui archiviano i propri dati. I clienti troveranno una panoramica delle regioni AWS disponibili nel sito web Regioni e zone di disponibilità. In conformità con l'AWS GDPR DPA, AWS non trasferirà i dati dei clienti al di fuori della regione AWS selezionata dal cliente, tranne quando ciò è necessario per fornire i servizi AWS avviati dal cliente o quando ciò è necessario per adempiere alle leggi o a un ordine valido e vincolante da parte di un ente governativo.

Con AWS, i clienti sono in possesso dei propri dati, ne controllano la posizione e chi ne ha accesso. AWS è trasparente riguardo a come i servizi AWS trattano i dati dei clienti. Come illustrato nel sito web Caratteristiche di privacy dei servizi AWS, ogni cliente può usare i servizi AWS con la certezza che i dati dei clienti rimarranno nella regione AWS selezionata.

Un numero limitato di servizi AWS comporta il trasferimento di dati dei clienti, ad esempio perché il trasferimento è parte integrante del servizio AWS (come per un servizio di distribuzione di contenuti) oppure al fine di sviluppare e migliorare gli stessi servizi AWS; in quest'ultimo caso i clienti possono negare il consenso al trasferimento. AWS vieta, e i suoi sistemi sono progettati per impedirlo, l'accesso remoto ai dati dei clienti da parte del personale AWS per qualsiasi fine, tra cui la manutenzione del servizio a meno che: l'accesso non sia richiesto dai clienti, sia necessario per impedire frodi o l'uso illecito oppure sia richiesto per adempiere alle normative vigenti.

Per maggiori informazioni sull'approccio di AWS alla gestione delle richieste delle autorità, consulta le sezioni Valutazione delle leggi del Paese destinatario e Misure supplementari del presente whitepaper.

Trattamento secondario

È possibile determinare il luogo in cui i dati del cliente vengono trattati consultando il sito Web AWS Sub-responsabili di AWS, in cui AWS elenca i subappaltatori che ha incaricato per le attività di trattamento dei dati cliente per conto del cliente (sub-responsabili).

I sub-responsabili del trattamento relativi a un singolo cliente dipendono dalla regione AWS selezionata dal cliente e dai particolari servizi AWS che il cliente utilizza.

Esistono tre tipi di sub-responsabili del trattamento:

- Entità di AWS che forniscono l'infrastruttura sulla quale vengono eseguiti i

servizi AWS.

- Entità AWS che supportano servizi AWS specifici che potrebbero richiedere a queste entità di elaborare i dati dei clienti.
- Terze parti con cui AWS ha firmato un contratto per la fornitura di attività di trattamento per servizi AWS specifici.

AWS aggiorna il sito web dei sub-responsabili almeno 30 giorni prima di ingaggiare un nuovo sub-responsabile e, attraverso l'iscrizione alle notifiche sugli aggiornamenti, AWS invierà via e-mail l'avviso relativo alle modifiche al sito Web.

Strumento di trasferimento

La presente sezione aiuta a soddisfare la fase 2 della valutazione sul trasferimento dei dati del CEPD.

> **Fase 2:** Verificare lo strumento usato per il trasferimento (per esempio le CCS).

Laddove i clienti danno l'ordine ai servizi AWS di trasferire i dati dei clienti fuori dal SEE in conformità con la sezione Mappatura dei trasferimenti dei dati dei clienti del presente whitepaper, AWS usa le CCS per convalidare tali trasferimenti. Sia la sentenza Schrems II sia le raccomandazioni del CEPD confermano che le CCS sono un meccanismo valido per il trasferimento dei dati personali disciplinati dal GDPR al di fuori del SEE. I clienti AWS possono quindi continuare a fare affidamento sulle CCS incluse nell'AWS GDPR DPA per i trasferimenti dei dati dei clienti, in conformità con il GDPR.

Valutazione delle leggi e della prassi del Paese destinatario

La presente sezione aiuta a eseguire la fase 3 della valutazione sul trasferimento dei dati del CEPD.

> **Fase 3:** Esaminare le leggi o le prassi dei paesi terzi che possono ledere l'efficacia delle salvaguardie appropriate dello strumento di trasferimento, usando le Raccomandazioni 02/2020 relative alle garanzie essenziali europee per le misure di sorveglianza.

AWS permette di scegliere tra un insieme di servizi AWS on demand che possono essere forniti e configurati per la creazione di prodotti e offerte di servizi personalizzati. AWS offre il controllo completo sui dati dei clienti in qualsiasi momento, attraverso strumenti semplici ma efficaci che consentono di determinare dove vengono archiviati i dati dei clienti, nonché di proteggere i dati dei clienti in transito e a riposo. In questo modo si è nella posizione ideale per individuare le leggi che si applicano ai dati dei clienti, perché è possibile definire come, dove e perché vengono trattati i dati che si usano con i servizi AWS.

In caso di domande sulle leggi statunitensi in materia di sorveglianza, tra cui la sezione 702 del Foreign Intelligence Surveillance Act 1978 (FISA), è possibile consultare il whitepaper *Informazioni sulle salvaguardie della privacy negli Stati Uniti in relazione alle CCS e ad altre basi legali UE per i trasferimenti di dati UE-USA dopo la sentenza Schrems II* che il Dipartimento del commercio, il Dipartimento della giustizia e l'Ufficio del direttore dell'intelligence nazionale degli Stati Uniti hanno emesso congiuntamente nel settembre 2020, con i dettagli sui limiti e sulle salvaguardie relativi al loro accesso ai dati in risposta alla sentenza Schrems II (il "White Paper").

Il "White Paper" afferma che per molte aziende è improbabile che si manifesti il problema dell'accesso ai propri dati personali da parte della sicurezza nazionale, perché tali dati non sono di interesse per le autorità della sicurezza nazionale. Il "White Paper" dichiara che:

- Le aziende che gestiscono "informazioni commerciali ordinarie come i registri sui dipendenti, sui clienti o sulle vendite, non avrebbero motivo di credere che le autorità di intelligence statunitensi cercherebbero di raccogliere tali dati".
- "La possibilità teorica che un'autorità di intelligence statunitense possa accedere unilateralmente ai dati trasferiti dall'UE senza che l'azienda lo sappia non è diversa dalla possibilità teorica che le autorità di intelligence di altri governi, compresi quelli degli stati membri dell'UE, o un'entità privata che agisce illegalmente, possano accedere ai dati". Il "White Paper" indica anche che tale accesso ai dati potrebbe avvenire in qualsiasi luogo del mondo, non solo negli Stati Uniti.
- È previsto un indennizzo personale, anche per i cittadini dell'UE, nel caso di violazioni della sezione 702 del FISA mediante misure non contemplate dalla corte nella sentenza Schrems II, incluse le disposizioni FISA che permettono azioni private per varie forme di risarcimento.
- Alla sezione 702 del FISA sono state aggiunte alcune salvaguardie della privacy, tra cui gli emendamenti approvati nel 2018 che hanno introdotto: (i) procedure di interrogazione (in aggiunta alle procedure di identificazione degli obiettivi e di riduzione al minimo); (ii) disposizioni volte a migliorare la vigilanza del Privacy and Civil Liberties Oversight Board; (iii) requisiti dei garanti della privacy e delle

libertà civili per altre autorità competenti; (iv) maggiori protezioni dagli informatori anonimi per gli appaltatori; e (v) requisiti di trasparenza, tra cui disposizioni per la divulgazione del numero di obiettivi della sezione 702 del FISA.

A prescindere dalle leggi vigenti e dal Paese di provenienza, AWS esamina singolarmente e indipendentemente ogni richiesta di applicazione della legge. Amazon ha diversi precedenti di ricusa formale delle richieste governative in merito a informazioni dei clienti che ritiene troppo estese o altrimenti inappropriate. AWS continuerà a esaminare scrupolosamente tali richieste, comprese quelle che entrano in conflitto con le leggi locali come il GDPR, e a contestare laddove ne abbia validi motivi.

AWS inoltre adotta e mette a disposizione misure supplementari volte a supportare l'efficacia delle CCS, così come viene descritto nella sezione Misure supplementari del presente whitepaper. Tali misure supplementari includono l'appendice supplementare all'AWS GDPR DPA, in cui AWS si fa carico di obblighi contrattuali rafforzati per fare fronte alle richieste di applicazione della legge, come esposto in maggiore dettaglio nella sezione Misure contrattuali del presente whitepaper.

Le raccomandazioni del CEPD consentono inoltre ai clienti AWS di considerare l'esperienza pratica di AWS "con istanze precedenti rilevanti di richieste di accesso ricevute da autorità pubbliche" all'infuori del SEE.

Per aiutare i clienti a valutare tali richieste precedenti, nella pagina web Amazon Information Requests AWS pubblica regolarmente report sui tipi e il volume delle richieste di applicazione della legge che AWS riceve. I dati indicati nei report sulla richiesta di informazioni dimostrano che le divulgazioni dei dati dei clienti da parte di AWS in seguito a richieste di informazioni da parte delle autorità sono molto rare.

Misure supplementari

La presente sezione aiuta a eseguire le fasi 4, 5 e 6 della valutazione sul trasferimento dei dati del CEPD.

> **Fase 4:** Se le leggi o le prassi dei Paesi terzi implicano che l'uso dello strumento di trasferimento in sé non fornirebbe un livello di protezione essenzialmente equivalente, identificare le misure contrattuali, tecniche od organizzative supplementari che sono necessarie ad alzare il livello di protezione dei dati trasferiti allo standard SEE di essenziale equivalenza.
>
> **Fase 5:** Adottare qualsiasi fase procedurale formale che possa essere richiesta dalla misura supplementare.
>
> **Fase 6:** Rivalutare, a intervalli adeguati, il livello di protezione garantito ai dati che l'esportatore trasferisce verso Paesi terzi e monitorare se vi siano stati o vi saranno sviluppi che possano condizionarlo.

Le raccomandazioni del CEPD individuano una lista non esauriente di misure supplementari che AWS e i suoi clienti possono adottare, a seconda del risultato della valutazione sul trasferimento dei dati dei clienti descritta nella sezione Panoramica delle raccomandazioni del CEPD del presente whitepaper.

Tali misure supplementari rientrano nelle tre categorie di seguito riportate:

- ***Misure tecniche***, come la cifratura e l'utilizzo dei log
- ***Protezioni contrattuali***, tra cui obblighi riguardanti le richieste di applicazione della legge sui dati come quelli di cui AWS si fa carico nell'appendice supplementare di AWS
- ***Misure organizzative***, che consistono nelle policy e negli standard interni, in misure volte a ridurre al minimo la raccolta e la conservazione dei dati e nell'adozione di codici di condotta

La presente sezione illustra le misure chiave supplementari di tipo tecnico, contrattuale e organizzativo che AWS adotta e mette a disposizione per proteggere i dati dei clienti e supportare l'efficacia delle CCS. AWS continuerà ad aggiornare tale documento con l'evolversi delle sue misure supplementari.

Misure tecniche

Controllo da parte del cliente

Il cliente ha il pieno controllo sui dati dei clienti attraverso servizi e strumenti AWS semplici ma efficaci che permettono di determinare dove verranno archiviati i dati dei clienti, come verranno protetti e chi vi potrà accedere.

Modello di responsabilità condivisa

AWS adotta un Modello di responsabilità condivisa, che ripartisce le responsabilità di sicurezza e conformità tra AWS e i clienti a seconda della modalità di funzionamento dei servizi AWS e al grado di controllo dei servizi AWS di cui ogni parte dispone. Ai sensi del Modello di responsabilità condivisa, AWS ha la responsabilità di offrire infrastruttura e servizi sicuri (sicurezza "DEL" cloud), mentre i clienti hanno la responsabilità di progettare e proteggere le applicazioni e le soluzioni che decidono di implementare in AWS Cloud (sicurezza "NEL" cloud).

Per la sicurezza del cloud, AWS implementa controlli e processi sia tecnici che fisici responsabili e sofisticati, progettati per impedire l'accesso ai dati dei clienti e la divulgazione degli stessi senza autorizzazione (come testimoniato dal programma di conformità spiegato dettagliatamente nel sito Web AWS Programmi per la conformità).

Per la sicurezza nel cloud, AWS mette a disposizione prodotti, strumenti e servizi che si possono usare per progettare e proteggere le proprie applicazioni e soluzioni. AWS fornisce esempi di tali prodotti, strumenti e servizi chiave nella parte restante della presente sezione. Per maggiori informazioni su tali prodotti, strumenti e servizi, consultare AWS Well-Architected.

Cifratura

La cifratura (compresa la gestione delle chiavi di cifratura) è una misura chiave supplementare di tipo tecnico descritta nelle raccomandazioni del CEPD. AWS fornisce servizi e strumenti di cifratura avanzati che possono essere usati per proteggere i dati dei clienti.

È possibile gestire le proprie chiavi di cifratura con una serie di soluzioni di cifratura native di AWS o di terza parte. AWS Key Management Service (KMS), in quanto servizio gestito, semplifica la creazione e il controllo delle chiavi di crittografia e si avvale di Hardware Security Modules (HSM) con certificazione FIPS-140-2 per proteggere la sicurezza delle chiavi.

Tutte le richieste di uso delle chiavi in AWS KMS vengono registrate nei log di AWS

CloudTrail, affinché i clienti possano sapere chi ha usato quale chiave, in quale contesto e quando. I dati sugli eventi registrati nei log di AWS CloudTrail non possono essere modificati. AWS KMS è progettato in modo che né AWS (compresi i dipendenti di AWS) né fornitori di terze parti di AWS abbiano la possibilità di recuperare, consultare o divulgare le chiavi principali dei clienti in formato non cifrato.

Sistema AWS Nitro

Il sistema AWS Nitro è la piattaforma sottostante di tutte le istanze Amazon Elastic Compute Cloud (Amazon EC2) più recenti e fornisce maggiore riservatezza e privacy alle applicazioni dei clienti. Attraverso l'uso di hardware, firmware e software appositamente progettati, il sistema AWS Nitro offre un livello di sicurezza e isolamento unico all'avanguardia nel settore dato che le funzioni di virtualizzazione, come l'archiviazione e le reti, sono affidate ad hardware dedicato e relativo firmware.

Il sistema AWS Nitro è inoltre progettato per non permettere l'accesso da parte degli operatori di AWS. Con il sistema AWS Nitro, non esiste alcun meccanismo che permetta a sistemi o persone di accedere ai server EC2 (l'infrastruttura host sottostante), leggere la memoria delle istanze EC2 o accedere a qualsiasi dato archiviato nell'*instance store* e nei volumi di Amazon Elastic Block Store (Amazon EBS) cifrati.

Misure contrattuali

AWS GDPR DPA

Nell'AWS GDPR DPA, AWS assume impegni contrattuali circa le misure che adotta e mette a disposizione per proteggere i dati dei clienti. Per esempio, AWS si impegna contrattualmente a:

(i) Implementare misure tecniche per proteggere la rete AWS

(ii) Assistere i clienti nell'adempiere agli obblighi in materia di sicurezza ai sensi del GDPR offrendo strumenti e funzionalità

(iii) Fornire certificazioni di terze parti e report di audit in modo che i clienti possano controllare la conformità di AWS all'AWS GDPR DPA

Addendum

AWS ha pubblicato un addendum all'AWS GDPR DPA che elenca gli impegni contrattuali a cui i clienti possono ricorrere come misure contrattuali supplementari in conformità alle raccomandazioni del CEPD. Nell'accordo supplementare, AWS si impegna a:

(i) Compiere ogni tentativo ragionevole per reindirizzare qualsiasi autorità

richiedente dati dei clienti verso il cliente interessato

(ii) Notificare prontamente il cliente interessato circa la richiesta, se legalmente autorizzata a farlo

(iii) Ricusare eventuali richieste eccessivamente ampie o inappropriate, compresi i casi in cui la richiesta entra in conflitto con le norme UE

Inoltre, qualora AWS fosse comunque obbligata a divulgare i dati dei clienti dopo aver esaurito i passaggi precedenti, AWS si impegna a divulgarne soltanto la quantità minima necessaria a soddisfare la richiesta.

Per supportare i clienti nella valutazione delle leggi dei paesi destinatari (si veda Valutazione delle leggi e della prassi del paese destinatario nel presente whitepaper), AWS garantisce di non aver alcun motivo di credere che la legislazione applicabile ad AWS o ai suoi responsabili secondari del trattamento , tra cui in qualsiasi paese verso cui i dati dei clienti vengono trasferiti, impedisca ad AWS di adempiere ai suoi obblighi ai sensi dell'AWS GDPR DPA o dell'appendice supplementare.

AWS si impegna inoltre a notificare prontamente qualsiasi modifica nella legislazione che ritenga possa avere un probabile impatto sostanziale sull'adempimento dei propri obblighi. Per maggiori informazioni si rimanda a AWS and EU data transfers: strengthened commitments to protect customer data (AWS e il trasferimento dei dati EU: rafforzare l'impegno nella protezione dei dati dei clienti).

Misure organizzative

Processi

AWS si avvale di processi interni per gestire le richieste da parte delle pubbliche autorità dei dati dei clienti e, a prescindere dalla fonte della richiesta o delle leggi applicabili, AWS esamina singolarmente ed indipendentemente ogni richiesta in conformità con le proprie linee guida e gli obblighi previsti dall'addendum supplementare di AWS. AWS limita rigorosamente, o rifiuta completamente, le richieste delle forze dell'ordine riguardanti i dati dei clienti provenienti da qualsiasi paese, inclusi gli Stati Uniti, laddove siano eccessivamente ampie o se AWS ha validi motivi per farlo.

Report sulle richieste di informazioni

AWS è consapevole dell'importanza rivestita dalla trasparenza per i suoi clienti e di conseguenza sulla pagina web Law Enforcement Information Requests pubblica regolarmente un report sulle richieste di informazioni (Information Request Report, IRR) sui tipi e sulla numerosità delle richieste che riceve da parte delle autorità pubbliche. A partire dal report luglio-dicembre 2020, AWS ha avviato un nuovo

formato IRR come misura organizzativa supplementare che offre maggiori informazioni sui tipi di richieste delle autorità pubbliche che AWS riceve e sul paese di origine delle stesse.

Per usare il nuovo formato IRR, si veda Amazon Information Request Report. Le informazioni indicate negli IRR dimostrano che le divulgazioni dei dati dei clienti da parte di AWS in seguito a richieste di informazioni da parte delle autorità sono molto rare.

Risorse aggiuntive

Per comprendere meglio come destreggiarsi con i requisiti in materia di privacy e protezione dei dati, invitiamo a leggere i whitepaper su sicurezza, rischio e conformità, nonché gli elenchi di controllo, le linee guida e le best practice pubblicati sul sito Web di AWS. Tale materiale è disponibile nei siti Web Conformità di AWS e Sicurezza in AWS Cloud.

Versioni del documento

Data	Descrizione
7 settembre 2021	Prima pubblicazione