

DPIA Whistleblowing	Fornitore piattaforma
----------------------------	------------------------------

Software: BigBlue Eye
Titolare del trattamento: BigBlue srl
La presente DPIA si compone di: 20 pagine
Rev 2.0 del 1 marzo 2024

AUTORE:	BigBlue Srl
REVISORE:	Provedel Fabio
VALIDATORE:	Bertelli Stefano
STATO:	Validata il: 11 febbraio 2024

Premessa

Ai sensi dell'art. 35 del Regolamento UE n. 2016/679 (in seguito anche "GDPR"), la DPIA corrisponde alla valutazione d'impatto del trattamento del dato sulla protezione dei dati personali, qualora il trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Ciò considerata la natura, il contesto e le finalità del trattamento.

Il GDPR introduce dunque una valutazione di stampo preliminare, che consente al Titolare del trattamento di prendere visione del rischio prima ancora di procedere al trattamento e di attivarsi perché tale rischio possa essere, se non annullato, quantomeno fortemente ridotto.

I principi fondamentali della DPIA risultano pertanto:

- i diritti e le libertà fondamentali dell'interessato, punto cardine dell'intero impianto del GDPR;
- la gestione dei rischi per la privacy, attraverso le misure tecniche ed organizzative di volta in volta adeguate rispetto al rischio.

Una DPIA poggia su due pilastri:

- i principi e i diritti fondamentali, i quali sono "non negoziabili", stabiliti dalla legge e che devono essere rispettati e non possono essere soggetti ad alcuna variazione, indipendentemente dalla natura, gravità e probabilità dei rischi;
- la gestione dei rischi per la privacy dei soggetti interessati, che determina i controlli tecnici e organizzativi opportuni a tutela dei dati personali.

La Metodologia di analisi dei rischi adottata nella conduzione delle attività di Data Privacy Impact Assessment è la metodologia di analisi CNIL del Garante Francese.

Standard applicabili al trattamento

Al trattamento in materia di segnalazioni e normativa whistleblowing si applicano le seguenti normative e standard.

- Regolamento UE n. 2016/679 (c.d. GDPR)
- D.lgs. n. 196/2003 (c.d. Codice Privacy) così come modificato dal D.lgs. n. 101/2018
- Direttiva UE 1937/2019
- D.lgs. n. 24/2023

Dati, processi e risorse di supporto

Di seguito si riportano le tipologie di dati personali che sono oggetto di trattamento a seguito di una segnalazione fatta ai sensi del D.lgs. n. 24/2023

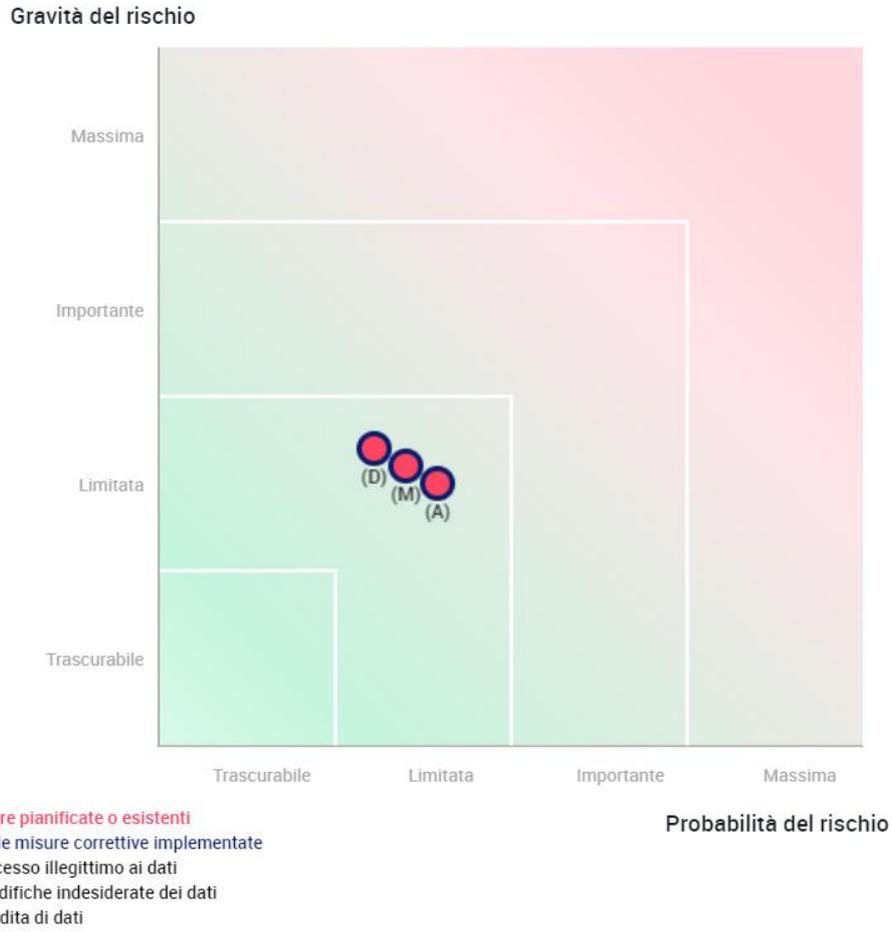
Categoria di dato personale	Categoria di interessato
Dati personali comuni e di contatto	dipendenti e collaboratori che effettuano una segnalazione o che ne sono oggetto. Fornitori che effettuano una segnalazione o vengono segnalati
Dati personali particolari (es. dati relativi alla salute, dati relativi all'appartenenza sindacale)	Dipendenti e collaboratori che effettuano una segnalazione o che ne sono oggetto. Fornitori che effettuano una segnalazione o vengono segnalati.

Dati giudiziari (es. condanne penali)	Dipendenti e collaboratori che effettuano una segnalazione o che ne sono oggetto Fornitori che effettuano una segnalazione o vengono segnalati
---------------------------------------	--

Ciclo di vita del trattamento dei dati (descrizione funzionale)

- Attivazione e configurazione della piattaforma
- Utilizzo della piattaforma - invio delle segnalazioni da parte dei segnalanti e accesso alle stesse da parte dei soggetti autorizzati
- Dismissione della piattaforma (termini contrattuali o di legge) con conseguente cancellazione sicura dei dati da parte del fornitore/provider del servizio.

Validazione: Mappatura dei rischi



Validazione: Piano d'azione

Panoramica

Principi fondamentali		Misure esistenti o pianificate	
Finalità	<input type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input checked="" type="checkbox"/>	Crittografia
Basi legali	<input type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input checked="" type="checkbox"/>	Controllo degli accessi fisici
Adeguatezza dei dati	<input type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input checked="" type="checkbox"/>	Controllo degli accessi logici
Esattezza dei dati	<input type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input checked="" type="checkbox"/>	Controllo dell'accesso ai dati
Periodo di conservazione	<input type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input checked="" type="checkbox"/>	Partizionamento
Informativa	<input type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input checked="" type="checkbox"/>	Controllo del trasferimento dei dati
Raccolta del consenso	<input type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input checked="" type="checkbox"/>	Tracciabilità/Controllo dell'inserimento dei dati
Diritto di accesso e diritto alla portabilità dei dati	<input type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input checked="" type="checkbox"/>	Protezione contro fonti di rischio non umane
Diritto di rettifica e diritto di cancellazione	<input type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input checked="" type="checkbox"/>	Backup
Diritto di limitazione e diritto di opposizione	<input type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input checked="" type="checkbox"/>	Contratto con il responsabile del trattamento
Responsabili del trattamento	<input type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input checked="" type="checkbox"/>	Gestione delle politiche di tutela della privacy
Trasferimenti di dati	<input type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input checked="" type="checkbox"/>	Gestire gli incidenti di sicurezza e le violazioni dei dati personali
		<input type="checkbox"/> <input checked="" type="checkbox"/>	Tracciabilità
		<input type="checkbox"/> <input checked="" type="checkbox"/>	Vulnerabilità
		<input type="checkbox"/> <input checked="" type="checkbox"/>	Manutenzione
		<input type="checkbox"/> <input checked="" type="checkbox"/>	Sicurezza dei canali informatici
		<input type="checkbox"/> <input checked="" type="checkbox"/>	Lotta contro il malware
		<input type="checkbox"/> <input checked="" type="checkbox"/>	Politica di tutela della privacy
		<input type="checkbox"/> <input checked="" type="checkbox"/>	Gestione dei rischi
			Rischi
		<input type="checkbox"/> <input checked="" type="checkbox"/>	Accesso illegittimo ai dati
		<input type="checkbox"/> <input checked="" type="checkbox"/>	Modifiche indesiderate dei dati
		<input type="checkbox"/> <input checked="" type="checkbox"/>	Perdita di dati

Misure Migliorabili
Misure Accettabili

Principi fondamentali
Nessun piano d'azione registrato.
Misure esistenti o pianificate
Nessun piano d'azione registrato.
Rischi
Nessun piano d'azione registrato.

Validazione: DPO e parere degli interessati

Nome del DPO/RPD:
Alla luce delle disposizioni dell'art. 37 del Regolamento privacy europeo, il Titolare non ha ritenuto obbligatorio procedere alla designazione della figura del Responsabile della protezione dei dati personali (RPD).
Posizione del DPO/RPD:
N/A
Parere del DPO/RPD:
N/A
Richiesta del parere degli interessati:
Non è stato chiesto il parere degli interessati.
Motivazione della mancata richiesta del parere degli interessati
La piattaforma risponde ad una norma di legge e quindi non è richiesto il parere degli interessati.

Contesto: Panoramica del trattamento

Quale è il trattamento in considerazione?

Sviluppo, fornitura e manutenzione di una piattaforma online per la gestione delle segnalazioni whistleblowing ai sensi della normativa Whistleblowing (D.Lgs 24 del 10 Marzo 2023 attuativo della Direttiva UE 2019/1937) riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione.

La piattaforma si chiama **BigBlue Eye**, sviluppata da BigBlue Srl ed ha le seguenti caratteristiche tecniche:

ARCHITETTURA DI SISTEMA: Web application in php caricata su AWS (Amazon Web Services).

Salva e legge i dati su database MySql sempre su AWS.

SOFTWARE IMPIEGATO: WebSmart, php v. 8.2, database MySql

ARCHITETTURA DI RETE: AWS (Amazon Web Services)

Per una descrizione più dettagliata si veda il documento allegato "brochure...pdf"

Quali sono le responsabilità connesse al trattamento?

Il fornitore garantisce che la piattaforma sviluppata assicura il rispetto degli obblighi di riservatezza nei riguardi del segnalante, della persona coinvolta, di chi è menzionato nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione.

Il trattamento riguardante il whistleblowing è attuato in conformità alle normative applicabili a protezione dei dati personali (Reg. 2018/1725 per la privacy riguardo alle istituzioni UE, Reg. UE 2016/679, D. Lgs 196/2003, D.Lgs 101/2018 e il D.Lgs 51/2018 per il trattamento di finalità di polizia).

Ci sono standard applicabili al trattamento?

La piattaforma **BigBlue Eye** è resa disponibile su server virtuale ospitato su AWS. AWS dispone di certificazioni di conformità ai sensi degli standard ISO/IEC 27001:2022, 27017:2015, 27018:2019, 27701:2019, 22301:2019, 20000-1:2018, 9001:2015, e CSA STAR CCM v4.0.

Le certificazioni sono disponibili ed aggiornate a questo link:
<https://aws.amazon.com/it/compliance/iso-certified/>

Valutazione: Accettabile

Commento di valutazione:

Le informazioni fornite sono esaurienti e dettagliate.
I fornitori applicano standard che garantiscono i principi di accountability e sicurezza dei dati.

Contesto:

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Dati personali di dipendenti, clienti, fornitori e collaboratori che effettuano una segnalazione o che ne sono oggetto.

I dati possono essere anche particolari e/o giudiziari in base al contenuto della segnalazione.

I dati sono conservati per cinque anni a partire dalla data di comunicazione dell'esito finale della procedura di segnalazione, come espressamente previsto dall'articolo 14 del D. lgs. 24/2023.

Nel caso in cui sia instaurato un giudizio, tale termine si prolunga fino alla conclusione del giudizio stesso.

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

I dati sono raccolti quando viene aperta una segnalazione.

Successivamente sono utilizzati dalle persone autorizzate per gestire le segnalazioni.

Dopo che è stato fornito l'esito finale della segnalazione i dati sono conservati per il periodo stabilito dalla norma.

La piattaforma gestisce (per ogni cliente) un utente amministratore che a sua volta può creare e gestire gli utenti che hanno accesso alle segnalazioni.

Quali sono le risorse di supporto ai dati?

I dati sono ospitati sulla piattaforma BigBlue Eye. Per il dettaglio si veda il documento allegato "brochure..pdf".

Valutazione: Accettabile

Commento di valutazione:

Le informazioni fornite sono esaurienti e dettagliate. Le modalità di trattamento ed i dati utilizzati sono pertinenti.

Principi Fondamentali Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Il trattamento è finalizzato esclusivamente allo sviluppo, fornitura e manutenzione della piattaforma BigBlue Eye per la gestione delle segnalazioni e all'adempimento degli obblighi legali previsti dalla normativa vigente in materia di whistleblowing.

Valutazione: Accettabile

Commento di valutazione:

I dati raccolti e le procedure di gestione sono adeguati e pertinenti nel rispetto delle norme in essere.

Quali sono le basi legali che rendono lecito il trattamento?

Il trattamento si fonda sulla base giuridica dell'adempimento di un obbligo di legge a cui sono tenuti i clienti della piattaforma (Art. 6.1. lett. c) GDPR).

Il trattamento si basa inoltre sulla esecuzione di un contratto tra fornitore della piattaforma e cliente (Art, 6.1 lett. b).

Valutazione: Accettabile

Commento di valutazione:

I dati raccolti e le procedure di gestione sono adeguati e pertinenti nel rispetto delle norme in essere.

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

I dati personali raccolti per le segnalazioni sono solo quelli espressamente necessari alla gestione della segnalazione, come normativamente previsto dall'articolo 12 del D.lgs. n. 24/2023. Il perseguimento delle finalità avviene nel rispetto del principio di minimizzazione (art. 5.1. lett. c) GDPR).

I dati personali raccolti per la registrazione e gestione degli utenti utilizzatori, sono: cognome, nome, e-mail, nome ditta e numero di cellulare.

Valutazione: Accettabile

Commento di valutazione:

I dati raccolti e le procedure di gestione sono adeguati e pertinenti nel rispetto delle norme in essere.

I dati sono esatti e aggiornati?

I dati personali relativi alle segnalazioni e agli utenti utilizzatori sono in carico ai clienti che utilizzano la piattaforma.

Valutazione: Accettabile

Commento di valutazione:

I dati raccolti e le procedure di gestione sono adeguati e pertinenti nel rispetto delle norme in essere.

Qual è il periodo di conservazione dei dati?

Le segnalazioni e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni, che decorrono dalla data di comunicazione dell'esito finale della procedura di segnalazione, come espressamente previsto dall'articolo 14 del D.lgs. n. 24/2023.

Nel caso in cui sia instaurato un giudizio, tale termine si prolunga fino alla conclusione del giudizio stesso.

Gli account disabilitati sono eliminati solo quando non ci sono più segnalazioni collegate a tale account.

Valutazione: Accettabile

Commento di valutazione:

I dati raccolti e le procedure di gestione sono adeguati e pertinenti nel rispetto delle norme in essere.

Principi Fondamentali

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Gli interessati (cioè i clienti fruitori della piattaforma) sono informati attraverso una specifica informativa resa ai sensi degli artt. 13-14 GDPR.

Valutazione: Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

Il trattamento non prevede il consenso degli interessati (clienti fruitori della piattaforma) in quanto è necessario all'esecuzione di un contratto (Art. 6.1 lett. b).

Valutazione: Accettabile

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

I clienti fruitori della piattaforma possono esercitare i diritti previsti dagli artt. 15 ss. del GDPR attraverso l'indirizzo di posta elettronica dedicato nei limiti di cui all'articolo 2-undecies del Codice

Privacy.

La portabilità è prevista nelle clausole contrattuali di recesso.

Valutazione: Accettabile

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

I clienti fruitori della piattaforma possono esercitare i diritti previsti dagli artt. 15 ss. del GDPR attraverso l'indirizzo di posta elettronica dedicato nei limiti di cui all'articolo 2-undecies del Codice Privacy.

Valutazione: Accettabile

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

I clienti fruitori della piattaforma possono esercitare i diritti previsti dagli artt. 15 ss. del GDPR attraverso l'indirizzo di posta elettronica dedicato nei limiti di cui all'articolo 2-undecies del Codice Privacy.

Valutazione: Accettabile

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

Le terze parti che trattano dati personali per conto del Titolare sono state nominate Responsabili del trattamento ai sensi dell'art. 28 GDPR, attraverso contratti o altri atti giuridici. Si veda la Nomina a Responsabile per AWS allegata "aws-dpa.pdf".

Valutazione: Accettabile

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

Per questa tipologia di trattamento non è previsto un trasferimento di dati personali al di fuori dello Spazio Economico Europeo (SEE).

Valutazione: Accettabile

Rischi
Misure esistenti o pianificate

Crittografia

Il contenuto della segnalazione viene trasmesso in forma criptata con protocollo HTTPS. Crittografia statica dei dati su database SQL.

Valutazione: Accettabile

Controllo degli accessi fisici

Per il dettaglio dei controlli effettuati da AWS si veda il link seguente:
<https://aws.amazon.com/it/compliance/shared-responsibility-model/>

Valutazione: Accettabile

Controllo degli accessi logici

Profili utente amministratore (lato cliente) che visualizzano e possono gestire le segnalazioni a loro assegnate.

Ogni profilo utente ha assegnata una tipologia di segnalazione.

Gli utenti di un cliente possono vedere solo i dati di loro competenza.

I profili utente amministratore accedono al sistema con l'e-mail e una password (lunga almeno 8 caratteri, almeno 1 lettera maiuscola, almeno 1 minuscola, almeno un numero e un carattere speciale).

Le segnalazioni sono effettuate in forma anonima o confidenziale. Per le segnalazioni confidenziali viene richiesto nome, cognome e un numero di cellulare per l'autenticazione tramite codice OTP ricevuto sul numero di telefono.

Ogni segnalante può verificare lo stato della segnalazione con una chiave univoca criptata che gli viene comunicata al momento di apertura della segnalazione. Ogni segnalazione ha associata una chiave univoca.

Il fornitore BigBlue Srl ha l'accesso amministrativo al back office per tutti i servizi di manutenzione, aggiornamento ed implementazione. L'accesso avviene su connessione crittografata con credenziali di accesso.

Valutazione: Accettabile

Controllo dell'accesso ai dati

Le seguenti misure sono state implementate per garantire che i dati personali possano essere accessibili solo in conformità con le autorizzazioni assegnate. Inoltre, è garantito che i dati personali non possono essere elaborati senza autorizzazione, cioè non possono essere registrati, letti, copiati, modificati o cancellati senza autorizzazione:

- Concetto di autorizzazione con assegnazione di autorizzazione differenziata
- Gestione dei diritti degli utenti da parte degli amministratori
- Identificazione e autenticazione dell'utente
- Regole di autorizzazione e di accesso
- Crittografia in movimento e a riposo
- Utilizzo di OTP

Valutazione: Accettabile

Partizionamento

Le seguenti misure sono state implementate per garantire che i dati raccolti per scopi diversi siano trattati separatamente:

- Separazione dell'ambiente produttivo e di prova/sviluppo
- Concetto di autorizzazione per l'accesso ai dati

- Configurazioni software sicure
- Nessuna elaborazione di dati produttivi in ambiente di test
- Separazione dei clienti (separazione logica)
- I dati dei clienti sono trattati solo per gli scopi definiti contrattualmente
- Crittografia

Valutazione: Accettabile

Controllo del trasferimento dei dati

Vengono implementate le seguenti misure di integrità dei dati, che in generale aiutano a proteggere contro l'elaborazione non autorizzata o illegale, la distruzione o il danneggiamento accidentale:

- Connessioni criptate per la trasmissione di dati
- Processo di gestione delle chiavi e degli accessi
- Autenticazione a più fattori
- Assenza di funzioni lato cliente per l'esportazione dei dati

Valutazione: Accettabile

Tracciabilità/Controllo dell'inserimento dei dati

Le seguenti misure sono state implementate per garantire che sia possibile verificare da chi sono stati inseriti, modificati o rimossi i dati personali:

- Registrazione logica dell'inserimento, della modifica e della cancellazione dei dati
- Assegnazione di diritti per gestire le segnalazioni
- Tracciabilità di input, modifiche, cancellazioni attraverso nomi utente individuali

Valutazione: Accettabile

Protezione contro fonti di rischio non umane

Per il dettaglio delle misure messe in atto da AWS si veda il link seguente:
<https://aws.amazon.com/it/compliance/shared-responsibility-model/>

Valutazione: Accettabile

Backup

Giornaliero dei dati del database SQL su AWS.

Valutazione: Accettabile

Contratto con il responsabile del trattamento

Il titolare ha provveduto a nominare Responsabile del Trattamento AWS.
Si vedano i documenti allegati "aws-dpa.pdf" e "aws-gdpr-compliance.pdf".

Valutazione: Accettabile

Gestione delle politiche di tutela della privacy

Il Titolare del Trattamento (bigBlue Srl) applica le seguenti procedure per la protezione dei dati:

- Formazione regolare dei dipendenti e impegno di tutti i dipendenti alla riservatezza
- Privacy per impostazione predefinita
- Politica aziendale sulla protezione dei dati
- Se necessario, attuazione della valutazione d'impatto sulla protezione dei dati secondo l'art. 35 GDPR UE

Valutazione: Accettabile

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

Possibilità di ripristino di eventuali dati persi o corrotti grazie al backup del database automatizzato. I dati sensibili sono criptati a database.

Certificazione con codice OTP e data certa per ogni attività effettuata.

Valutazione: Accettabile

Tracciabilità

Meccanismo di certificazione tramite token OTP per le segnalazioni confidenziali.

In questo modo le segnalazioni sono certificate con Nome, Cognome e numero di cellulare e si può constatare l'autenticità della segnalazione.

Ogni evento o attività (come il momento di presa in carico della segnalazione ad esempio) viene certificato, inoltre, da data certa con un certificato virtuale garantendo in questo modo certezza sui processi e sui tempi.

I dati sono conservati seguendo le tempistiche di conservazione delle segnalazioni.

Valutazione: Accettabile

Vulnerabilità

Documentazione delle procedure operative, formazione sull'utilizzo dello strumento, aggiornamento di software applicativo, di sistema e di sviluppo e dell'hardware.

Valutazione: Accettabile

Manutenzione

Manutenzione periodica del software php e database MySql nel rispetto delle regole imposte da AWS.

Valutazione: Accettabile

Sicurezza dei canali informatici

L'applicazione è installata su AWS.

I dati delle segnalazioni sono criptati in modo statico con chiave esadecimale.

La trasmissione dei dati avviene con protocollo HTTPS.

Valutazione: Accettabile

Lotta contro il malware

Conforme alle regole imposte da AWS.

Valutazione: Accettabile

Politica di tutela della privacy

Gestione del personale con autorizzazione al trattamento dei dati personali attraverso la creazione di profili utente "Amministratori".

Formazione sull'utilizzo del programma.

Valutazione: Accettabile

Gestione dei rischi

Dati salvati su AWS, procedure di backup e ripristino.

Accesso ai dati sensibili con password univoca e criptata.

Vedasi registro dei trattamenti ed analisi dei rischi effettuata.

Valutazione: Accettabile

Rischi

Accesso illegittimo ai dati

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Ritorsione sul segnalante, Perdita di dati, Perdita della reputazione del segnalato senza aver potuto dimostrare l'eventuale estraneità ai fatti addebitategli, Perdita della reputazione del segnalato senza la possibilità di addurre prove a supporto dell'innocenza della propria condotta., Violazione dati personali, Perdita della reputazione, Violazione della riservatezza del segnalante

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Accessi illeciti, Minacce relative all'anonimato e alla riservatezza, Misure di sicurezza non adeguate

Quali sono le fonti di rischio?

Hacker, Virus informatici, Comportamento degli utenti, Cronologia e cache del browser

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Crittografia, Controllo degli accessi logici, Controllo dell'accesso ai dati, Partizionamento, Tracciabilità/Controllo dell'inserimento dei dati, Controllo del trasferimento dei dati, Controllo degli accessi fisici, Contratto con il responsabile del trattamento, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Tracciabilità, Sicurezza dei canali informatici, Politica di tutela della privacy, Gestione dei rischi, Lotta contro il malware, Gestione delle politiche di tutela della privacy, Vulnerabilità, Manutenzione

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Limitata, Le misure di sicurezza messe in atto forniscono un livello di protezione adeguato contro i rischi individuati.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Limitata, Le misure di sicurezza messe in atto forniscono un livello di protezione adeguato contro i rischi individuati.

Valutazione: Accettabile

Rischi
Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Perdita della reputazione, Violazione della riservatezza del segnalante, Perdita della reputazione del segnalato senza aver potuto dimostrare l'eventuale estraneità ai fatti addebitategli, Perdita della reputazione del segnalato senza la possibilità di addurre prove a supporto dell'innocenza della propria condotta., Perdita di dati, Ritorsione sul segnalante, Violazione dati personali

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Accessi illeciti, Misure di sicurezza non adeguate, Minacce relative all'anonimato e alla riservatezza

Quali sono le fonti di rischio?

Hacker, Virus informatici, Cronologia e cache del browser, Comportamento degli utenti

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Crittografia, Controllo degli accessi fisici, Controllo degli accessi logici, Controllo dell'accesso ai dati, Partizionamento, Controllo del trasferimento dei dati, Tracciabilità/Controllo dell'inserimento dei dati, Protezione contro fonti di rischio non umane, Backup, Contratto con il responsabile del trattamento, Gestione delle politiche di tutela della privacy, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Tracciabilità, Vulnerabilità, Manutenzione, Sicurezza dei canali informatici, Lotta contro il malware, Politica di tutela della privacy, Gestione dei rischi

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?

Limitata, Le misure di sicurezza messe in atto forniscono un livello di protezione adeguato contro i rischi individuati.

Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?

Limitata, Le misure di sicurezza messe in atto forniscono un livello di protezione adeguato contro i rischi individuati.

Valutazione: Accettabile

Rischi **Perdita di dati**

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

Perdita di dati, Ritorsione sul segnalante, Violazione dati personali, Perdita della reputazione del segnalato senza la possibilità di addurre prove a supporto dell'innocenza della propria condotta., Perdita della reputazione, Perdita della reputazione del segnalato senza aver potuto dimostrare l'eventuale estraneità ai fatti addebitategli.

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

Accessi illeciti, Misure di sicurezza non adeguate

Quali sono le fonti di rischio?

Hacker, Virus informatici, Comportamento degli utenti, Cronologia e cache del browser

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Controllo degli accessi fisici, Controllo degli accessi logici, Controllo dell'accesso ai dati, Partizionamento, Controllo del trasferimento dei dati, Tracciabilità/Controllo dell'inserimento dei dati, Protezione contro fonti di rischio non umane, Backup, Sicurezza dei canali informatici, Gestione dei rischi, Lotta contro il malware

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Limitata, Le misure di sicurezza messe in atto forniscono un livello di protezione adeguato contro i rischi individuati.

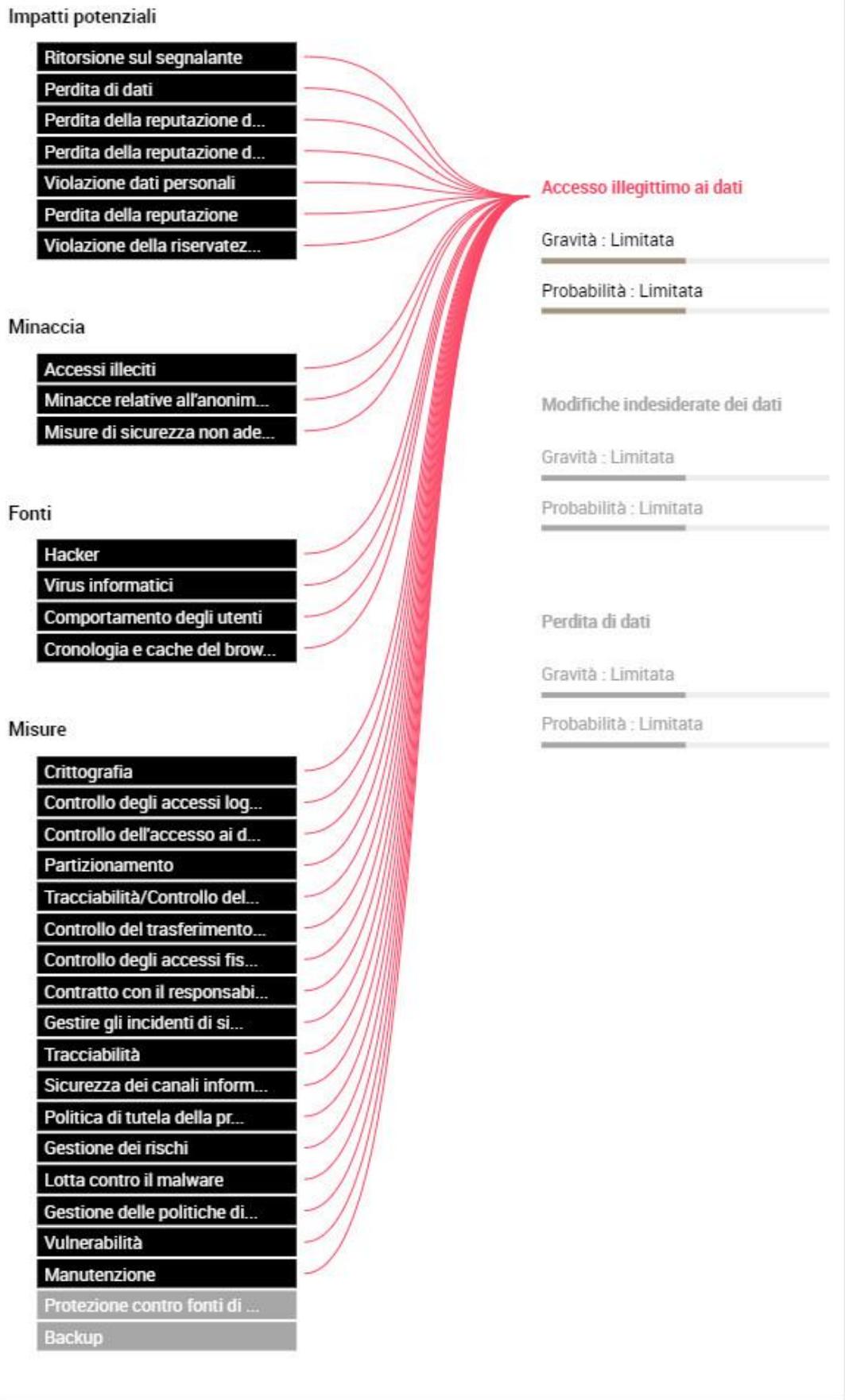
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Limitata, Le misure di sicurezza messe in atto forniscono un livello di protezione adeguato contro i rischi individuati.

Valutazione: Accettabile

Rischi **Panoramica dei rischi**

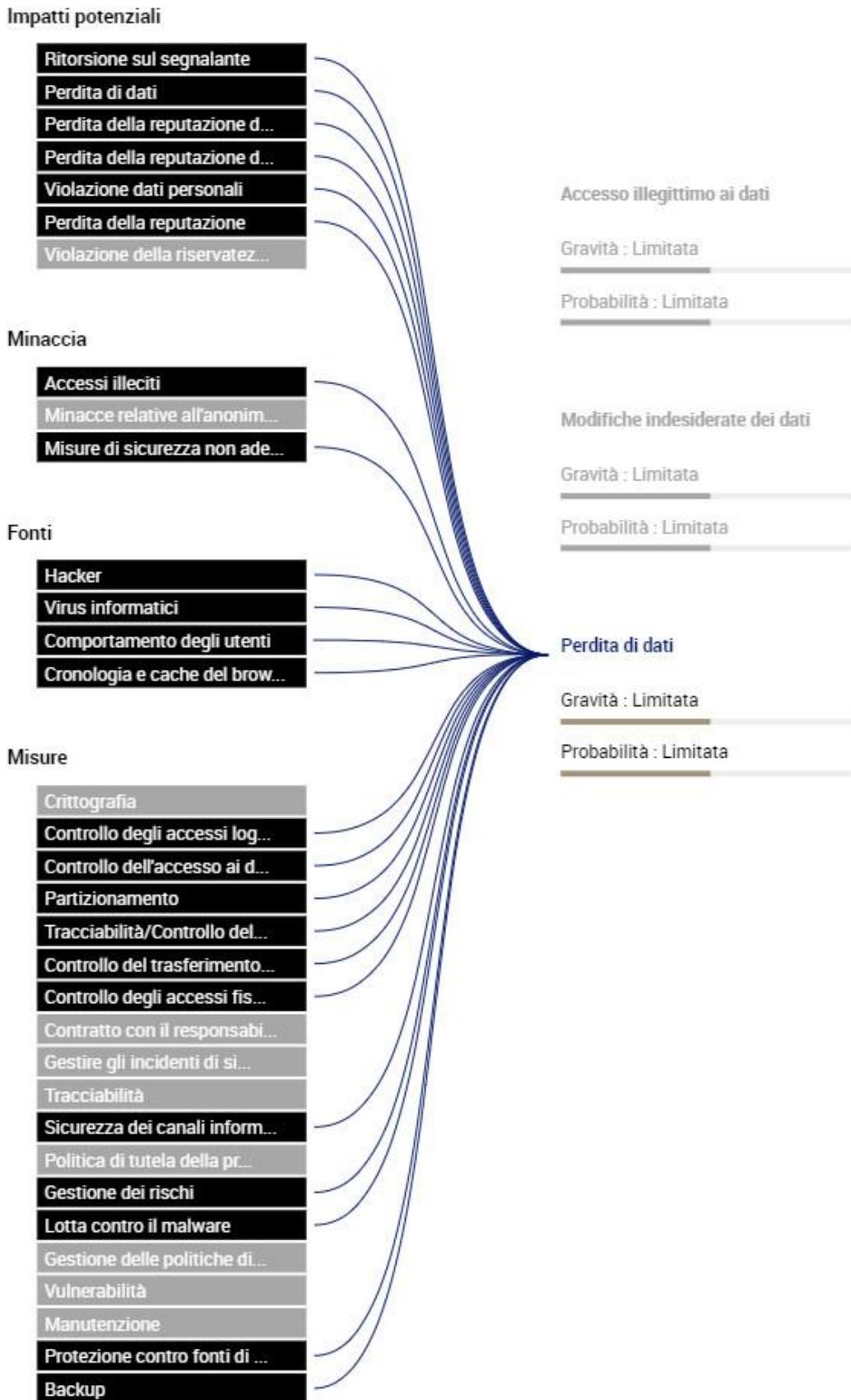
RISCHI ACCESSO ILLEGITTIMO



RISCHI MODIFICHE INDESIDERATE



RISCHI PERDITA DATI



Conclusioni

Dall'analisi sull'impatto dei rischi, valutati in base ai risultati emersi dalla mappatura dei rischi, i parametri emersi sono accettabili in quanto evidenziano valori indicati nell'area "limitata" del grafico; il valore emerso può essere ritenuto accettabile in relazione dai parametri oggettivi considerati.

Si ritiene pertanto, che il trattamento in oggetto, presenta un grado di rischio sui diritti e libertà dell'interessato rientrante nei parametri accettabili e di conseguenza ***non è richiesta una consultazione preventiva all'Autorità Garante.***

Allegati:

aws-dpa

aws-gdpr-compliance

Brochure Whistleblowing bigblue eye

AWS DATA PROCESSING ADDENDUM

This Data Processing Addendum (“**DPA**”) supplements the AWS Customer Agreement available at <http://aws.amazon.com/agreement>, as updated from time to time between Customer and AWS, or other agreement between Customer and AWS governing Customer’s use of the Services (the “**Agreement**”). This DPA is an agreement between you and the entity you represent (“**Customer**”, “**you**” or “**your**”) and Amazon Web Services, Inc. and the AWS Contracting Party or AWS Contracting Parties (as applicable) under the Agreement (together “**AWS**”). Unless otherwise defined in this DPA or in the Agreement, all capitalized terms used in this DPA will have the meanings given to them in Section 17 of this DPA.

1. Data Processing.

1.1 **Scope and Roles.** This DPA applies when Customer Data is processed by AWS. In this context, AWS will act as processor to Customer, who can act either as controller or processor of Customer Data.

1.2 **Customer Controls.** Customer can use the Service Controls to assist it with its obligations under Applicable Data Protection Law, including its obligations to respond to requests from data subjects. Taking into account the nature of the processing, Customer agrees that it is unlikely that AWS would become aware that Customer Data transferred under the Standard Contractual Clauses is inaccurate or outdated. Nonetheless, if AWS becomes aware that Customer Data transferred under the Standard Contractual Clauses is inaccurate or outdated, it will inform Customer without undue delay. AWS will cooperate with Customer to erase or rectify inaccurate or outdated Customer Data transferred under the Standard Contractual Clauses by providing the Service Controls that Customer can use to erase or rectify Customer Data.

1.3 Details of Data Processing.

1.3.1 **Subject matter.** The subject matter of the data processing under this DPA is Customer Data.

1.3.2 **Duration.** As between AWS and Customer, the duration of the data processing under this DPA is determined by Customer.

1.3.3 **Purpose.** The purpose of the data processing under this DPA is the provision of the Services initiated by Customer from time to time.

1.3.4 **Nature of the processing.** Compute, storage and such other Services as described in the Documentation and initiated by Customer from time to time.

1.3.5 **Type of Customer Data.** Customer Data uploaded to the Services under Customer’s AWS accounts.

1.3.6 **Categories of data subjects.** The data subjects could include Customer’s customers, employees, suppliers and End Users.

1.4 **Compliance with Laws.** Each party will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this DPA, including Applicable Data Protection Law.

2. **Customer Instructions.** The parties agree that this DPA and the Agreement (including Customer providing instructions via configuration tools such as the AWS management console and APIs made available by AWS for the Services) constitute Customer’s documented instructions regarding AWS’s processing of Customer Data (“**Documented Instructions**”). AWS will process

Customer Data only in accordance with Documented Instructions (which if Customer is acting as a processor, could be based on the instructions of its controllers). Additional instructions outside the scope of the Documented Instructions (if any) require prior written agreement between AWS and Customer, including agreement on any additional fees payable by Customer to AWS for carrying out such instructions. Customer is entitled to terminate this DPA and the Agreement if AWS declines to follow instructions requested by Customer that are outside the scope of, or changed from, those given or agreed to be given in this DPA. Taking into account the nature of the processing, Customer agrees that it is unlikely AWS can form an opinion on whether Documented Instructions infringe Applicable Data Protection Law. If AWS forms such an opinion, it will immediately inform Customer, in which case, Customer is entitled to withdraw or modify its Documented Instructions.

- 3. Confidentiality of Customer Data.** AWS will not access or use, or disclose to any third party, any Customer Data, except, in each case, as necessary to maintain or provide the Services, or as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order). If a governmental body sends AWS a demand for Customer Data, AWS will attempt to redirect the governmental body to request that data directly from Customer. As part of this effort, AWS may provide Customer's basic contact information to the governmental body. If compelled to disclose Customer Data to a governmental body, then AWS will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless AWS is legally prohibited from doing so.
- 4. Confidentiality Obligations of AWS Personnel.** AWS restricts its personnel from processing Customer Data without authorization by AWS as described in the Security Standards. AWS imposes appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security.
- 5. Security of Data Processing**
 - 5.1 AWS has implemented and will maintain the technical and organizational measures for the AWS Network as described in the Security Standards and this Section. In particular, AWS has implemented and will maintain the following technical and organizational measures:
 - (a) security of the AWS Network as set out in Section 1.1 of the Security Standards;
 - (b) physical security of the facilities as set out in Section 1.2 of the Security Standards;
 - (c) measures to control access rights for authorized personnel to the AWS Network as set out in Section 1.3 of the Security Standards; and
 - (d) processes for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures implemented by AWS as described in Section 2 of the Security Standards.
 - 5.2 Customer can elect to implement technical and organizational measures to protect Customer Data. Such technical and organizational measures include the following which can be obtained by Customer from AWS as described in the Documentation, or directly from a third-party supplier:
 - (a) pseudonymization and encryption to ensure an appropriate level of security;
 - (b) measures to ensure the ongoing confidentiality, integrity, availability and resilience of the processing systems and services that are operated by Customer;

measures to allow Customer to backup and archive appropriately in order to restore availability and access to Customer Data in a timely manner in the event of a physical or technical incident; and

- (c) processes for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures implemented by Customer.

6. Sub-processing.

6.1 **Authorized Sub-processors.** Customer provides general authorization to AWS's use of sub-processors to provide processing activities on Customer Data on behalf of Customer ("**Sub-processors**") in accordance with this Section. The AWS website (currently posted at <https://aws.amazon.com/compliance/sub-processors/>) lists Sub-processors that are currently engaged by AWS. At least 30 days before AWS engages a Sub-processor, AWS will update the applicable website and provide Customer with a mechanism to obtain notice of that update. To object to a Sub-processor, Customer can: (i) terminate the Agreement pursuant to its terms; (ii) cease using the Service for which AWS has engaged the Sub-processor; or (iii) move the relevant Customer Data to another Region where AWS has not engaged the Sub-processor.

6.2 **Sub-processor Obligations.** Where AWS authorizes a Sub-processor as described in Section 6.1:

- (i) AWS will restrict the Sub-processor's access to Customer Data only to what is necessary to provide or maintain the Services in accordance with the Documentation, and AWS will prohibit the Sub-processor from accessing Customer Data for any other purpose;
- (ii) AWS will enter into a written agreement with the Sub-processor and, to the extent that the Sub-processor performs the same data processing services provided by AWS under this DPA, AWS will impose on the Sub-processor the same contractual obligations that AWS has under this DPA; and
- (iii) AWS will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause AWS to breach any of AWS's obligations under this DPA.

7. **AWS Assistance with Data Subject Requests.** Taking into account the nature of the processing, the Service Controls are the technical and organizational measures by which AWS will assist Customer in fulfilling Customer's obligations to respond to data subjects' requests under Applicable Data Protection Law. If a data subject makes a request to AWS, AWS will promptly forward such request to Customer once AWS has identified that the request is from a data subject for whom Customer is responsible. Customer authorizes on its behalf, and on behalf of its controllers when Customer is acting as a processor, AWS to respond to any data subject who makes a request to AWS, to confirm that AWS has forwarded the request to Customer. The parties agree that Customer's use of the Service Controls and AWS forwarding data subjects' requests to Customer in accordance with this Section, represent the scope and extent of Customer's required assistance.

8. **Optional Security Features.** AWS makes available many Service Controls that Customer can elect to use. Customer is responsible for (a) implementing the measures described in Section 5.2, as appropriate, (b) properly configuring the Services, (c) using the Service Controls to allow Customer to restore the availability and access to Customer Data in a timely manner in the event of a physical or technical incident (for example backups and routine archiving of Customer Data), and

(d) taking such steps as Customer considers adequate to maintain appropriate security, protection, and deletion of Customer Data, which includes use of encryption technology to protect Customer Data from unauthorized access and measures to control access rights to Customer Data.

9. Security Incident Notification.

9.1 **Security Incident.** AWS will (a) notify Customer of a Security Incident without undue delay after becoming aware of the Security Incident, and (b) take appropriate measures to address the Security Incident, including measures to mitigate any adverse effects resulting from the Security Incident.

9.2 **AWS Assistance.** To enable Customer to notify a Security Incident to supervisory authorities or data subjects (as applicable), AWS will cooperate with and assist Customer by including in the notification under Section 9.1(a) such information about the Security Incident as AWS is able to disclose to Customer, taking into account the nature of the processing, the information available to AWS, and any restrictions on disclosing the information, such as confidentiality. Taking into account the nature of the processing, Customer agrees that it is best able to determine the likely consequences of a Security Incident.

9.3 **Unsuccessful Security Incidents.** Customer agrees that:

(i) an unsuccessful Security Incident will not be subject to this Section 9. An unsuccessful Security Incident is one that results in no unauthorized access to Customer Data or to any of AWS's equipment or facilities storing Customer Data, and could include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents; and

(ii) AWS's obligation to report or respond to a Security Incident under this Section 9 is not and will not be construed as an acknowledgement by AWS of any fault or liability of AWS with respect to the Security Incident.

9.4 **Communication.** Notification(s) of Security Incidents, if any, will be delivered to one or more of Customer's administrators by any means AWS selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on the AWS management console and secure transmission at all times.

9.5 **Notification Obligations.** If AWS notifies Customer of a Security Incident, or Customer otherwise becomes aware of any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data, Customer will be responsible for (a) determining if there is any resulting notification or other obligation under Applicable Data Protection Law and (b) taking necessary action to comply with those obligations. This does not limit AWS's obligations under this Section 9.

10. AWS Certifications and Audits.

10.1 **AWS ISO-Certification and SOC Reports.** In addition to the information contained in this DPA, upon Customer's request, and provided that the parties have an applicable NDA in place, AWS will make available the following documents and information:

(i) the certificates issued for the ISO 27001 certification, the ISO 27017 certification, the ISO 27018 certification, and the ISO 27701 certification (or the certifications or other documentation evidencing compliance with such alternative standards as are substantially equivalent to ISO 27001, ISO 27017, ISO 27018, and ISO 27701); and

- (ii) the System and Organization Controls (SOC) 1 Report, the System and Organization Controls (SOC) 2 Report and the System and Organization Controls (SOC) 3 Report (or the reports or other documentation describing the controls implemented by AWS that replace or are substantially equivalent to the SOC 1, SOC 2 and SOC 3).
 - 10.2 **AWS Audits.** AWS uses external auditors to verify the adequacy of its security measures, including the security of the physical data centers from which AWS provides the Services. This audit: (a) will be performed at least annually; (b) will be performed according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001; (c) will be performed by independent third-party security professionals at AWS's selection and expense; and (d) will result in the generation of an audit report ("**Report**"), which will be AWS's Confidential Information.
 - 10.3 **Audit Reports.** At Customer's written request, and provided that the parties have an applicable NDA in place, AWS will provide Customer with a copy of the Report so that Customer can reasonably verify AWS's compliance with its obligations under this DPA.
 - 10.4 **Privacy Impact Assessment and Prior Consultation.** Taking into account the nature of the processing and the information available to AWS, AWS will assist Customer in complying with Customer's obligations in respect of data protection impact assessments and prior consultation, by providing the information AWS makes available under this Section 10.
- 11. Customer Audits.** Customer chooses to conduct any audit, including any inspection, it has the right to request or mandate on its own behalf, and on behalf of its controllers when Customer is acting as a processor, under Applicable Data Protection Law or the Standard Contractual Clauses, by instructing AWS to carry out the audit described in Section 10. If Customer wishes to change this instruction regarding the audit, then Customer has the right to request a change to this instruction by sending AWS written notice as provided for in the Agreement. If AWS declines to follow any instruction requested by Customer regarding audits, including inspections, Customer is entitled to terminate the Agreement in accordance with its terms.
- 12. Transfers of Personal Data.**
- 12.1 **Regions.** Customer can specify the location(s) where Customer Data will be processed within the AWS Network (each a "**Region**"), including Regions in the EEA. Once Customer has made its choice, AWS will not transfer Customer Data from Customer's selected Region(s) except as necessary to provide the Services initiated by Customer, or as necessary to comply with the law or valid and binding order of a governmental body.
 - 12.2 **Application of Standard Contractual Clauses.** Subject to Section 12.3, the Standard Contractual Clauses will only apply to Customer Data subject to the GDPR that is transferred, either directly or via onward transfer, to any Third Country (each a "**Data Transfer**").
 - 12.2.1 When Customer is acting as a controller, the Controller-to-Processor Clauses will apply to a Data Transfer.
 - 12.2.2 When Customer is acting as a processor, the Processor-to-Processor Clauses will apply to a Data Transfer. Taking into account the nature of the processing, Customer agrees that it is unlikely that AWS will know the identity of Customer's controllers because AWS has no direct relationship with Customer's controllers and therefore, Customer will fulfil AWS's obligations to Customer's controllers under the Processor-to-Processor Clauses.
 - 12.3 **Alternative Transfer Mechanism.** The Standard Contractual Clauses will not apply to a Data Transfer if AWS has adopted Binding Corporate Rules for Processors or an alternative recognized compliance standard for lawful Data Transfers.

13. **Termination of the DPA.** This DPA will continue in force until the termination of the Agreement (the “**Termination Date**”).
14. **Return or Deletion of Customer Data.** At any time up to the Termination Date, and for 90 days following the Termination Date, subject to the terms and conditions of the Agreement, AWS will return or delete Customer Data when Customer uses the Service Controls to request such return or deletion. No later than the end of this 90-day period, Customer will close all AWS accounts containing Customer Data.
15. **Duties to Inform.** Where Customer Data becomes subject to confiscation during bankruptcy or insolvency proceedings, or similar measures by third parties while being processed by AWS, AWS will inform Customer without undue delay. AWS will, without undue delay, notify all relevant parties in such action (for example, creditors, bankruptcy trustee) that any Customer Data subjected to those proceedings is Customer’s property and area of responsibility and that Customer Data is at Customer’s sole disposition.
16. **Entire Agreement; Conflict.** This DPA incorporates the Standard Contractual Clauses by reference. Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between the Agreement and this DPA, the terms of this DPA will control, except that the Service Terms will control over this DPA. Nothing in this document varies or modifies the Standard Contractual Clauses.
17. **Definitions.** Unless otherwise defined in the Agreement, all capitalized terms used in this DPA will have the meanings given to them below:
 - “**API**” means an application program interface.
 - “**Applicable Data Protection Law**” means all laws and regulations applicable to and binding on the processing of Customer Data by a party, including, as applicable, the GDPR.
 - “**AWS Network**” means the servers, networking equipment, and host software systems (for example, virtual firewalls) that are within AWS’s control and are used to provide the Services.
 - “**Binding Corporate Rules**” has the meaning given to it in the GDPR.
 - “**controller**” has the meaning given to it in the GDPR.
 - “**Controller-to-Processor Clauses**” means the standard contractual clauses between controllers and processors for Data Transfers, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and currently located at https://d1.awsstatic.com/Controller_to_Processor_SCCs.pdf.
 - “**Customer Data**” means the Personal Data that is uploaded to the Services under Customer’s AWS accounts.
 - “**Documentation**” means the then-current documentation for the Services located at <http://aws.amazon.com/documentation> (and any successor locations designated by AWS).
 - “**EEA**” means the European Economic Area.
 - “**GDPR**” means Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
 - “**Personal Data**” means personal data, personal information, personally identifiable information or other equivalent term (each as defined in Applicable Data Protection Law).
 - “**processing**” has the meaning given to it in the GDPR and “process”, “processes” and “processed” will be interpreted accordingly.
 - “**processor**” has the meaning given to it in the GDPR.

“Processor-to-Processor Clauses” means the standard contractual clauses between processors for Data Transfers, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and currently located at [https://d1.awsstatic.com/Processor to Processor SCCs.pdf](https://d1.awsstatic.com/Processor_to_Processor_SCCs.pdf).

“Region” has the meaning given to it in Section 12.1 of this DPA.

“Security Incident” means a breach of AWS’s security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data.

“Security Standards” means the security standards attached to this DPA as Annex 1.

“Service Controls” means the controls, including security features and functionalities, that the Services provide, as described in the Documentation.

“Standard Contractual Clauses” means (i) the Controller-to-Processor Clauses, or (ii) the Processor-to-Processor Clauses, as applicable in accordance with Sections 12.2.1 and 12.2.2.

“Third Country” means a country outside the EEA not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR).

Annex 1

Security Standards

Capitalized terms not otherwise defined in this document have the meanings assigned to them in the Agreement.

1 Information Security Program. AWS will maintain an information security program designed to (a) enable Customer to secure Customer Data against accidental or unlawful loss, access, or disclosure, (b) identify reasonably foreseeable risks to the security and availability of the AWS Network, and (c) minimize physical and logical security risks to the AWS Network, including through regular risk assessment and testing. AWS will designate one or more employees to coordinate and be accountable for the information security program.

AWS's information security program will include the following measures:

1.1 Logical Security.

A. Access Controls. AWS will make the AWS Network accessible only to authorized personnel, and only as necessary to maintain and provide the Services. AWS will maintain access controls and policies to manage authorizations for access to the AWS Network from each network connection and user, including through the use of firewalls or functionally equivalent technology and authentication controls. AWS will maintain access controls designed to (i) restrict unauthorized access to data, and (ii) segregate each customer's data from other customers' data.

B. Restricted User Access. AWS will (i) provision and restrict user access to the AWS Network in accordance with least privilege principles based on personnel job functions, (ii) require review and approval prior to provisioning access to the AWS Network above least privileged principles, including administrator accounts; (iii) require at least quarterly review of AWS Network access privileges and, where necessary, revoke AWS Network access privileges in a timely manner, and (iv) require two-factor authentication for access to the AWS Network from remote locations.

C. Vulnerability Assessments. AWS will perform regular external vulnerability assessments and penetration testing of the AWS Network, and will investigate identified issues and track them to resolution in a timely manner.

D. Application Security. Before publicly launching new Services or significant new features of Services, AWS will perform application security reviews designed to identify, mitigate and remediate security risks.

E. Change Management. AWS will maintain controls designed to log, authorize, test, approve and document changes to existing AWS Network resources, and will document change details within its change management or deployment tools. AWS will test changes according to its change management standards prior to migration to production. AWS will maintain processes designed to detect unauthorized changes to the AWS Network and track identified issues to a resolution.

F. Data Integrity. AWS will maintain controls designed to provide data integrity during transmission, storage and processing within the AWS Network. AWS will provide Customer the ability to delete Customer Data from the AWS Network.

G. Business Continuity and Disaster Recovery. AWS will maintain a formal risk management program designed to support the continuity of its critical business functions ("**Business Continuity Program**"). The Business Continuity Program includes processes and procedures for identification of, response to, and recovery from, events that could prevent or materially impair AWS's provision of the Services (a

“BCP Event”). The Business Continuity Program includes a three-phased approach that AWS will follow to manage BCP Events:

- (i) **Activation & Notification Phase.** As AWS identifies issues likely to result in a BCP Event, AWS will escalate, validate and investigate those issues. During this phase, AWS will analyze the root cause of the BCP Event.
- (ii) **Recovery Phase.** AWS assigns responsibility to the appropriate teams to take steps to restore normal system functionality or stabilize the affected Services.
- (iii) **Reconstitution Phase.** AWS leadership reviews actions taken and confirms that the recovery effort is complete and the affected portions of the Services and AWS Network have been restored. Following such confirmation, AWS conducts a post-mortem analysis of the BCP Event.

H. Incident Management. AWS will maintain corrective action plans and incident response plans to respond to potential security threats to the AWS Network. AWS incident response plans will have defined processes to detect, mitigate, investigate, and report security incidents. The AWS incident response plans include incident verification, attack analysis, containment, data collection, and problem remediation. AWS will maintain an AWS Security Bulletin (as of the Effective Date, <http://aws.amazon.com/security/security-bulletins/>) which publishes and communicates security related information that may affect the Services and provides guidance to mitigate the risks identified.

I. Storage Media Decommissioning. AWS will maintain a media decommissioning process that is conducted prior to final disposal of storage media used to store Customer Data. Prior to final disposal, storage media that was used to store Customer Data will be degaussed, erased, purged, physically destroyed, or otherwise sanitized in accordance with industry standard practices designed to ensure that the Customer Data cannot be retrieved from the applicable type of storage media.

1.2 Physical Security.

A. Access Controls. AWS will (i) implement and maintain physical safeguards designed to prevent unauthorized physical access, damage, or interference to the AWS Network, (ii) use appropriate control devices to restrict physical access to the AWS Network to only authorized personnel who have a legitimate business need for such access, (iii) monitor physical access to the AWS Network using intrusion detection systems designed to monitor, detect, and alert appropriate personnel of security incidents, (iv) log and regularly audit physical access to the AWS Network, and (v) perform periodic reviews to validate adherence with these standards.

B. Availability. AWS will (i) implement redundant systems for the AWS Network designed to minimize the effect of a malfunction on the AWS Network, (ii) design the AWS Network to anticipate and tolerate hardware failures, and (iii) implement automated processes designed to move customer data traffic away from the affected area in the case of hardware failure.

1.3 AWS Employees.

A. Employee Security Training. AWS will implement and maintain employee security training programs regarding AWS information security requirements. The security awareness training programs will be reviewed and updated at least annually.

B. Background Checks. Where permitted by law, and to the extent available from applicable governmental authorities, AWS will require that each employee undergo a background investigation

that is reasonable and appropriate for that employee's position and level of access to the AWS Network.

2 Continued Evaluation. AWS will conduct periodic reviews of the information security program for the AWS Network. AWS will update or alter its information security program as necessary to respond to new security risks and to take advantage of new technologies.



Whitepaper AWS

Conformità al regolamento generale sulla protezione dei dati in AWS



Conformità al regolamento generale sulla protezione dei dati in AWS: Whitepaper AWS

Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e il trade dress di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in qualsiasi modo che possa causare confusione tra i clienti o in qualsiasi modo che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà dei rispettivi proprietari, che possono o meno essere affiliati, collegati o sponsorizzati da Amazon.

Table of Contents

Riassunto	1
Riassunto	1
Panoramica sul Regolamento generale sulla protezione dei dati	2
Modifiche introdotte dal GDPR per le organizzazioni che operano nell'UE	2
Come AWS si è preparato al GDPR	2
Addendum sul trattamento dei dati (DPA) di AWS	3
Il ruolo di AWS nell'ambito del GDPR	3
AWS come responsabile del trattamento	4
AWS come titolare del trattamento dei dati	4
Modello di responsabilità condivisa della sicurezza	4
Framework di conformità e standard di sicurezza rigorosi	6
Programma per la conformità in AWS	6
Cloud Computing Compliance Controls Catalog (C5)	6
Controllo dell'accesso ai dati	8
AWS Identity and Access Management	8
Token di accesso temporaneo tramite AWS STS	9
Autenticazione a più fattori	10
Accesso alle risorse AWS	11
Definizione dei limiti per l'accesso ai servizi regionali	12
Controllo dell'accesso alle applicazioni Web e alle applicazioni per dispositivi mobili	14
Monitoraggio e registrazione	15
Gestisci e configura le risorse con AWS Config	15
Verifica di conformità e analisi della sicurezza	16
Raccolta ed elaborazione dei registri	18
Scoprire e proteggere i dati su larga scala	20
Centralizzare la gestione della sicurezza	21
Protezione dei dati in AWS	24
Crittografia dei dati a riposo	24
Crittografia dei dati in transito	25
Strumenti di crittografia	26
AWS Key Management Service	27
Servizi e strumenti di crittografia AWS	30
Protezione dei dati fin dalla progettazione e per impostazione predefinita	31
In che modo AWS ti può aiutare	32

Collaboratori	35
Revisioni del documento	36
Avvisi	37

Conformità al regolamento generale sulla protezione dei dati in AWS

Data di pubblicazione: dicembre 2020 ([Revisioni del documento](#))

Riassunto

Questo documento fornisce informazioni sui servizi e le risorse che Amazon Web Services (AWS) offre ai clienti per aiutarli ad allinearsi ai requisiti del Regolamento generale sulla protezione dei dati (GDPR) che potrebbero applicarsi alle loro attività. Tra questi, la conformità di AWS agli standard di sicurezza IT, l'attestazione AWS C5 (Cloud Computing Compliance Controls Catalog), la conformità al Codice di condotta CISPE (Cloud Infrastructure Services Providers in Europe), controlli di accesso ai dati, strumenti di monitoraggio e registrazione, crittografia, gestione delle chiavi.

Panoramica sul Regolamento generale sulla protezione dei dati

Il [Regolamento generale sulla protezione dei dati \(GDPR, General Data Protection Regulation\)](#) è una legge europea sulla privacy ([Regolamento 2016/679 del Parlamento e del Consiglio dell'Unione europea del 27 aprile 2016](#)) che è entrata in vigore il 25 maggio 2018. Il GDPR sostituisce la Direttiva UE sulla protezione dei dati (Direttiva 95/46/CE) e ha lo scopo di armonizzare le leggi relative alla protezione dei dati in tutta l'Unione europea (UE) con l'applicazione di un'unica legge vincolante in ogni stato membro.

Il GDPR si applica a tutti i trattamenti di dati personali da parte di organizzazioni aventi sede nell'UE o che elaborano dati personali di residenti nell'UE quando offrono beni o servizi a persone nell'UE o monitorano il comportamento dei residenti dell'UE nell'UE. Per "dati personali", si intendono informazioni di qualunque tipo relative a una persona fisica identificata o identificabile.

Modifiche introdotte dal GDPR per le organizzazioni che operano nell'UE

Uno degli scopi principali del GDPR è l'armonizzazione in tutti gli Stati membri delle modalità di trattamento, uso e scambio sicuro dei dati personali. Le organizzazioni dovranno dimostrare, su base continuativa, la sicurezza dei dati trattati e la conformità al GDPR, implementando e rivedendo regolarmente misure tecniche e organizzative, oltre ai requisiti di conformità applicabili al trattamento dei dati personali. In caso di violazioni delle norme del GDPR, le autorità di controllo potranno emettere ammende fino a 20 milioni di euro o pari al 4% del fatturato annuo globale dell'organizzazione, se maggiore.

Come AWS si è preparato al GDPR

Gli esperti della conformità, della protezione dei dati e della sicurezza di AWS lavorano fianco a fianco con i clienti in tutto il mondo per rispondere alle loro domande e aiutarli a prepararsi a eseguire carichi di lavoro nel cloud in conformità con i requisiti del GDPR. Questi team esaminano anche il livello di preparazione di AWS in merito ai requisiti del GDPR.

 Note

Tutti i servizi AWS possono essere utilizzati in conformità con il GDPR.

Addendum sul trattamento dei dati (DPA) di AWS

AWS offre un Addendum sul trattamento dei dati conforme al GDPR (GDPR DPA) che consente di soddisfare gli obblighi contrattuali stabiliti dal GDPR. L'[Addendum di AWS sul trattamento dei dati conforme al GDPR \(GDPR DPA\) è integrato nei Termini del servizio AWS](#) e si applica automaticamente a tutti i clienti in tutto il mondo che lo richiedono per essere conformi al GDPR.

Il 16 luglio 2020, la Corte di giustizia dell'Unione europea (CGUE) ha emesso una sentenza in merito allo scudo UE-USA per la privacy e alle clausole contrattuali tipo (SCC, Standard Contractual Clauses), note anche come "clausole del modello". La CGUE ha stabilito che lo scudo UE-USA per la privacy non è più valido per il trasferimento di dati personali dall'Unione europea (UE) agli Stati Uniti (USA). Tuttavia, nella stessa sentenza, la CGUE ha convalidato che le aziende possono continuare a utilizzare le SCC come meccanismo per il trasferimento di dati al di fuori dell'UE.

In seguito a questa sentenza, i clienti e i partner di AWS possono continuare a utilizzare AWS per trasferire i loro contenuti dall'Europa agli Stati Uniti e ad altri paesi, in conformità con le leggi sulla protezione dei dati dell'UE, incluso il Regolamento generale sulla protezione dei dati (GDPR). I clienti AWS possono fare affidamento sulle SCC incluse nell'Addendum sul trattamento dei dati di AWS (DPA) se scelgono di trasferire i propri dati al di fuori dell'Unione Europea in conformità al GDPR. Con l'evolversi del panorama normativo e legislativo, lavoreremo per garantire che i nostri clienti e partner possano continuare a usufruire dei vantaggi dei servizi AWS ovunque operino. Per ulteriori informazioni, consulta le [Domande frequenti sullo scudo UE-USA per la privacy](#).

Il ruolo di AWS nell'ambito del GDPR

Secondo il GDPR, AWS è sia responsabile sia titolare del trattamento dei dati.

Ai sensi dell'articolo 32, i titolari e i responsabili del trattamento sono tenuti ad "attuare misure tecniche e organizzative adeguate" che tengano conto "dell'avanzamento e dei costi di attuazione e della natura, dell'ambito, del contesto e delle finalità del trattamento nonché del rischio di variazione di probabilità e della gravità per i diritti e le libertà delle persone fisiche". Il GDPR fornisce suggerimenti specifici sul tipo di azioni che potrebbero essere obbligatorie nell'ambito della sicurezza, che includono:

- La [pseudonimizzazione](#) e la crittografia dei dati personali..
- Opzioni che assicurino su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento.
- La possibilità di ripristinare la disponibilità e l'accesso ai dati personali in modo tempestivo in caso di problema tecnico o incidente.
- Una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

AWS come responsabile del trattamento

Quando i clienti e i partner della rete APN (AWS Partner Network) utilizzano i servizi AWS per elaborare dei contenuti propri che contengono informazioni personali, AWS funge da responsabile del trattamento dei dati. I clienti e i partner APN possono utilizzare i controlli disponibili nei servizi AWS, inclusi quelli di configurazione della sicurezza, per l'elaborazione delle informazioni personali. In questi casi, il cliente o i partner APN possono agire da titolare o responsabile del trattamento dei dati e AWS si comporta da responsabile principale o secondario del trattamento. L'Addendum sul trattamento dei dati di AWS conforme al GDPR incorpora gli impegni di AWS come responsabile del trattamento dei dati.

AWS come titolare del trattamento dei dati

Quando AWS raccoglie dati personali e determina le finalità e i mezzi di elaborazione degli stessi, agisce in qualità di titolare del trattamento dei dati. Per esempio, quando AWS elabora le informazioni dell'account per la registrazione dell'account, l'amministrazione, l'accesso ai servizi, o le informazioni di contatto relative all'account AWS per fornire assistenza ai clienti, agisce come responsabile del trattamento.

Modello di responsabilità condivisa della sicurezza

La sicurezza e la compliance sono responsabilità condivise tra AWS e il cliente. Quando i clienti trasferiscono sistemi e dati informatici dal loro computer al cloud, le responsabilità di sicurezza vengono condivise tra il cliente e il fornitore di servizi cloud. Quando i clienti passano al cloud AWS, AWS è responsabile della protezione dell'infrastruttura globale su cui vengono eseguiti tutti i servizi offerti nell'AWS Cloud. Per i servizi astratti, come Amazon S3 e Amazon DynamoDB AWS, è anche responsabile della sicurezza del sistema operativo e della piattaforma. I clienti AWS e i partner APN

che agiscono da titolari o responsabili del trattamento dei dati sono responsabili per gli eventuali dati personali che inseriscono nel cloud AWS. Comunemente, ci si riferisce a questa differenziazione della responsabilità con l'opposizione tra la sicurezza del cloud e la sicurezza nel cloud. Questo modello condiviso può aiutare a ridurre il carico operativo dei clienti e fornire loro la flessibilità e il controllo necessari per distribuire la propria infrastruttura nel cloud AWS. Per ulteriori informazioni, consulta il [Modello di responsabilità condivisa AWS](#).

Il GDPR non apporta alcuna modifica al modello di responsabilità condivisa AWS, che continuerà a essere in vigore per clienti e partner APN che utilizzano i servizi di cloud computing. Tale modello costituisce un approccio utile per illustrare le diverse responsabilità di AWS (in qualità di responsabile o subincaricato del trattamento dei dati) e di clienti e partner APN (come titolari o responsabili del trattamento dei dati) in conformità con il GDPR.

Framework di conformità e standard di sicurezza rigorosi

Ai sensi del GDPR, tra le misure tecniche e organizzative adeguate che possono essere richieste, ci sono "[...] la capacità di garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di elaborazione", nonché il ripristino affidabile, i test e i processi generali di gestione del rischio.

Programma per la conformità in AWS

AWS mantiene costantemente uno standard elevato in termini di sicurezza e la conformità in tutte le sue operazioni globali. La sicurezza è stata sempre la nostra massima priorità, l'essenza della nostra attività. AWS viene sottoposto regolarmente a verifiche di attestazione di terze parti indipendenti per garantire che le attività di controllo funzionino come previsto. Più specificamente, AWS è sottoposto a verifiche di conformità che prendono come riferimento framework di sicurezza globali e regionali che dipendono dalla regione e dal settore. Attualmente, AWS partecipa a più di 50 diversi programmi di verifica.

I risultati di queste verifiche sono documentati dall'ente di valutazione e resi disponibili per tutti i clienti AWS tramite [AWS Artifact](#). AWS Artifact è un portale self-service gratuito che offre l'accesso on-demand ai rapporti di conformità AWS. I nuovi report vengono resi disponibili in AWS Artifact, permettendo ai clienti di monitorare costantemente il livello di sicurezza e di conformità di AWS attraverso l'accesso immediato agli ultimi report.

I clienti possono usufruire di certificazioni e accreditamenti riconosciuti a livello internazionale, che provano la conformità a rigorosi standard internazionali, come ISO 27017 per la sicurezza del cloud, ISO 27018 per la privacy del cloud, SOC 1, SOC 2 e SOC 3, PCI DSS livello 1 e altri. AWS aiuta inoltre i clienti ad adeguarsi agli standard di sicurezza locali come ad esempio il Common Cloud Computing Controls Catalogue (C5) del BSI, una normativa tedesca.

Per informazioni più dettagliate sui programmi di certificazione AWS, i report e gli attestati di terze parti, consulta [Programmi per la conformità di AWS](#). Per informazioni specifiche sui servizi, consulta [Servizi AWS coperti dal programma di compliance](#).

Cloud Computing Compliance Controls Catalog (C5)

[Cloud Computing Compliance Controls Catalog \(C5\)](#) è uno schema di attestazione riconosciuto dal governo tedesco introdotto in Germania dall'Ufficio federale per la sicurezza informatica (Bundesamt

für Sicherheit in der Informationstechnik, BSI). È stato creato per aiutare le organizzazioni a dimostrare la sicurezza a livello operativo contro gli attacchi informatici comuni nell'ambito delle [Security Recommendations for Cloud Providers](#) (Raccomandazioni in materia di sicurezza ai fornitori di cloud) del governo tedesco.

Le misure tecniche e organizzative per la protezione dei dati e delle informazioni hanno come obiettivo la sicurezza dei dati e mirano a garantirne la riservatezza, l'integrità e la disponibilità. C5 definisce requisiti di sicurezza che possono essere rilevanti anche per la protezione dei dati. I clienti AWS e i rispettivi consulenti per la conformità possono utilizzare l'attestato C5 per comprendere la gamma di servizi di sicurezza IT offerti da AWS durante il trasferimento dei loro carichi di lavoro nel cloud. C5 aggiunge il livello di sicurezza IT definito a livello normativo equivalente allo standard IT-Grundschutz, con l'aggiunta di controlli specifici per il cloud.

Il C5 include ulteriori controlli relativi alla posizione dei dati, al provisioning dei servizi, alla sede giurisdizionale, alla certificazione esistente e agli obblighi di divulgazione delle informazioni, oltre a una descrizione completa del servizio. Queste informazioni permettono al cliente di valutare il tipo di correlazione esistente tra le normative legali (ad esempio, quelle sulla privacy dei dati), le proprie policy o il proprio ambiente delle minacce e l'utilizzo dei servizi di cloud computing.

Controllo dell'accesso ai dati

L'articolo 25 del GDPR stabilisce che il titolare del trattamento "deve mettere in atto misure tecniche e organizzative adeguate per garantire che, per impostazione predefinita, siano trattati solo i dati personali necessari per ciascuna finalità specifica del trattamento". I seguenti meccanismi di controllo degli accessi di AWS possono aiutare i clienti a garantire la conformità al presente requisito, concedendo l'accesso alle risorse AWS e ai dati dei clienti esclusivamente alle applicazioni, agli amministratori e agli utenti autorizzati:

AWS Identity and Access Management

Quando si crea un account AWS, viene creato automaticamente anche un account utente root per quell'account AWS. Questo account utente ha accesso completo a tutti i servizi e le risorse AWS presenti nell'account AWS. È consigliabile utilizzare questo account solo per la creazione iniziale di ruoli e account utente aggiuntivi e per eseguire attività amministrative che lo richiedono, non per le attività quotidiane. AWS consiglia di applicare il principio del privilegio minimo fin dall'inizio: definire account utente e ruoli diversi per attività diverse e specificare il set minimo di autorizzazioni necessarie per completare ciascuna attività. Questo approccio rappresenta un modo per mettere a punto un concetto chiave introdotto nel GDPR: la protezione dei dati fin dalla progettazione. [AWS Identity and Access Management](#) (IAM) è un servizio Web che puoi utilizzare per controllare in modo sicuro l'accesso alle tue risorse AWS.

Le identità IAM con autorizzazioni specifiche vengono definite in base agli utenti e ai ruoli. Un utente autorizzato può assumere un ruolo IAM per eseguire attività specifiche. Quando si assume il ruolo, vengono create delle credenziali temporanee. Ad esempio, è possibile utilizzare i ruoli IAM per fornire in modo sicuro alle applicazioni eseguite in [Amazon Elastic Compute Cloud](#) (Amazon EC2) le credenziali temporanee necessarie per accedere ad altre risorse AWS, come i bucket Amazon S3 e [Amazon Relational Database Service](#) (Amazon RDS) o i database [Amazon DynamoDB](#). Analogamente, [i ruoli di esecuzione](#) forniscono [AWS Lambda](#) alle funzioni le autorizzazioni necessarie per accedere ad altri servizi e risorse AWS, come [Amazon CloudWatch Logs](#) per lo streaming di log o la lettura di un messaggio da una [coda Amazon Simple Queue Service](#) (Amazon SQS). Quando crei un ruolo, aggiungi delle policy per definire le autorizzazioni.

Per aiutare i clienti a monitorare le policy delle risorse e identificare eventuali risorse per le quali è stato concesso in maniera non intenzionale l'accesso pubblico o tra account, è possibile abilitare [IAM Access Analyzer](#), che genera risultati completi utili per identificare le risorse a cui è possibile

accedere dall'esterno di un account AWS. IAM Access Analyzer utilizza la logica matematica e l'inferenza per valutare le policy delle risorse e determinare i possibili percorsi di accesso consentiti dalle policy. IAM Access Analyzer monitora continuamente le policy nuove o aggiornate e analizza le autorizzazioni concesse utilizzando le policy per i ruoli IAM, oltre che per risorse di servizi come i bucket Amazon S3, [AWS Key Management Service](#) (AWS KMS) le chiavi, le code Amazon SQS e le funzioni Lambda.

[Access Analyzer per S3](#) invia avvisi sui bucket configurati per permettere l'accesso a chiunque su Internet o ad altri account AWS, inclusi gli account AWS esterni all'organizzazione. Quando un bucket è a rischio in Access Analyzer per Amazon S3, è possibile bloccare tutti gli accessi pubblici al bucket con un solo clic. Ti consigliamo di bloccare tutti gli accessi ai bucket, a meno che l'accesso pubblico non sia necessario per supportare un caso d'uso specifico. Prima di bloccare tutti gli accessi pubblici, assicurati che le applicazioni continuino a funzionare correttamente senza accesso pubblico. Per ulteriori informazioni, consulta [Utilizzo del blocco dell'accesso pubblico di Amazon S3](#).

IAM fornisce inoltre informazioni sull'ultimo accesso per aiutarti a identificare le autorizzazioni non utilizzate, in modo che tu possa revocarle per gli utenti/gruppi/ruoli interessati. Grazie alle informazioni sull'ultimo accesso è possibile perfezionare le policy e consentire l'accesso solo ai servizi e alle operazioni necessarie. In questo modo è più facile applicare e conformarsi alle [best practice dei privilegi minimi](#). È possibile visualizzare le informazioni sull'ultimo accesso per entità o policy esistenti in IAM o in un intero [AWS Organizations](#) ambiente.

Token di accesso temporaneo tramite AWS STS

Puoi utilizzare [AWS Security Token Service](#) (AWS STS) per creare e fornire agli utenti attendibili le credenziali di sicurezza provvisorie per garantire l'accesso alle tue risorse AWS. Il funzionamento delle credenziali di sicurezza provvisorie è quasi identico rispetto a quello delle credenziali delle chiavi di accesso a lungo termine utilizzabili dagli utenti IAM, ma presenta le seguenti differenze:

- Le credenziali di sicurezza provvisorie sono utilizzabili a breve termine. È possibile configurare il periodo di validità, da 15 minuti fino a un massimo di 12 ore. Dopo la scadenza del periodo di validità, AWS non riconosce più le credenziali e nega tutte le richieste di accesso effettuate dall'API utilizzando tali credenziali.
- Le credenziali di sicurezza provvisorie non vengono archiviate nell'account utente. Invece, vengono generate dinamicamente e assegnate all'utente quando richiesto. Un utente può richiedere delle nuove credenziali di sicurezza provvisorie al momento (o prima) della scadenza di quelle in uso, purché disponga delle autorizzazioni per farlo.

In base a queste differenze, l'utilizzo delle credenziali temporanee offre i seguenti vantaggi:

- Non è necessario distribuire le credenziali di sicurezza AWS a lungo termine con un'applicazione, né incorporarle in essa.
- Le credenziali provvisorie costituiscono la base dei ruoli e della federazione delle identità. Puoi fornire agli utenti l'accesso alle tue risorse AWS definendo un'identità AWS temporanea per loro.
- Le credenziali di sicurezza provvisorie hanno una durata limitata e personalizzabile. Per questo motivo non è necessario ruotarle o revocarle esplicitamente quando non sono più necessarie. Dopo la loro scadenza, le credenziali di sicurezza provvisorie non possono essere riutilizzate. È possibile specificare il periodo massimo di validità delle credenziali.

Autenticazione a più fattori

Per incrementare il livello di sicurezza, puoi aggiungere l'autenticazione a due fattori per il tuo account e per i singoli utenti. Quando è abilitata, l'autenticazione a più fattori (MFA) richiede a coloro che effettuano l'accesso alla [Console di gestione AWS](#) il nome utente e la password (il primo fattore), oltre a una risposta di autenticazione dal loro dispositivo AWS MFA (il secondo fattore). È possibile attivare la MFA per il proprio account AWS e per singoli utenti IAM creati nell'account. Inoltre, la MFA permette di controllare l'accesso alle API dei servizi AWS.

Ad esempio, puoi definire una policy che consenta l'accesso completo a tutte le operazioni delle API di AWS in Amazon EC2 agli utenti che superano l'autenticazione MFA e neghi esplicitamente l'accesso a specifiche operazioni API, ad esempio `StopInstances` e `TerminateInstances`, a coloro che non sono autenticati.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAllActionsForEC2",
      "Effect": "Allow",
      "Action": "ec2:*",
      "Resource": "*"
    },
    {
      "Sid": "DenyStopAndTerminateWhenMFAIsNotPresent",
      "Effect": "Deny",
      "Action": [
```

```
        "ec2:StopInstances",
        "ec2:TerminateInstances"
    ],
    "Resource": "*",
    "Conditions": {
        "BoolIfExists": {"aws:MultiFactorAuthPresent":false}
    }
}
}
```

Per aggiungere un ulteriore livello di sicurezza ai bucket Amazon S3, puoi configurare la funzione [Cancellazione MFA](#), che richiede un'autenticazione aggiuntiva per modificare lo stato del controllo delle versioni di un bucket ed eliminare definitivamente una versione dell'oggetto. La funzione Cancellazione MFA fornisce così una protezione ulteriore nel caso in cui le credenziali di sicurezza fossero compromesse.

Per utilizzare la funzione Cancellazione MFA è necessario un dispositivo MFA fisico o virtuale per generare un codice di autenticazione. Consulta la [pagina Autenticazione a più fattori](#) per visionare l'elenco dei dispositivi MFA hardware o virtuali supportati.

Accesso alle risorse AWS

Per implementare un accesso granulare alle risorse AWS, è possibile assegnare autorizzazioni di livello diverso a persone diverse per risorse diverse. Ad esempio, puoi consentire l'accesso completo ad Amazon EC2, Amazon S3, DynamoDB, [Amazon Redshift](#) e altri servizi AWS solo ad alcuni utenti.

Puoi limitare le autorizzazioni per gli altri utenti, concedendo l'accesso in sola lettura solo ad alcuni bucket Amazon S3, l'autorizzazione ad amministrare solo alcune istanze di Amazon EC2 o l'accesso limitato solo ai tuoi dati di fatturazione.

La policy seguente costituisce un esempio di come è possibile consentire tutte le operazioni su un bucket Amazon S3 specifico e negare esplicitamente l'accesso a tutti i servizi AWS che non sono Amazon S3.

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
{
  "Effect": "Allow",
  "Action": "s3:*",
  "Resource": [
    "arn:aws:s3:::bucket-name",
    "arn:aws:s3:::bucket-name/*"
  ],
},
{
  "Effect": "Deny",
  "NotAction": "s3:*",
  "NotResource": [
    "arn:aws:s3:::bucket-name",
    "arn:aws:s3:::bucket-name/*"
  ]
}
]
```

È possibile allegare una policy a un account utente o a un ruolo. Per altri esempi di policy IAM, consulta [Esempi di policy IAM basate sull'identità](#).

Definizione dei limiti per l'accesso ai servizi regionali

La proprietà dei dati rimane al cliente, che potrà scegliere a quali servizi AWS consentirne elaborazione, archiviazione e hosting. AWS non accede né utilizza i contenuti dei clienti per alcun motivo senza il loro consenso. In base al modello di responsabilità condivisa, sei tu che scegli le regioni AWS in cui vengono archiviati i tuoi contenuti, il che ti permette di distribuire i servizi AWS nelle posizioni di tua scelta, in base ai tuoi requisiti geografici specifici. Ad esempio, se desideri che i tuoi contenuti siano localizzati solo in Europa, puoi scegliere di distribuire i servizi AWS esclusivamente in una delle regioni AWS europee.

Le policy IAM forniscono un modo semplice per limitare l'accesso ai servizi in regioni specifiche. Puoi aggiungere una condizione globale ([aws:RequestedRegion](#)) alle policy IAM associate ai tuoi principali IAM da applicare a tutti i servizi AWS. Ad esempio, [la seguente policy](#) utilizza l'elemento `NotAction` con l'effetto `Deny` di negare esplicitamente l'accesso a tutte le operazioni non elencate nell'istruzione se la Regione richiesta non è europea. Le autorizzazioni per eseguire operazioni nei servizi CloudFront, IAM, [Amazon Route 53](#) e [AWS Support](#) non devono essere negate perché si tratta di servizi globali AWS molto diffusi.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAllOutsideRequestedRegions",
      "Effect": "Deny",
      "NotAction": [
        "cloudfront:*",
        "iam:*",
        "route53:*",
        "support:*"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotLike": {
          "aws:RequestedRegion": [
            "eu-*"
          ]
        }
      }
    }
  ]
}
```

Questa policy IAM di esempio può essere implementata anche come Service Control Policy (SCP) in AWS Organizations, che definisce i limiti di autorizzazioni applicati a specifici account AWS o unità organizzative (OU) all'interno di un'organizzazione. Ciò consente di controllare l'accesso degli utenti ai servizi regionali in ambienti multi-account complessi.

Per le regioni introdotte di recente sono disponibili funzionalità di limitazione geografica. [Le regioni introdotte dopo il 20 marzo 2019](#) sono disabilitate per impostazione predefinita. È necessario abilitare queste regioni prima di poterle utilizzare. Per abilitare o disabilitare una regione AWS disabilitata per impostazione predefinita puoi utilizzare la Console di gestione AWS. Attraverso l'abilitazione e la disabilitazione delle regioni è possibile controllare se gli utenti dell'account hanno accesso alle risorse in quella regione. Per ulteriori informazioni, consulta [Gestione delle regioni AWS](#).

Controllo dell'accesso alle applicazioni Web e alle applicazioni per dispositivi mobili

AWS fornisce servizi per la gestione del controllo dell'accesso ai dati contenuti nelle applicazioni dei clienti. Per aggiungere funzionalità di accesso utente e di controllo dell'accesso alle applicazioni Web e a quelle per dispositivi mobili, è possibile utilizzare [Amazon Cognito](#). [Il bacino d'utenza di Amazon Cognito](#) fornisce una directory utente in grado di dimensionare le risorse per centinaia di milioni di utenti. È possibile aggiungere l'autenticazione a più fattori o MFA, (Multi-factor authentication) a un bacino d'utenza per proteggere l'identità degli utenti. Inoltre, attraverso l'autenticazione adattiva, che utilizza un modello basato sul rischio, è possibile prevedere quando potrebbe essere necessario utilizzare un altro fattore di autenticazione.

I [pool di identità di Amazon Cognito](#) (Identità federate), permettono di controllare chi ha avuto accesso alle risorse e da dove ha avuto origine l'accesso (applicazione Web o per dispositivi mobili). È possibile utilizzare queste informazioni per creare ruoli e policy IAM per consentire o negare l'accesso a una risorsa in base al tipo di origine dell'accesso (applicazione Web o per dispositivi mobili) e al provider di identità.

Monitoraggio e registrazione

L'articolo 30 del GDPR stabilisce che "... tutti i titolari del trattamento e, ove applicabile, il rappresentante del titolare del trattamento, devono tenere un registro delle attività di trattamento sotto la propria responsabilità". Questo articolo include anche dettagli su quali informazioni devono essere registrate quando si monitora il trattamento di tutti i dati personali. I titolari e i responsabili del trattamento sono inoltre tenuti a inviare le notifiche di violazione in modo tempestivo, quindi è importante rilevare rapidamente gli incidenti. Per aiutare i clienti a garantire la conformità a tali obblighi, AWS offre diversi servizi di monitoraggio e registrazione.

Gestisci e configura le risorse con AWS Config

[AWS Config](#) fornisce una vista dettagliata della configurazione delle risorse AWS nel tuo account AWS. Sono inclusi il modo in cui le risorse sono correlate tra loro e come erano configurate in precedenza, in modo che tu possa vedere come le configurazioni e le relazioni sono cambiate nel corso del tempo.

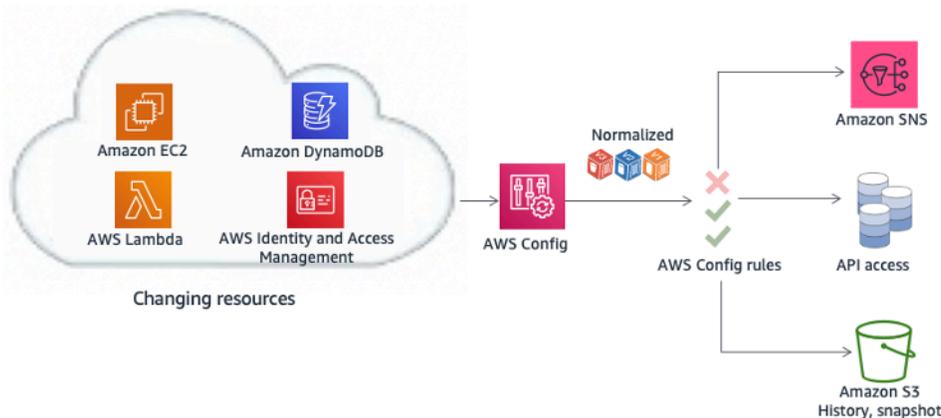


Figura 1. Monitorare i cambiamenti di configurazione nel tempo con AWS Config

Una risorsa AWS è un'entità con la quale si può lavorare in AWS, ad esempio un'istanza Amazon Elastic Compute Cloud (EC2), un [volume Amazon Elastic Block Store](#) (Amazon EBS), un gruppo di sicurezza o un [Amazon Virtual Private Cloud](#) (Amazon VPC). Per un elenco completo delle risorse AWS supportate da AWS Config, consulta la pagina [Tipologie di risorse AWS supportate](#).

Con AWS Config è possibile eseguire le seguenti operazioni:

- Valutare le configurazioni delle tue risorse AWS rispetto alle impostazioni desiderate.

- Ottenere uno snapshot delle configurazioni attuali delle risorse supportate associate al tuo account AWS.
- Ottenere le configurazioni di una o più risorse esistenti nel tuo account.
- Visualizzare la cronologia delle configurazioni di una o più risorse.
- Ricevere una notifica ogni volta che una risorsa viene creata, modificata o eliminata.
- Visualizzare le relazioni tra le risorse. Ti permette, ad esempio, di trovare tutte le risorse che utilizzano un particolare gruppo di sicurezza.

Verifica di conformità e analisi della sicurezza

[AWS CloudTrail](#) permette di monitorare in modo continuo l'attività dell'account AWS. Acquisisce la cronologia delle chiamate API AWS per il tuo account, incluse le chiamate API effettuate tramite la Console di gestione AWS, i kit SDK AWS, gli strumenti a riga di comando e i servizi AWS di livello superiore. Permette inoltre di identificare quali utenti e account hanno richiamato le API [per i servizi che supportano AWS CloudTrail](#), l'indirizzo IP sorgente da cui sono state effettuate le chiamate e quando sono avvenute. È possibile integrare CloudTrail in applicazioni che utilizzano l'API, automatizzare la creazione di trail per l'organizzazione, controllare lo stato dei trail e monitorare il modo in cui gli amministratori attivano e disattivano la registrazione di CloudTrail.

CloudTrail permette di aggregare i suoi registri da [più regioni](#) e [più account AWS](#) in un unico bucket Amazon S3. AWS consiglia di scrivere i registri, in particolare quelli AWS CloudTrail, in un bucket Amazon S3 con accesso limitato in un account AWS designato per la registrazione (Log Archive). Le autorizzazioni sul bucket dovrebbero impedire l'eliminazione dei registri e dovrebbero anche essere crittografate a riposo, utilizzando la crittografia lato server con chiavi di crittografia gestite da Amazon S3 (SSE-S3) o chiavi gestite da AWS KMS (SSE-KMS). La funzione di convalida dell'integrità dei file di registro permette di determinare se un file di registro è stato modificato, eliminato o modificato dopo che CloudTrail lo ha distribuito. Questa caratteristica è stata sviluppata usando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende ardua, a livello di programmazione, qualsiasi operazione di modifica, eliminazione o contraffazione dei file di registro di CT, senza che tale operazione venga rilevata. È possibile utilizzare l'interfaccia a riga di comando AWS (AWS CLI) per convalidare i file nella posizione in cui CloudTrail li ha distribuiti.

CloudTrail consente di analizzare i registri aggregati in un bucket Amazon S3 per scopi di verifica o per attività di risoluzione dei problemi. Quando i registri sono centralizzati, è possibile integrarli con le soluzioni SIEM (Security Information and Event Management) o utilizzare i servizi AWS, come [Amazon Athena](#) o [CloudTrail Insights](#), per analizzarli e [visualizzarli utilizzando i pannelli di controllo di](#)

[Amazon QuickSight](#). Una volta centralizzati i registri CloudTrail, puoi utilizzare lo stesso account in cui sono archiviati i registri per centralizzare i registri da altre fonti, come CloudWatch Logs e i sistemi di bilanciamento del carico AWS.

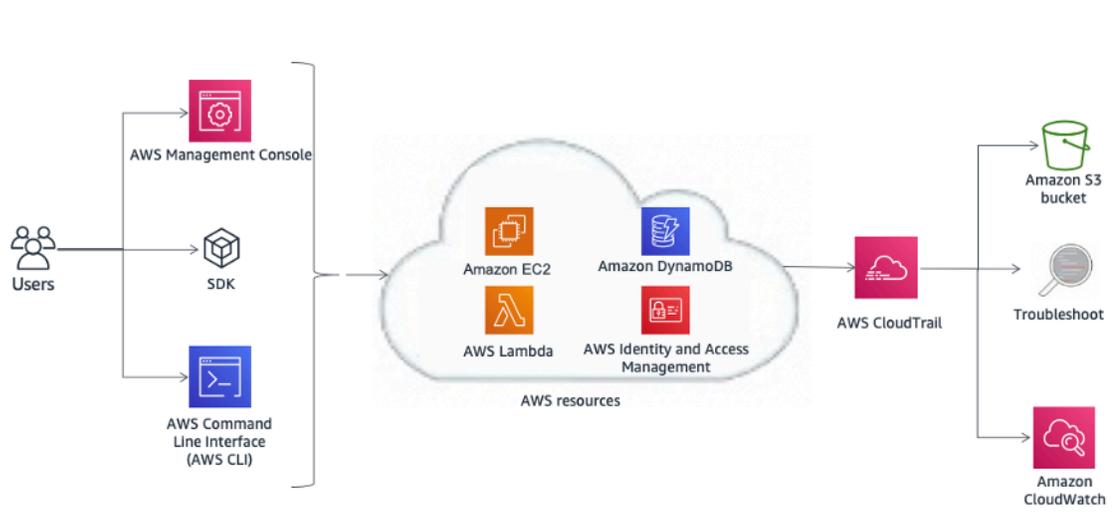


Figura 2. Architettura di esempio per la verifica della conformità e l'analisi della sicurezza con AWS CloudTrail

I registri AWS CloudTrail possono anche attivare eventi Amazon CloudWatch preconfigurati. È possibile utilizzare questi eventi per inviare una notifica agli utenti o ai sistemi riguardo a un evento che si è verificato o a un'operazione correttiva. Ad esempio, se desideri monitorare le attività sulle tue istanze Amazon EC2, puoi creare una [regola per gli eventi CloudWatch](#). Quando si verifica un'attività specifica sull'istanza Amazon EC2 e l'evento viene acquisito nei registri, la regola attiva una AWS Lambda funzione che invia un'e-mail di notifica dell'evento all'amministratore. (Vedi Figura 3). Alcune delle informazioni incluse nell'e-mail sono quando si è verificato l'evento, quale utente ha eseguito l'azione, dettagli di Amazon EC2 e altro. Il diagramma seguente mostra l'architettura della notifica degli eventi.

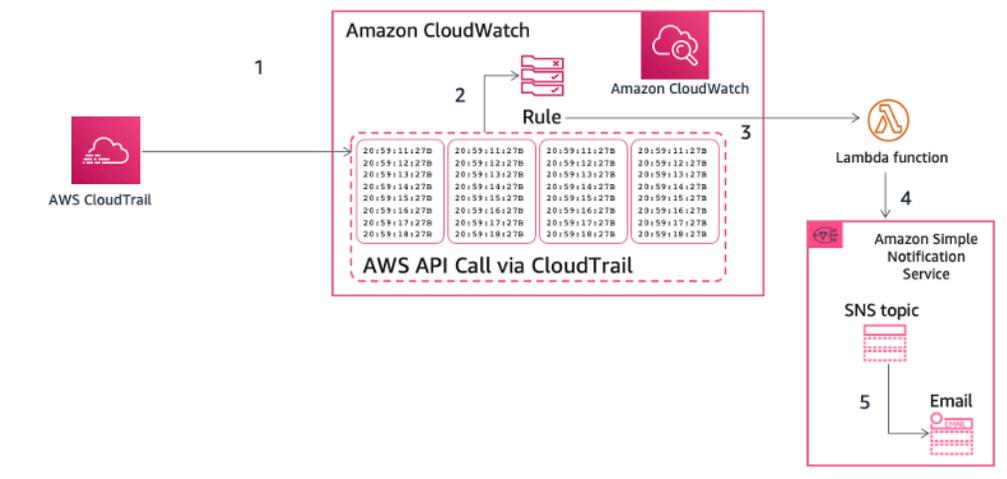


Figura 3. Esempio di notifica degli AWS CloudTrail eventi

Raccolta ed elaborazione dei registri

Con CloudWatch Logs è possibile monitorare, archiviare e accedere ai file di registro da istanze Amazon EC2, AWS CloudTrail, Route 53 e altre fonti. Consulta la pagina della documentazione [Servizi AWS che pubblicano i registri in CloudWatch Logs](#).

Le informazioni sui registri includono, ad esempio:

- Registrazione granulare degli accessi a oggetti Amazon S3
- Informazioni dettagliate sui flussi nella rete tramite i flussi di log di VPC.
- Verifica della configurazione basata su regole e operazioni con AWS Config
- Filtraggio e monitoraggio degli accessi HTTP alle applicazioni con funzioni WAF (Web Application Firewall) in CloudFront

I parametri e i registri delle applicazioni personalizzati possono anche essere pubblicati su CloudWatch Logs installando [CloudWatch Agent](#) su istanze Amazon EC2 o server locali.

Con CloudWatch Logs Insights è possibile analizzare i registri in modo interattivo ed eseguire query per rispondere in modo più efficiente ed efficace ai problemi operativi.

CloudWatch permette di elaborare i suoi registri quasi in tempo reale, configurando filtri per le sottoscrizioni, e di distribuirli ad altri servizi come un cluster [Amazon OpenSearch Service](#) (OpenSearch Service), un flusso [Amazon Kinesis](#), un flusso Amazon Kinesis Data Firehose o Lambda per personalizzare l'elaborazione, l'analisi o il caricamento su altri sistemi.

Con i [filtri parametrici di CloudWatch](#) è possibile definire modelli di ricerca nei dati di registro, trasformarli in parametri di CloudWatch numerici e impostare allarmi in base ai requisiti aziendali. Ad esempio, seguendo la raccomandazione di AWS di non utilizzare l'utente root per le attività quotidiane, è possibile [impostare un filtro parametrico CloudWatch specifico](#) su un registro di CloudTrail (distribuito a CloudWatch Logs) per creare un parametro personalizzato e configurare un allarme per inviare alle parti interessate una notifica quando le credenziali di root vengono utilizzate per accedere al tuo account AWS.

Registri quali i registri di accesso ai server Amazon S3, i registri di accesso Elastic Load Balancing e AWS Global Accelerator i flussi di log possono essere distribuiti direttamente a un bucket Amazon S3. L'abilitazione dei [registri di accesso al server Amazon Simple Storage Service](#) ti permette, ad esempio, di ottenere informazioni dettagliate sulle richieste che vengono effettuate al tuo bucket Amazon S3. Un record dei registri di accesso contiene dettagli sulla richiesta, ad esempio il tipo di richiesta, le risorse specificate nella richiesta e l'ora e la data di elaborazione della richiesta. Per ulteriori informazioni sui contenuti di un messaggio di registro, consulta la sezione intitolata [Formato dei registri di accesso al server Amazon Simple Storage Service](#) nella Amazon Simple Storage Service Developer Guide. I registri degli accessi al server sono utili per molte applicazioni in quanto forniscono ai proprietari dei bucket informazioni sulla natura delle richieste effettuate dai client non sottoposti al loro controllo. Per impostazione predefinita, Amazon S3 non raccoglie i registri di accesso al servizio ma, una volta abilitata la registrazione, distribuisce i registri di accesso al tuo bucket solitamente entro poche ore. Se hai bisogno di una distribuzione più rapida o devi distribuire i registri a più destinazioni, [valuta la possibilità di utilizzare i registri di CloudTrail](#) o una combinazione dei registri CloudTrail e Amazon S3. È possibile crittografare i registri a riposo, configurando la crittografia degli oggetti predefinita nel bucket di destinazione. Gli oggetti sono crittografati con la crittografia lato server con le chiavi gestite da Amazon S3 (SSE-S3) o le chiavi master del cliente (CMK) archiviate in [AWS Key Management Service](#) (AWS KMS).

Per interrogare e analizzare i registri archiviati in un bucket Amazon S3 è possibile utilizzare [Amazon Athena](#). Amazon Athena è un servizio di query interattivo che permette di effettuare l'analisi dei dati in Amazon S3 utilizzando un SQL standard. Athena permette di eseguire query specifiche utilizzando ANSI SQL, senza dover aggregare o caricare i dati su Athena. Athena è in grado di elaborare set di dati non strutturati, semi-strutturati e strutturati e si integra con [Amazon QuickSight](#) per una facile visualizzazione.

I registri sono anche un'utile fonte di informazioni per il rilevamento automatico delle minacce. [Amazon GuardDuty](#) è un servizio di monitoraggio continuo della sicurezza che analizza ed elabora eventi provenienti da diverse fonti, ad esempio flussi di log VPC, registri degli eventi di gestione di CloudTrail, registri degli eventi di dati di CloudTrail Amazon S3 e registri DNS. Utilizza feed di

intelligence di minacce, come elenchi di domini e di IP dannosi nonché il machine learning per identificare attività inattese e potenzialmente non autorizzate e dannose nell'ambiente AWS. Appena viene abilitato in una regione, GuardDuty avvia immediatamente l'analisi dei registri degli eventi di CloudTrail. Utilizza la gestione di CloudTrail e gli eventi di dati di Amazon S3 direttamente da CloudTrail attraverso un flusso di eventi indipendente e ripetitivo.

Scoprire e proteggere i dati su larga scala con Amazon Macie

L'articolo 32 del GDPR stabilisce che "... il titolare del trattamento e il responsabile del trattamento devono attuare misure tecniche e organizzative adeguate per garantire un livello di sicurezza appropriato al rischio, incluse tra le altre quando applicabili: [...]"

(b) opzioni che garantiscono riservatezza, integrità, disponibilità e resilienza di sistemi e servizi di elaborazione in modo continuo.

[...]

(d) Una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento".

Disporre di un processo di classificazione dei dati continuo è fondamentale per adattare l'elaborazione dei dati di sicurezza alla natura dei dati. Se la tua organizzazione gestisce dati sensibili, devi poter monitorare la loro posizione, proteggerli in modo adeguato e dimostrare l'effettiva implementazione di misure a tutela della privacy e della sicurezza dei dati, al fine di soddisfare la conformità ai requisiti delle normative. Per aiutare i suoi clienti a identificare e proteggere i propri dati sensibili su larga scala, AWS offre [Amazon Macie](#), un servizio di tutela della sicurezza e della riservatezza dei dati completamente gestito, che rileva e protegge i dati sensibili archiviati nei bucket S3 utilizzando modelli di pattern matching e machine learning progettati per il rilevamento di informazioni personali di identificazione (PII). Amazon Macie esegue la scansione di questi bucket e fornisce una categorizzazione dei dati in essi contenuti, utilizzando identificatori di dati gestiti progettati per il rilevamento di diverse categorie di dati sensibili. Macie è in grado di [rilevare PII](#) quali nome completo, indirizzo e-mail, data di nascita, numero di identificazione nazionale, codice fiscale o numero di riferimento e altro. L'utente può definire identificatori di dati personalizzati che riflettono gli scenari particolari della sua organizzazione (ad esempio, numeri di account dei clienti o classificazione interna dei dati).

Amazon Macie valuta in modo continuativo l'oggetto all'interno dei bucket e fornisce automaticamente un riepilogo dei risultati (Figura 4) per tutti i dati non crittografati o accessibili pubblicamente che

corrispondono alla categoria di dati definita. Questi dati possono includere avvisi per qualsiasi oggetto o bucket non crittografato e pubblicamente accessibile condiviso con account AWS al di fuori di quelli definiti in AWS Organizations. Amazon Macie è integrato con altri servizi AWS, ad esempio [AWS Security Hub](#), per generare risultati di sicurezza fruibili e fornire un'azione automatica e reattiva basata sui risultati (Figura 5).

The screenshot displays the Amazon Macie console interface. On the left, a 'Findings' table lists several high-severity findings. The first finding is selected, and its details are shown in a right-hand pane titled 'SensitiveData:S3Object/Multiple'.

Severity	Region	Account ID	Resource	Created at	Updated at
High	us-east-1	[Redacted]	maciestestbucket-rch1/testdata/request.zip	05-10-2020 23:36:27 (16 hours ago)	05-10-2020 23:36:27 (16 hours ago)

The detailed view on the right shows the following information:

- Overview:** Severity: High, Region: us-east-1, Account ID: [Redacted], Resource: maciestestbucket-rch1/testdata/request.zip, Created at: 05-10-2020 23:36:27 (16 hours ago), Updated at: 05-10-2020 23:36:27 (16 hours ago).
- Result:** Job ID: c2ca1ac623b4337c9c43e2a815a903a7.
- Details:** Status: COMPLETE, Size classified: 264 bytes, MIME type: application/zip, Detailed result location: s3://macie-output-rch/AWSLogs/[Redacted]/Macie/us-...
- Financial info:** Credit card number: 1.
- Personal info:** Address: 1, Spain passport number: 1, Usa passport number: 1, Usa social security number: 1.

Figura 4. Ispezioni dei dati e risultati di esempio

Centralizzare la gestione della sicurezza

Molte organizzazioni devono affrontare sfide legate alla visibilità e alla gestione centralizzata dei loro ambienti. Man mano che l'impronta operativa di un'organizzazione cresce, questa sfida diventa sempre più gravosa, a meno che non si valuti attentamente la progettazione della sicurezza. La mancanza di conoscenza, combinata con una gestione decentralizzata e non uniforme dei processi di governance e sicurezza, può rendere vulnerabile il tuo ambiente.

AWS fornisce strumenti per aiutarti a soddisfare alcuni dei requisiti più impegnativi per la gestione e la governance dell'IT e strumenti per supportare un approccio di protezione dei dati basato sulla progettazione.

[AWS Control Tower](#) offre un modo per configurare e governare un ambiente AWS multi-account nuovo e sicuro. Automatizza la configurazione di una [zona di destinazione](#), che è un ambiente multi-account basato su progetti di best practice, e abilita la governance utilizzando guardrail selezionabili da un elenco predefinito. I guardrail implementano regole di governance per la sicurezza, la

conformità e le operations. AWS Control Tower permette di effettuare la gestione delle identità utilizzando la directory predefinita di AWS IAM Identity Center (IAM Identity Center) e consente la verifica tra account utilizzando IAM Identity Center e IAM. Centralizza anche i registri provenienti da CloudTrail e quelli di AWS Config, che sono archiviati in Amazon S3.

[AWS Security Hub](#) è un altro servizio che supporta la centralizzazione e può migliorare la visibilità all'interno di un'organizzazione. Security Hub centralizza e dà priorità ai risultati della sicurezza e della conformità provenienti da tutti gli account e i servizi AWS, come Amazon GuardDuty e [Amazon Inspector](#), e può essere integrato con software di sicurezza di partner di terze parti per aiutarti ad analizzare le tendenze in materia di sicurezza e identificare i problemi di sicurezza prioritari.

[Amazon GuardDuty](#) è un servizio di rilevamento delle minacce intelligente che aiuta i clienti a monitorare e proteggere in modo più accurato e semplice i propri account AWS, i carichi di lavoro e i dati archiviati in Amazon S3. GuardDuty analizza miliardi di eventi provenienti da diverse fonti nei tuoi account AWS, tra cui eventi di AWS CloudTrail gestione, eventi di dati di CloudTrail Amazon S3, flussi di log di Amazon Virtual Private Cloud e registri DNS. Ad esempio, il servizio è in grado di rilevare chiamate API inconsuete, comunicazioni sospette in uscita verso indirizzi IP malevoli noti o possibili furti di dati effettuati tramite query DNS. GuardDuty è in grado di fornire risultati più accurati sfruttando l'intelligence sulle minacce basata sul machine learning e partner di sicurezza di terze parti.

[Amazon Inspector](#) è un servizio di valutazione della sicurezza automatizzato che aiuta a migliorare la sicurezza e la conformità delle applicazioni distribuite sulle istanze Amazon EC2. Amazon Inspector esamina automaticamente le applicazioni per rilevare esposizione, vulnerabilità e deviazioni dalle best practice. Dopo aver eseguito una valutazione, Amazon Inspector fornisce un elenco dettagliato con i risultati dell'analisi, ordinati secondo il livello di gravità.

[Amazon CloudWatch Events](#) ti consente di configurare l'account AWS per inviare eventi ad altri account AWS o di diventare un ricevitore di eventi provenienti da altri account o organizzazioni. Questo meccanismo può essere molto utile per implementare scenari di risposta agli incidenti tra account, intraprendendo azioni correttive tempestive (ad esempio, invocando una funzione Lambda o eseguendo un comando su un'istanza Amazon EC2), se necessario, ogni volta che si verifica un evento di incidente di sicurezza.

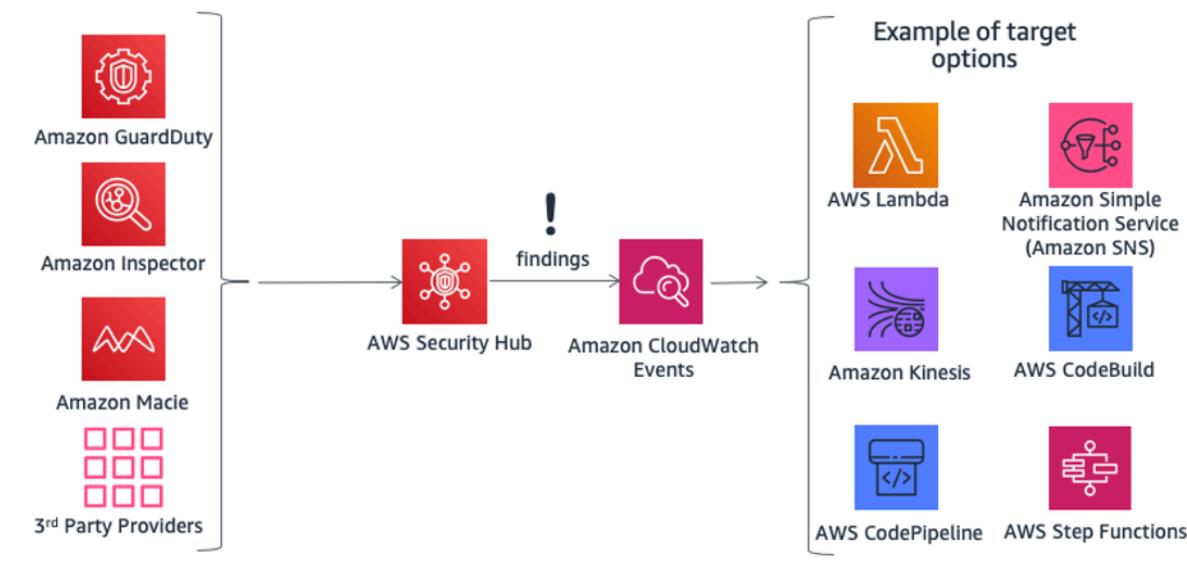


Figura 5. Intraprendere un'azione con AWS Security Hub e Amazon CloudWatch Events

[AWS Organizations](#) aiuta a gestire e governare in maniera centralizzata ambienti complessi.

Permette di controllare l'accesso, la conformità e la sicurezza in un ambiente multi-account. AWS Organizations supporta le [policy di controllo dei servizi \(SCP\)](#), che definiscono le operazioni disponibili sui servizi AWS che possono essere eseguite con account o unità organizzative (OU) specifici all'interno di un'organizzazione.

[AWS Systems Manager](#) offre visibilità e controllo dell'infrastruttura su AWS. Permette di visualizzare i dati operativi di più servizi AWS da una console unificata e di automatizzare le attività operative da eseguire su di essi. È possibile ottenere informazioni sulle attività recenti delle API, sulle modifiche alla configurazione delle risorse, sugli avvisi operativi, sull'inventario del software e sullo stato di conformità delle patch. Tramite l'integrazione con altri servizi AWS, puoi anche intervenire sulle risorse a seconda delle tue esigenze operative, assicurandoti che il tuo ambiente sia in uno stato di conformità.

Ad esempio, l'integrazione di Amazon Inspector con AWS Systems Manager ti permette di semplificare e automatizzare le valutazioni della sicurezza grazie alla possibilità di installare automaticamente l'agente Amazon Inspector offerta da Amazon Elastic Compute Cloud Systems Manager quando viene avviata un'istanza Amazon EC2. È possibile anche eseguire correzioni automatiche dei risultati di Amazon Inspector grazie alle funzioni di Amazon EC2 System Manager e Lambda.

Protezione dei dati in AWS

L'articolo 32 del GDPR stabilisce che le organizzazioni sono tenute ad "[...] attuare misure tecniche e organizzative appropriate per garantire un livello di sicurezza adeguato al rischio, che comprendono [...] la pseudonimizzazione e la crittografia dei dati personali [...]". Inoltre, le organizzazioni sono tenute a tutelarsi contro la divulgazione o gli accessi non autorizzati ai dati personali".

La crittografia riduce i rischi associati all'archiviazione dei dati personali perché rende i dati illeggibili a coloro che non possiedono la chiave corretta. Una strategia di crittografia completa può aiutare a mitigare l'impatto di eventi di sicurezza di vario tipo, tra cui alcuni tipi di violazione della sicurezza.

Crittografia dei dati a riposo

[La crittografia dei dati a riposo](#) è fondamentale per soddisfare la conformità alle normative e per garantire la protezione dei dati. Aiuta a garantire che i dati sensibili archiviati sui dischi non siano leggibili da utenti o applicazione senza una chiave valida. AWS offre diverse opzioni per la crittografia a riposo e la gestione delle chiavi di crittografia. Come, ad esempio, la possibilità di crittografare i dati arbitrari utilizzando il Kit SDK di crittografia AWS con una chiave di migrazione certificabile (CMK) creata e gestita in AWS KMS.

I dati crittografati possono essere archiviati in modo sicuro a riposo e decrittografati solo da una parte che dispone delle autorizzazioni per accedere alla CMK. AWS CloudTrail ti consente di usufruire di dati riservati crittografati in busta, di gestire le autorizzazioni e la crittografia autenticata attraverso meccanismi di policy e di registrare le verifiche. Alcuni dei servizi di AWS Foundation offrono funzionalità di crittografia a riposo integrate, che permettono di crittografare i dati prima che vengano scritti su una risorsa di archiviazione non volatile. Ad esempio, è possibile crittografare volumi Amazon EBS e configurare bucket S3 per la crittografia lato server (SSE) usando la crittografia AES-256. Amazon S3 supporta anche la crittografia lato client, che consente di crittografare i dati prima di inviarli ad Amazon S3. Gli SDK AWS supportano la crittografia lato client, che semplifica le operazioni di crittografia e decrittografia degli oggetti. Amazon RDS supporta anche la crittografia dei dati trasparente (TDE).

È possibile crittografare i dati negli archivi di istanze Amazon EC2 Linux utilizzando librerie Linux integrate. Questo metodo consente di crittografare i file in modo trasparente, proteggendo i dati riservati. Di conseguenza, le applicazioni che trattano i dati ignorano il livello di crittazione del disco.

È possibile utilizzare due metodi per crittografare i file negli archivi di istanze:

- **Crittografia a livello di disco:** consiste nella crittografia dell'intero disco, o di un blocco al suo interno, utilizzando una o più chiavi di crittografia. La crittografia del disco opera al di sotto del livello di file system, non si basa su un sistema operativo specifico e nasconde informazioni su directory e file come nome e dimensione. La crittografia del disco viene fornita, ad esempio, da Encrypting File System, un'estensione Microsoft di New Technology File System (NTFS) del sistema operativo Windows NT.
- **Crittografia a livello di file system:** con questo metodo, vengono crittografati i file e le directory ma non l'intero disco o la partizione. La crittografia a livello di file system opera su file system ed è trasferibile da un sistema operativo all'altro.

Per i [volumi di archiviazione di istanze SSD NVMe](#) (Non-Volatile Memory Express), la crittografia a livello di disco è l'opzione predefinita. I dati sull'archiviazione dell'istanza NVMe sono crittografati utilizzando un codice di cifratura a blocchi XTS-AES-256 implementato tramite un modulo hardware sull'istanza. Le chiavi crittografiche sono generate utilizzando il modulo hardware e sono univoche per ciascun dispositivo di storage dell'istanza NVMe. Quando l'istanza viene arrestata o terminata, tutte le chiavi crittografiche vengono distrutte e non possono essere ripristinate. Non è possibile utilizzare le proprie chiavi di crittografia.

Crittografia dei dati in transito

AWS consiglia vivamente di crittografare i dati in transito da un sistema all'altro, comprese le risorse all'interno e all'esterno di AWS.

Quando crei un account AWS, ad esso viene assegnata una sezione logicamente isolata del cloud AWS, denominata Amazon Virtual Private Cloud (Amazon VPC). Qui puoi avviare le risorse AWS in una rete virtuale definita da te. Ciò ti permette di avere il controllo completo sul tuo ambiente virtuale di rete, grazie alla possibilità di selezionare un intervallo di indirizzi IP personale, creare subnet, configurare tabelle di routing e gateway di rete e altro. Inoltre, ti consente di creare una connessione VPN hardware tra il tuo data center aziendale e la VPC per utilizzare il cloud AWS come estensione del data center aziendale.

Per proteggere la comunicazione tra l'Amazon VPC e il datacenter aziendale, puoi scegliere tra [diverse opzioni di connettività VPN](#) quella più adatta alle tue esigenze. L'AWS Client VPN permette di abilitare l'accesso sicuro alle risorse AWS che utilizzano servizi VPN basati su client. Puoi anche scegliere di utilizzare un'appliance VPN software di terze parti disponibile in AWS Marketplace, da installare su un'istanza Amazon EC2 nel tuo Amazon VPC. In alternativa, è possibile creare una connessione VPN IPsec per proteggere la comunicazione tra il VPC e la rete remota. È possibile

utilizzare [AWS Direct Connect](#) per creare una connessione privata dedicata da una rete remota all'Amazon VPC. Puoi combinare questa connessione con un AWS Site-to-Site VPN per creare una connessione privata crittografata IPsec.

AWS fornisce endpoint HTTPS che utilizzano il protocollo TLS, che garantisce una comunicazione crittografata in transito quando si utilizzano le API AWS. È possibile utilizzare il servizio [AWS Certificate Manager](#) (ACM) per generare, gestire e implementare i certificati privati e pubblici utilizzati per abilitare il trasporto crittografato tra i sistemi per i tuoi carichi di lavoro. ACM integra Elastic Load Balancing, che viene utilizzato per supportare i protocolli HTTPS. Quando viene utilizzato per distribuire i contenuti, Amazon CloudFront supporta la crittografia degli endpoint.

Strumenti di crittografia

AWS offre diversi servizi, strumenti e meccanismi di crittografia dei dati altamente scalabili per proteggere i dati archiviati ed elaborati in AWS. Per informazioni sulle funzionalità del servizio AWS e sulla sua gestione della privacy, consulta [Funzionalità del servizio AWS per considerazioni sulla privacy](#).

I servizi crittografici di AWS utilizzano un'ampia gamma di tecnologie di crittografia e archiviazione progettate per mantenere l'integrità dei dati a riposo o in transito. AWS offre quattro strumenti principali per le operazioni crittografiche.

- [AWS Key Management Service](#) (AWS KMS) è un servizio gestito da AWS che genera e gestisce sia [chiavi master](#) sia [chiavi di dati](#). AWS KMS è integrato [con molti servizi AWS](#) per fornire la crittografia lato server dei dati utilizzando AWS KMS chiavi provenienti dagli account dei clienti. AWS KMS I moduli di protezione hardware (HSM) sono certificati FIPS 140-2 livello 2.
- [AWS CloudHSM](#) fornisce moduli [HSM](#) certificati FIPS 140-2 livello 3. Permettono di archiviare in modo sicuro una varietà di chiavi crittografiche autogestite, comprese le chiavi master e le chiavi dei dati.
- Servizi e strumenti di crittografia AWS
 - [AWS Encryption SDK](#) fornisce una libreria di crittografia lato client per implementare operazioni di crittografia e decrittografia su tutti i tipi di dati.
 - [Amazon DynamoDB Encryption Client](#) fornisce una libreria di crittografia lato client per crittografare le tabelle di dati prima di inviarle a un servizio di database, come [Amazon DynamoDB](#).

AWS Key Management Service

[AWS Key Management Service](#) è un servizio gestito che semplifica la creazione e il controllo delle chiavi di crittografia utilizzate per crittografare i dati e utilizza moduli di protezione hardware (HSM) per garantire la sicurezza delle chiavi. AWS KMS è integrato con altri servizi AWS per aiutarti a proteggere i dati archiviati tramite questi servizi. AWS KMS è integrato anche con AWS CloudTrail per fornire i registri di tutti gli utilizzi delle tue chiavi e aiutarti a soddisfare le esigenze normative e di conformità.

È possibile creare, importare e modificare regolarmente le chiavi con la massima semplicità, nonché definire delle policy di utilizzo e monitorarne l'uso tramite la AWS Management Console oppure utilizzando AWS SDK o AWS CLI.

Le chiavi di migrazione certificabili (CMK) in AWS KMS, sia quelle importate sia quella create da KMS, vengono archiviate in formato crittografato in risorse di archiviazione estremamente durevoli, per semplificarne il recupero quando necessario. È possibile impostare KMS in modo che esegua la rotazione automatica delle chiavi CMK create in KMS una volta all'anno, senza dover crittografare nuovamente i dati già codificati utilizzando la chiave master. Non dovrai tenere traccia delle versioni precedenti delle chiavi CMK perché risulteranno sempre disponibili in KMS per decrittografare automaticamente i dati precedentemente crittografati.

AWS KMS permette di eseguire una serie di controlli sugli accessi, compresa la verifica delle concessioni e delle condizioni contenute nelle policy delle chiavi o nelle policy IAM, consentendoti di controllare chi ha accesso alle chiavi CMK e con quali servizi possono essere utilizzate. È inoltre possibile importare chiavi dall'infrastruttura di gestione delle chiavi in uso per impiegarle in KMS.

Ad esempio, la seguente policy utilizza la `kms:ViaService` di condizione per consentire l'utilizzo di una CMK gestita dal cliente per le azioni specificate solo quando la richiesta proviene da Amazon EC2 o Amazon RDS in una regione specifica (`us-west-2`) per conto di un utente specifico (`ExampleUser`).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:user/ExampleUser"
      }
    }
  ]
}
```

```
    "Action": [
      "kms:Encrypt*",
      "kms:Decrypt",
      "kms:ReEncrypt*",
      "kms:GenerateDataKey*",
      "kms:CreateGrant",
      "kms:ListGrants",
      "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "kms:ViaService": [
          "ec2.us-west-2.amazonaws.com",
          "rds.us-west-2.amazonaws.com"
        ]
      }
    }
  }
}
```

Integrazione con i servizi AWS

AWS KMS è integrato con una serie di servizi AWS. Consulta il [sito Web KMS](#) per un elenco completo dei servizi integrati. Queste integrazioni semplificano l'utilizzo di AWS KMSCMK per crittografare i dati archiviati attraverso questi servizi. Numerosi servizi integrati consentono di utilizzare, oltre a una CMK gestita dal cliente, una CMK gestita da AWS, creata e gestita automaticamente ma utilizzabile solo all'interno del servizio specifico che l'ha creata.

Funzionalità di verifica

[AWS CloudTrail](#) registra tutti gli utilizzi di una chiave archiviata in AWS KMS in un file di registro che viene distribuito al bucket Amazon S3 specificato dal cliente durante la configurazione di CloudTrail. Le informazioni registrate includono i dettagli relativi all'utente, la chiave, l'operazione eseguita, nonché la data e l'ora di utilizzo di tale chiave.

Sicurezza

AWS KMS è progettato per garantire che nessuno abbia accesso alle tue chiavi master. Il servizio è stato sviluppato su sistemi progettati per mantenere al sicuro le chiavi master con tecniche di protezione avanzate, ad esempio salvando su disco solo chiavi master crittografate, disattivandone l'archiviazione in memoria e selezionando i sistemi che possono accedere all'host e utilizzarle.

L'accesso al software di aggiornamento viene monitorato mediante un processo di controllo multilaterale che viene monitorato e verificato da un gruppo indipendente interno ad AWS.

Per ulteriori informazioni su AWS KMS, consulta il whitepaper [AWS Key Management Service](#).

AWS CloudHSM

Il [AWS CloudHSM](#) è un modulo di protezione hardware (HSM) basato su cloud che consente di soddisfare i requisiti di conformità aziendali, contrattuali e normativi in merito alla sicurezza dei dati, consentendo di generare e utilizzare le chiavi di crittografia su un hardware certificato FIPS 140-2 livello 3.

Con AWS CloudHSM è possibile controllare le chiavi di crittografia e le operazioni crittografiche eseguite dall'HSM.

I partner di AWS e Marketplace AWS offrono un'ampia gamma di soluzioni per la protezione dei dati sensibili all'interno della piattaforma AWS. Per applicazioni e dati soggetti a obblighi contrattuali o normativi relativi alla gestione delle chiavi crittografiche, può essere necessaria una protezione aggiuntiva. Fino ad ora, l'unica opzione era quella di archiviare i dati sensibili (o le chiavi di crittografia che proteggono i dati sensibili) On-premise nei data center locali. Questa soluzione ha probabilmente rappresentato un ostacolo alla migrazione delle tue applicazioni nel cloud o ne ha rallentato notevolmente le prestazioni. AWS CloudHSM ti consente di proteggere le tue chiavi di crittografia in HSM progettati e certificati secondo standard governativi che garantiscono una gestione sicura delle chiavi. È possibile generare, archiviare e gestire le chiavi utilizzate per la crittografia dei dati in maniera sicura, facendo in modo che solo tu abbia accesso ad esse. AWS CloudHSM consente di soddisfare i rigorosi requisiti di gestione delle chiavi all'interno del cloud senza compromettere in alcun modo le prestazioni dell'applicazione.

Il servizio AWS CloudHSM funziona con Amazon VPC. Le istanze AWS CloudHSM sono assegnate all'interno del tuo Amazon VPC con un indirizzo IP specificato da te, il che ti permette di avere una connettività di rete semplice e privata alle tue istanze Amazon EC2. Collocare le istanze HSM vicino alle istanze Amazon EC2 permette di diminuire la latenza di rete, migliorando così le prestazioni delle applicazioni. AWS fornisce un accesso dedicato ed esclusivo (a tenant singolo) alle istanze HSM, isolato rispetto a quello di altri clienti AWS. Disponibile in più regioni e zone di disponibilità, AWS CloudHSM permette di aggiungere alle tue applicazioni un'archiviazione delle chiavi sicura e durevole.

Integrazione con i servizi AWS e le applicazioni di terze parti

È possibile utilizzare CloudHSM con Amazon Redshift, Amazon RDS for Oracle o applicazioni di terze parti (ad esempio, SafeNet Virtual KeySecure) come radice di attendibilità, Apache (terminazione SSL) o Microsoft SQL Server (crittografia trasparente dei dati). È inoltre possibile utilizzare AWS CloudHSM per la scrittura di applicazioni e continuare a utilizzare le librerie crittografiche standard, tra cui PKCS #11, Java JCA/JCE e Microsoft CAPI e CNG.

Attività di verifica

Per tenere traccia delle modifiche alle risorse o delle attività di verifica per scopi di sicurezza e conformità, è possibile rivedere le chiamate API di gestione su AWS CloudHSM effettuate dal tuo account utilizzando AWS CloudTrail. Inoltre, è possibile controllare le operazioni nel dispositivo HSM con syslog o inviando messaggi di registro syslog all'agente di raccolta log.

Servizi e strumenti di crittografia AWS

AWS offre meccanismi conformi a un'ampia gamma di standard di sicurezza crittografica che ti consentono di implementare una crittografia basata sulle best practice. [AWS Encryption SDK](#) è una libreria di crittografia lato client disponibile in Java, Python, C, JavaScript e un'interfaccia a riga di comando che supporta Linux, macOS e Windows. Offre funzionalità avanzate di protezione dei dati, tra cui suite di algoritmi a chiave simmetrica sicuri e autenticati, come AES-GCM a 256 bit con derivazione e firma delle chiavi. Essendo stato progettato specificamente per le applicazioni che utilizzano Amazon DynamoDB, il [client di crittografia DynamoDB](#) consente agli utenti di proteggere i dati della tabella prima che vengano inviati al database. Inoltre, esegue la verifica e la decrittografia dei dati quando vengono recuperati. Il client è disponibile in Java e Python.

Infrastruttura Linux DM-Crypt

Dm-crypt è un meccanismo di crittografia Linux a livello di kernel che permette agli utenti di montare un sistema di file crittografati. Montare un file system significa collegarlo a una directory (punto di montaggio), rendendolo disponibile per il sistema operativo. Dopo il montaggio, tutti i file nel sistema di file sono disponibili per le applicazioni senza ulteriori interazioni. Questi file, tuttavia, vengono crittografati al momento di essere archiviati su disco.

Il mappatore dei dispositivi è un'infrastruttura nel kernel Linux 2.6 e 3.x che permette di creare in modo generico livelli virtuali di dispositivi a blocchi. Il target crypt del mappatore del dispositivo fornisce una crittografia trasparente di dispositivi a blocchi usando l'API di crittografia del kernel. La [soluzione in questo post](#) prevede l'utilizzo di dm-crypt in combinazione con un file system con backup

su disco mappato da Logical Volume Manager (LVM) su un volume logico. LVM esegue la gestione dei volumi logici per il kernel Linux.

Protezione dei dati fin dalla progettazione e per impostazione predefinita

Ogni volta che un utente o un'applicazione tenta di utilizzare la AWS Management Console, l'API AWS o l'interfaccia a riga di comando di AWS, viene inviata una richiesta ad AWS. Il servizio AWS riceve la richiesta ed esegue una serie di passaggi per stabilire se accettare o rifiutare la richiesta, in base a una [logica di valutazione delle policy](#) specifica. Tutte le richieste, ad eccezione delle richieste di credenziali di root, sono negate su AWS per impostazione predefinita (viene applicata la policy della negazione per impostazione predefinita). Ciò significa che tutto ciò che non è esplicitamente consentito dalla policy viene negato. Durante la definizione delle policy e come best practice, AWS suggerisce di applicare il [principio del privilegio minimo](#), il che significa che ogni componente (come utenti, moduli o servizi) deve poter accedere solo alle risorse necessarie per completare le proprie attività.

Questo approccio è in linea con l'articolo 25 del GDPR, che stabilisce che "il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate per garantire che, per impostazione predefinita, siano trattati solo i dati personali necessari per ciascuna finalità specifica del trattamento".

AWS fornisce anche strumenti per implementare l'infrastructure as code, un potente meccanismo per includere la sicurezza fin dal momento della progettazione dell'architettura. AWS CloudFormation fornisce un linguaggio comune per descrivere ed eseguire il provisioning di tutte le risorse dell'infrastruttura, comprese le policy e i processi di sicurezza. Con questi strumenti e pratiche, la sicurezza diventa parte del codice e può essere controllata, monitorata e modificata (con un sistema di controllo delle versioni) in base ai requisiti dell'organizzazione. In questo modo viene abilitata la protezione dei dati fin dalla progettazione, poiché è possibile includere i processi e le policy di sicurezza nella definizione dell'architettura e monitorarli costantemente mediante misure di sicurezza interne all'organizzazione.

In che modo AWS ti può aiutare

Tabella 1. In che modo AWS può aiutarti a gestire la conformità al GDPR

Area	Descrizione	Servizi e strumenti AWS
Solido framework di conformità	Tra le misure tecniche organizzative adeguate che possono essere richieste, ci sono "la capacità di assicurare su base permanente e la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento".	SOC 1 / SSAE 16 / ISAE 3402 (ex SAS 70) / SOC 2 / SOC 3 PCI DSS Livello 1 ISO 9001 / ISO 27001 / ISO 27017 / ISO 27018 NIST FIPS 140-2 Common Cloud Computing Controls Catalog (C5)
Controllo degli accessi ai dati	Il titolare del trattamento "... deve mettere in atto misure tecniche e organizzative adeguate per garantire che, per impostazione predefinita, siano trattati solo i dati personali necessari per	AWS Identity and Access Management (IAM) Amazon Cognito AWS Shield e AWS WAF AWS Resource Access Manager Amazon CloudFront AWS Organizations AWS CloudTrail

Area	Descrizione	Servizi e strumenti AWS
Monitoraggio e registrazione	<p>ciascuna finalità specifica del trattamento".</p> <p>"Tutti i titolari del trattamento e, ove applicabile, il rappresentante del titolare del trattamento, devono tenere un registro delle attività di trattamento sotto la propria responsabilità".</p> <p>"... il titolare del trattamento e il responsabile del trattamento devono attuare misure tecniche e organizzative adeguate per garantire un livello di sicurezza appropriato al rischio [...]"</p>	<p>AWS Config</p> <p>Amazon CloudWatch</p> <p>AWS Control Tower</p> <p>Amazon GuardDuty</p> <p>Amazon Inspector</p> <p>Amazon Macie</p> <p>AWS Systems Manager</p> <p>AWS Security Hub</p> <p>Strumenti e kit SDK AWS</p>

Area	Descrizione	Servizi e strumenti AWS
Protezione dei dati in AWS	Le organizzazioni devono "mettere in atto misure tecniche e organizzative appropriate per garantire un livello di sicurezza adeguato al rischio, tra le quali la pseudonimizzazione e la crittografia dei dati personali".	AWS Certificate Manager AWS CloudHSM AWS Key Management Service

Collaboratori

I collaboratori di questo documento includono:

- Tim Anderson, specialista tecnico di settore, Amazon Web Services
- Carmela Gambardella, Public Sector Solutions Architect, Amazon Web Services
- Giuseppe Russo, responsabile dei controlli di sicurezza, Amazon Web Services
- Marta Taggart, Senior Program Manager, Amazon Web Services
- Luca Iannario, Public Sector Solutions Architect, Amazon Web Services

Revisioni del documento

Data	Descrizione
Novembre 2017	Prima pubblicazione
Dicembre 2020	Aggiornato con l'aggiunta di nuovi servizi e funzionalità AWS.

Avvisi

I clienti sono responsabili della propria valutazione autonoma delle informazioni contenute in questo documento. Questo documento: (a) è solo a scopo informativo, (b) mostra 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 fa parte né modifica alcun accordo tra AWS e i suoi clienti.

© 2021, Amazon Web Services, Inc., o sue affiliate. Tutti i diritti riservati.

big blue[®] EYE



WHISTLEBLOWING

è il software
per la gestione delle segnalazioni in
conformità alla
Direttiva UE 2019/1937

La direttiva sul Whistleblowing in Italia

La Direttiva europea sul Whistleblowing nasce con l'obiettivo di rafforzare la protezione dei soggetti che segnalano violazioni delle disposizioni normative comunitarie su tutto il territorio dell'Unione e di armonizzare le legislazioni dei 27 Stati membri, con l'introduzione di uno standard minimo, imprescindibile, di tutela dei segnalanti dalle ritorsioni.



A chi si rivolge

PA

Tutte le amministrazioni pubbliche (art. 1, co. 2, del d. lgs. n. 165 del 2001)

AZIENDE

Tutte le aziende con più di 50 dipendenti

MOG 231

Aziende con MOG 231, indipendentemente dal numero di dipendenti

Attuazione della Direttiva Le date da ricordare



Entrata in vigore

Entrata in vigore del Decreto Legislativo 10 marzo 2023, n. 24, recante attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019



Obbligo per aziende con + 250 dipendenti

Data entro la quale le imprese con 250 o più dipendenti dovranno adottare le disposizioni del decreto



Obbligo per aziende con + 50 dipendenti

Entro questa data dovranno adeguarsi alla normativa anche le aziende che hanno impiegato tra i 50 e i 249 dipendenti nell'ultimo anno.

Fino al 15 luglio 2023, i whistleblower italiani continueranno a essere tutelati dal quadro normativo vigente (D. Lgs. 231/2001, L. 179/2017, L. 190/2012)

Che cosa cambia

Le aziende devono:

Dotarsi di un canale informatico sicuro

Le aziende dovranno acquisire un software per la gestione delle segnalazioni interno all'azienda che garantisca la riservatezza dell'identità del whistleblower tramite crittografia dei dati, progettato secondo i principi della privacy by design e by default in conformità al GDPR.

Comunicare la presa in carico

Occorre informare i whistleblower di aver ricevuto della segnalazione entro 7 giorni dall'invio e fornire riscontro entro 3 mesi dalla data di ricevimento, o 3 mesi e 7 giorni in caso di mancato avviso di ricezione.

Condividere le procedure

L'impresa deve mettere a disposizione informazioni chiare sulle procedure da seguire per effettuare una segnalazione, inserendole sia nel canale informatico che sul proprio sito internet.

LE POSSIBILI SANZIONI

PER CHI NON SI ADEGUA ALLA NORMATIVA

Dovessero verificarsi violazioni, ANAC avrà il potere di applicare al responsabile **sanzioni amministrative pecuniarie fino a 50.000 euro**.

- **Da 5.000 a 30.000 euro** in caso di ritorsioni o ostacoli alle segnalazioni, o violazioni della riservatezza.
- **Da 10.000 a 50.000 euro** nel caso non sia stato istituito il canale di segnalazione, non siano state adottate procedure di gestione o la gestione delle procedure non sia stata conforme, e in caso di mancato svolgimento dell'attività di verifica e analisi delle segnalazioni.

Decisamente più onerose sono le multe applicate per le **violazioni del GDPR**, con un tetto massimo pari al **2% del fatturato complessivo o 10 milioni di euro** nel caso di violazioni di dati personali (*data breach*).

PERCHE' RISCHIARE PESANTI SANZIONI?

big blue[®] EYE

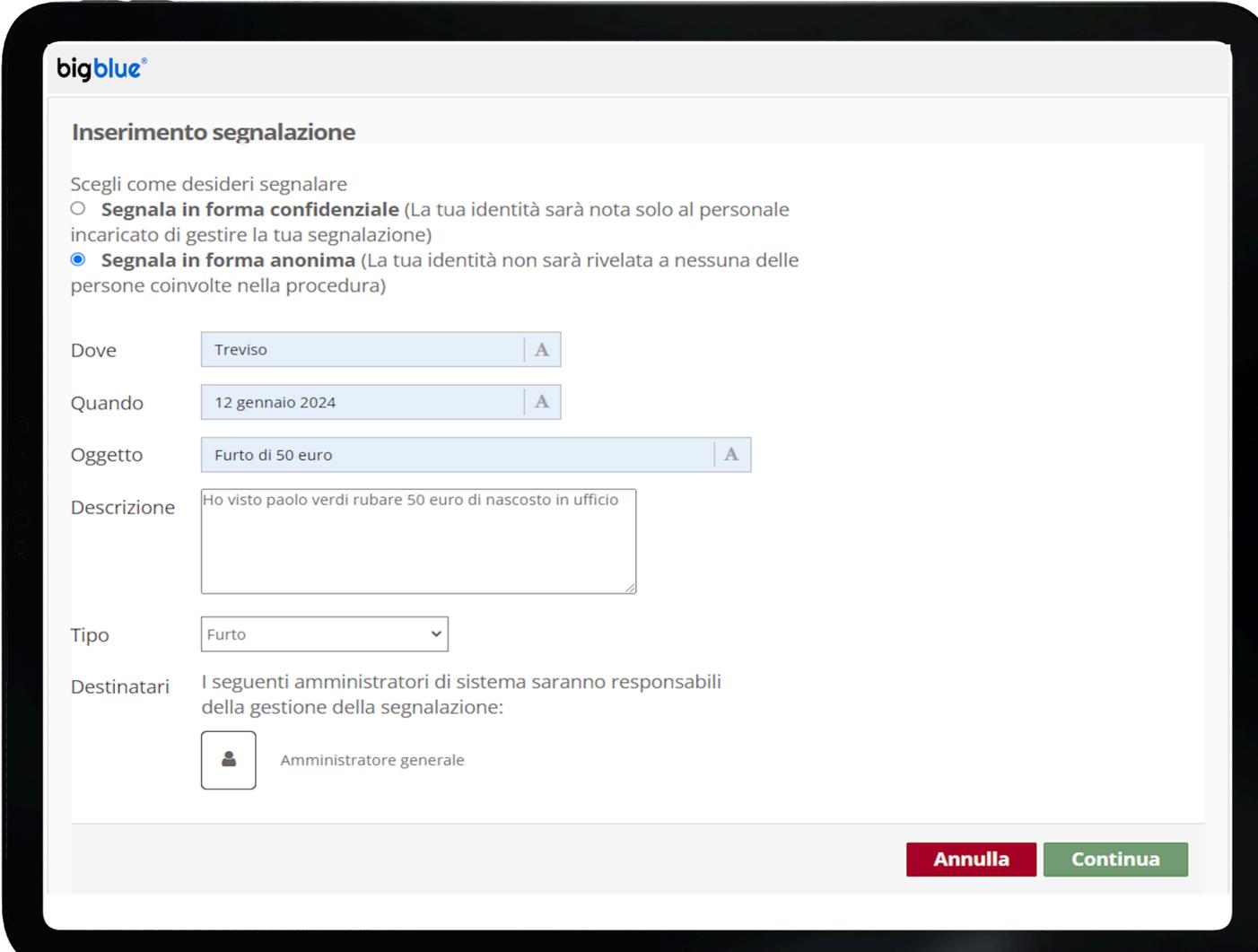
 **WHISTLEBLOWING**

- è la soluzione perfetta per adempiere in modo**
- **SEMPLICE**
 - **SICURO**
- alla normativa vigente**

Segnalazioni in forma

- Anonima
- Confidenziale

Consultazione anche su smartphone dello stato di avanzamento della segnalazione



bigblue[®]

Inserimento segnalazione

Scegli come desideri segnalare

Segnala in forma confidenziale (La tua identità sarà nota solo al personale incaricato di gestire la tua segnalazione)

Segnala in forma anonima (La tua identità non sarà rivelata a nessuna delle persone coinvolte nella procedura)

Dove **A**

Quando **A**

Oggetto **A**

Descrizione

Tipo

Destinatari I seguenti amministratori di sistema saranno responsabili della gestione della segnalazione:

 Amministratore generale

Annulla **Continua**



Segnalazioni in forma confidenziale:

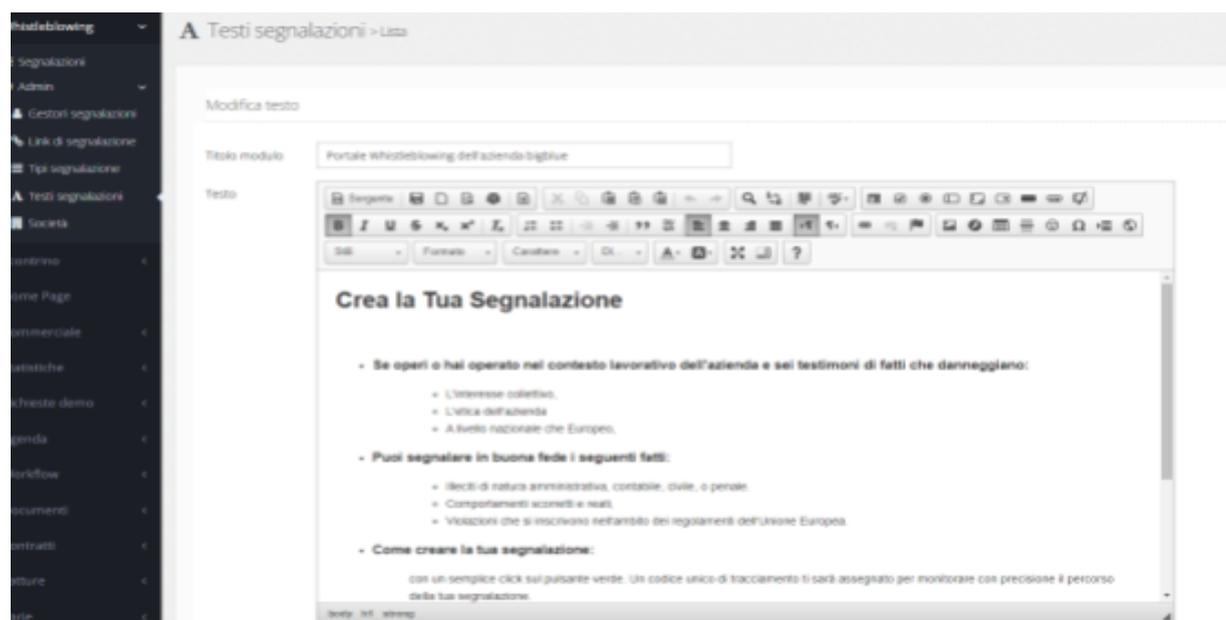
- Verifica identità del segnalante mediante token OTP su cellulare
- Completa protezione dell'identità del segnalante grazie alla crittografia dei dati
- firma digitale della segnalazione

Firmato da: Rossi Paolo
Numero telefonico: 3936468227
Transaction ID: 137
Transactiontoken: qZ4Ym
Ora/data firma: 12/01/2024 - 14:29:36.
Indirizzo IP: 188.125.106.133

Firma segnalante

Gli amministratori possono impostare

- testo del modulo segnalazione
- tipologie di segnalazione



CRM Tabelle > Lista

Q Ricerca

Nuova Voce

	Descrizione	Descrizione (en)
  	Furto	Furto
  	Abuso di potere	Abuso di potere
  	Abuso d'ufficio	Abuso d'ufficio
  	Altro	Altro
  	Comportamento inaccettabile	Comportamento inaccettabile
  	Conflitto di interessi	Conflitto di interessi
  	Corruzione	Corruzione
  	Diritti e tutele individuali	Diritti e tutele individuali
  	Frode	Frode
  	Frode negli appalti	Frode negli appalti
  	Sfruttamento, abuso	Sfruttamento, abuso
  	Altro	Altro

Assegnazione automatica delle segnalazioni ai responsabili associati alle categorie

- Ogni responsabile ha una categoria di illecito associata
- Quando un utente compila una segnalazione, la segnalazione verrà assegnata in automatico al gestore appropriato

Dati Anagrafici

Cognome: 

Nome: 

Cellulare: 

E-Mail: 

Tipo:

- Generale**
- Furto
- Abuso d'ufficio
- Abuso di potere
- Altro
- Comportamento inaccettabile
- Conflitto di interessi
- Corruzione
- Diritti e tutele individuali
- Frode
- Frode negli appalti
- Sfruttamento, abuso
- Altro



Ogni evento o attività viene certificato da data certa, fondamentale !!!! perchè:

Il segnalatore che non ha ricevuto riscontro entro i termini stabiliti, in merito alle misure previste o adottate per rispondere alla segnalazione (interna ed esterna) è autorizzato a divulgare pubblicamente informazioni sulle violazioni tramite

- stampa
- mezzi elettronici
- comunque tramite mezzi di diffusione in grado di raggiungere un numero elevato di persone

con conseguenze chiaramente dannose per l'azienda

Il modulo Whistleblowing di bigblue appone, dunque, automaticamente un certificato virtuale ad ogni attività svolta garantendo in questo modo certezza sui processi e sui tempi, opponibile anche in sede legale.

Tutti i dati sono su AWS (in miglior cloud secondo Gartner)

- **sempre aggiornati**
- **Totalmente crittografati**

RISIEDONO SU



**Il cloud più affidabile
attualmente disponibile**

big blue[®] EYE

 WHISTLEBLOWING

[SCOPRI DI PIU'](#)