# Protezione dei dati

# Codice di condotta per i provider di servizi di infrastrutture cloud

**27 GENNAIO 2017**

# Introduzione

I servizi di cloud computing forniscono dei vantaggi agli utenti del settore pubblico e privato, che comprendono riduzione dei costi, flessibilità, sicurezza e scalabilità. Un aspetto fondamentale per i clienti che desiderano utilizzare i servizi di cloud computing per il trattamento dei dati personali è l'adesione di tale trattamento alla normativa dell'UE applicabile in materia di protezione dei dati.

Vi è un'ampia gamma di provider di servizi cloud che fornisce molteplici modelli di cloud computing. Tuttavia, le considerazioni sulla protezione dei dati non sono applicabili uniformemente a tutti i modelli di cloud. L'estensione del trattamento dei dati personali da parte dei provider di servizi di cloud computing e l'entità del loro controllo sulla gestione dei dati dipendono dal tipo di servizi di cloud computing forniti. Inoltre i provider dei diversi tipi di servizi di cloud computing avranno necessariamente differenti ruoli e responsabilità, soprattutto in relazione alla protezione e alla sicurezza dei dati.

Ad esempio:

- Un provider di Software-as-a-Service (**SaaS**) generalmente offre come servizio un software applicativo appositamente concepito per il trattamento dei dati personali (per es. un servizio e-mail, un software ERP, servizi di marketing ecc.). Il provider del SaaS ha il potere di esercitare un ampio controllo sui dati personali trattati attraverso l'utilizzo del SaaS, nonché sulle modalità di tale trattamento dei dati. Pertanto, è in grado di offrire ai propri clienti impegni tecnici e contrattuali in base allo specifico SaaS fornito e che riflettono il grado di controllo di cui i provider del SaaS dispongono relativamente alla conformità della protezione dei dati.
- D'altro canto, un provider di Infrastructure-as-a-Service (**IaaS**) fornisce esclusivamente un hardware virtuale o un'infrastruttura informatica. I suoi clienti hanno piena libertà di scelta sulle modalità in cui tale infrastruttura viene utilizzata. Ad esempio, un cliente che fa uso di un IaaS può scegliere liberamente quali dati desidera elaborare mediante l'infrastruttura, in quali paesi, per quali scopi e come intende proteggere i dati. I provider di IaaS non sanno se la loro infrastruttura viene utilizzata dai clienti per il trattamento di dati personali. In virtù della natura stessa dello Iaas, i provider di Iaas non sono in grado di personalizzare i loro servizi in base a ciascun ambito di utilizzo da parte dello specifico cliente. Tuttavia, i provider di Iaas offrono i propri servizi con lo stesso livello di sicurezza a prescindere dall'utilizzo o meno dell'infrastruttura del provider di Iaas per il trattamento di dati personali da parte del cliente.

Il presente Codice di condotta (il **Codice**) è incentrato sui provider di Iaas. All'interno del presente Codice, i provider di Iaas vengono denominati "provider di servizi di infrastrutture cloud" (**CISP**). Lo scopo del Codice è consentire ai clienti di determinare se i servizi di un'infrastruttura cloud sono adatti al trattamento dei dati personali che il cliente desidera svolgere. La natura marcatamente variegata dei servizi di infrastruttura cloud rispetto ad altri tipi di servizi di cloud computing richiede un Codice specifico appositamente concepito per gli Iaas. Inoltre un Codice a parte consentirà di migliorare la comprensione dello Iaas all'interno dell'Unione europea generando trasparenza. Così facendo, sarà possibile contribuire alla creazione di un ambiente di fiducia, incoraggiando uno standard elevato riguardo la protezione dei dati. Nella fattispecie, ne avranno beneficio le piccole e medie imprese (**PMI**), nonché gli utenti, i provider, gli amministratori pubblici e non solo.

Il Codice comprende un insieme di requisiti rivolti ai CISP e agli incaricati del trattamento dati illustrati nella Sezione 4 (Requisiti per la Protezione dei dati) e nella Sezione 5 (Requisiti di trasparenza), i quali congiuntamente costituiscono i **Requisiti** del **Codice**. Inoltre, all'interno della Sezione 7 (Governance), viene illustrata una struttura amministrativa che ha lo scopo di facilitare l'applicazione, la gestione e l'evoluzione del Codice.

Il Codice è uno strumento facoltativo che permette al CISP di valutare e dimostrare la propria adesione ai requisiti del Codice relativamente a uno o a vari servizi offerti. La suddetta conformità può essere (i) attestata da un revisore indipendente di una terza parte o (ii) mediante l'autovalutazione del CISP e l'autodichiarazione di conformità.

I CISP che hanno dimostrato la propria adesione al Codice sulla base delle loro procedure di governance potranno utilizzare i corrispettivi marchi di conformità del Codice.

I clienti sono invitati a verificare che i Requisiti del Codice, qualsiasi altra garanzia contrattuale fornita dal CISP e le sue politiche siano conformi ai corrispondenti requisiti previsti dalla normativa dell'UE applicabile in materia di protezione dei dati. I clienti possono verificare l'adesione del CISP al Codice consultando la lista del sito web che elenca tutte le organizzazioni che hanno dichiarato la loro adesione al presente Codice (www.cispe.eu) (**Registro pubblico del CISPE**).

# 1 Struttura del codice

Il presente Codice è strutturato nella maniera seguente:

- **Scopo:** descrive il fulcro del Codice relativo alla normativa dell'UE applicabile in materia di **protezione dei dati**.
- **Ambito:** designa il campo di applicazione del Codice.
- **Requisiti per la protezione dei dati:** illustra i diritti e gli obblighi sostanziali dei CISP aderenti sulla base di principi chiave quali la limitazione delle finalità, i diritti del titolare dei dati, i trasferimenti, la sicurezza, la verifica, la responsabilità ecc.
- **Requisiti di trasparenza:** descrive le modalità in cui il CISP aderente dimostra di avere un adeguato livello di sicurezza per i dati personali.
- **Adesione:** descrive le condizioni in cui i CISP dichiarano la propria adesione al Codice.
- **Governance:** descrive le modalità in cui il Codice viene gestito, applicato e rivisto, ivi compresi i ruoli e gli obblighi dei suoi organi amministrativi.

# 2 Scopo

Lo scopo del presente Codice è consentire ai clienti di determinare se il servizio dell'infrastruttura cloud che desidera utilizzare è adatta alle attività di trattamento dei dati che il cliente intende svolgere. In definitiva, l'obiettivo del presente Codice è aiutare i clienti a scegliere il giusto servizio di infrastruttura cloud in base alle proprie esigenze specifiche.

La dichiarazione di adesione del CISP al presente Codice per un servizio specifico dovrebbe infondere fiducia e sicurezza fra i clienti sul fatto che:

- possono utilizzare quello specifico servizio per il trattamento dei dati personali in conformità con la normativa dell'UE applicabile in materia di protezione dei dati;
- il CISP soddisfa i Requisiti del Codice per tale servizio.

Nel momento in cui utilizzano un qualsiasi servizio di infrastruttura cloud, i clienti sono incoraggiati a svolgere la propria valutazione dell'attività di trattamento specifica e la sua conformità in base alla normativa dell'UE applicabile in materia di protezione dei dati. Il presente Codice ha lo scopo di assistere i clienti nelle suddette valutazioni ma non ne costituisce una sostituzione.

Il Codice non sostituisce il contratto tra il CISP e il cliente. Il CISP e il suo cliente sono liberi di stabilire le modalità di fornitura del servizio in un accordo per iscritto (**Contratto di servizio**). I CISP dovrebbero valutare se l'attuale Contratto di servizio da loro offerto ai nuovi clienti per i servizi entri in conflitto con i Requisiti del Codice, soprattutto prima di dichiararne la propria adesione.

Il Codice non rappresenta una consulenza legale. L'adesione al Codice non garantirà la conformità del CISP o di un cliente alla normativa applicabile. I CISP e i clienti sono invitati a ottenere una consulenza adeguata sui requisiti della normativa applicabile.

# 3 Ambito

Il Codice comprende un insieme di requisiti rivolti ai CISP e agli incaricati del trattamento dei dati con un'attenzione particolare rivolta alla sicurezza. Questi ultimi vengono illustrati nella Sezione 4 (Requisiti per la Protezione dei dati) e nella Sezione 5 (Requisiti di trasparenza). Nel Codice, i requisiti nel loro insieme vengono denominati Requisiti del Codice.

Qualsiasi CISP può dichiarare la propria adesione ai Requisiti del Codice per qualunque servizio di infrastruttura cloud se:

- il servizio soddisfa i Requisiti del Codice;
- relativamente a tale servizio, il CISP rispetta tutte le norme dell'UE applicabili in materia di protezione dei dati e ne è altresì vincolato, ivi compresa la Direttiva dell'UE sulla protezione dei dati personali (e qualsiasi altro recepimento a livello nazionale della stessa), nonché il Regolamento generale sulla protezione dei dati (GDPR), non appena sarà entrato in vigore;
- il servizio fornisce al cliente la capacità di scegliere di utilizzare il servizio per immagazzinare ed elaborare i propri dati completamente all'interno del SEE.

Al CISP è consentito di scegliere di dichiarare l'adesione ai Requisiti del Codice anche solo per alcuni specifici servizi dell'infrastruttura cloud. Tali CISP devono garantire che i potenziali clienti siano esplicitamente e inequivocabilmente informati su quali servizi aderiscono ai Requisiti del Codice. Qualsiasi CISP che dichiari la propria conformità al Codice deve essere in grado di soddisfare tutti i Requisiti del Codice per ciascun servizio oggetto di tale dichiarazione.

La corretta identificazione del responsabile del trattamento dei dati e di qualsiasi incaricato del trattamento dati è fondamentale per la normativa dell'UE in materia di protezione dei dati. I suddetti concetti vengono illustrati nella Sezione 4 (Protezione dei dati) del presente Codice.

Nell'ambito del servizio dell'infrastruttura cloud, il CISP avrà il ruolo di incaricato del trattamento

dei dati del cliente (il quale può essere a sua volta responsabile o incaricato). I Requisiti del Codice illustrano i principi che i CISP in qualità di incaricati del trattamento dei dati sono tenuti a rispettare.

Gli obblighi giuridici del responsabile del trattamento, stabiliti dalla normativa dell'UE applicabile in materia di protezione dei dati, presentano un ambito più ampio rispetto a quelli degli incaricati del trattamento dati. Gli incaricati del trattamento dati possono svolgere un ruolo di sostegno nell'ottemperanza degli obblighi del responsabile del trattamento dei dati. Il Codice cerca di spiegare le modalità in cui i CISP, in qualità di incaricati del trattamento dati, possono offrire assistenza ai propri clienti, che sono sia responsabili che incaricati del trattamento dei dati nella catena di fornitura.

Riguardo i dati trattati per conto di un cliente utilizzando il servizio di infrastruttura cloud, il CISP non (a) accederà né utilizzerà tali dati, salvo per quanto strettamente necessario per la fornitura dei servizi al cliente e non (b) gestirà tali dati per perseguire gli scopi del CISP, ivi compresi, nello specifico, finalità relative a data mining, profilazione o marketing diretto.

Al CISP è consentito di assolvere la funzione di responsabile del trattamento dei dati relativamente agli specifici dati personali fornitigli dal cliente. Tali dati comprendono, ad esempio, le informazioni relative agli account (tra cui i nomi utente, gli indirizzi e-mail e le informazioni di fatturazione), fornite al CISP dal cliente per la creazione o gestione dell'account del cliente utilizzato per accedere al servizio del CISP.

Il presente Codice non può essere applicato qualora il CISP possieda tali dati in qualità di responsabile del trattamento dati.

# 4 Requisiti per la protezione dei dati

La normativa dell'UE in materia di protezione dei dati fa una distinzione fra (a) il "responsabile del trattamento dei dati", parte che determina le finalità e gli strumenti del trattamento dei dati personali e (b) un "incaricato del trattamento dei dati", parte che gestisce i dati personali per conto del responsabile del trattamento.

I CISP forniscono un'infrastruttura self-service e on-demand che è completamente controllata dai clienti, anche per quanto riguarda l'upload sul servizio di infrastruttura cloud di qualsiasi dato personale e, in tal caso, le modalità in cui i dati personali vengono elaborati.

**Il cliente nel ruolo di responsabile o incaricato del trattamento**

I servizi dell'infrastruttura cloud vengono utilizzati come parte di una molteplicità di diverse operazioni commerciali che possono coinvolgere diverse parti nella catena di fornitura. Tuttavia, in linea generale, qualora il cliente archivi o elabori dati utilizzando i servizi del CISP:

- Il cliente diverrà responsabile del trattamento di tali dati personali qualora il cliente stabilisca le finalità per cui i dati verranno elaborati e abbia scelto le modalità in cui intende farlo.
- Il cliente diverrà incaricato del trattamento di tali dati personali qualora utilizzi il servizio del CISP esclusivamente per il trattamento dei dati personali per conto e in base alla volontà di una terza parte (che potrebbe essere il responsabile del trattamento o un'altra terza parte della catena di fornitura).

**Il CISP nel ruolo di incaricato del trattamento**

Qualora il cliente decida di archiviare o di elaborare i dati personali utilizzando i servizi del CISP, quest'ultimo diverrà l'incaricato del cliente.

**Scopo della presente sezione del Codice dedicata ai Requisiti per la protezione dei dati**

Lo scopo della presente Sezione 4 (Requisiti per la protezione dei dati) è chiarire il ruolo del CISP come incaricato del trattamento sulla base della normativa dell'UE applicabile in materia di protezione dei dati nell'ambito dei servizi di infrastruttura cloud.

Il Codice persegue questo obiettivo nel modo seguente:

a) individuando i requisiti per gli incaricati del trattamento in base alla normativa dell'UE applicabile in materia di protezione dei dati (**requisito per gli Incaricati del Trattamento**);
b) applicando i requisiti per gli Incaricati del Trattamento all'ambito dei servizi di infrastruttura cloud, distribuendo le responsabilità per il soddisfacimento di tali requisiti tra il CISP e il cliente e stabilendo i requisiti specifici del CISP sulla base del Codice (**Requisito** per il **CISP**).

Le responsabilità per il soddisfacimento di tali requisiti tra il CISP e il cliente e stabilendo i requisiti specifici del CISP sulla base del Codice (**Requisito** per il **CISP**).

Oltre al Codice, i CISP e i clienti sono invitati a tenere conto di tutti i requisiti previsti dalla normativa dell'UE applicabile in materia di protezione dei dati riguardo la corrispettiva fornitura e utilizzo dei servizi di infrastruttura cloud.

Un obiettivo chiave del Codice è illustrare i requisiti fondamentali dei CISP in base alla normativa vigente dell'UE in materia di protezione dei dati. In particolare, ciò comprende il GDPR, non appena entrerà in vigore, e i requisiti nel Codice sono definiti avendo come fonte di riferimento il suddetto regolamento. Il Codice verrà rivisto e aggiornato per adeguarlo alle modifiche apportate alla normativa dell'UE applicabile in materia di protezione dei dati, conformemente alla Sezione 7 (Governance), oltre a qualsiasi altra specificazione vincolante eventualmente fornita da un'autorità di vigilanza competente relativamente al GDPR.

### 4.1 Trattamento lecito dei dati personali

**Requisito per l'Incaricato del trattamento:**

Il responsabile del trattamento deve garantire che i dati personali vengano gestiti lecitamente. Il trattamento viene considerato lecito solamente se si verificano determinate condizioni. Salvo disposizione contraria sancita dalla legge, all'incaricato del trattamento è consentito elaborare i dati personali soltanto previa documentata istruzione da parte del responsabile del trattamento (come previsto dal punto 3, lettera a, dell'Art. 28 del GDPR).

**Requisito per il CISP:**

Il CISP potrà elaborare i dati personali conformemente alle istruzioni del cliente. Il Contratto di servizio e l'utilizzo da parte del cliente delle caratteristiche e funzionalità rese disponibili dal CISP come parte del servizio rappresentano le istruzioni complete e finali del cliente nei confronti del CISP relativamente al trattamento dei dati personali.

**Precisazione:**

I contenuti che sono oggetto dell'upload effettuato dal cliente attraverso il servizio (siano o meno dati personali) non possono in alcun modo essere controllati dai CISP. I CISP non hanno alcun ruolo nella decisione del cliente sull'utilizzo o il mancato utilizzo del servizio di infrastruttura cloud per il trattamento dei dati personali, il suo scopo e se/come ciò venga protetto. Pertanto, i CISP non sono in grado di valutare se esista o meno una base giuridica per il trattamento. Pertanto, la loro responsabilità si limita (a) al rispetto delle istruzioni del cliente con le modalità previste o che si evincono dal Contratto di servizio e (b) alla fornitura di informazioni sul servizio in conformità a quanto illustrato nella Sezione 5 (Requisiti di trasparenza) del Codice.

### 4.2 Termini e condizioni contrattuali per i servizi del CISP Requisito per l'Incaricato del trattamento

È necessario che il trattamento dei dati da parte di un incaricato venga disciplinato da un contratto scritto vincolante tra l'incaricato del trattamento e il responsabile del trattamento che stabilisca l'oggetto, la durata, la natura e lo scopo di tale trattamento, nonché il tipo di dati personali e le categorie di dati che sono oggetto degli obblighi e dei diritti del responsabile del trattamento. Il contratto può essere in formato elettronico. (come previsto dal punto 3 dell'Art. 28 del GDPR).

**Requisito per il CISP:**

È compito del CISP stabilire le caratteristiche del servizio e le modalità in cui viene fornito, nonché i diritti e i doveri del cliente nell'ambito del Contratto di servizio, conformemente a quanto illustrato nelle seguenti sezioni (a) e (b).

**Precisazione:**

I CISP forniscono un'infrastruttura. I clienti hanno piena libertà di scelta sulle modalità in cui tale infrastruttura viene utilizzata e possono stabilire, in qualsiasi momento, come e per quale scopo utilizzare l'infrastruttura.

### (a) Descrizione del trattamento

Per assecondare le caratteristiche dei servizi di infrastruttura e per evitare di dover modificare il Contratto di servizio o di stipularne uno nuovo ogniqualvolta il cliente o l'utente finale del cliente sceglie di modificare il modo in cui utilizza il servizio, la descrizione del trattamento all'interno del Contratto di servizio deve essere redatta in modo da agevolare le modifiche dei clienti ai loro casi di utilizzo.

Per una maggiore flessibilità, i Contratti di servizio possono offrire una descrizione generica del trattamento mediante l'uso dei servizi dell'infrastruttura cloud, ad esempio, "elaborazione, archiviazione e fornitura di contenuti nella rete del CISP".

### (b) Tipologia di Contratto di servizio

A condizione che venga messo per iscritto (anche in formato elettronico) e che sia legalmente vincolante, il Contratto di servizio stipulato tra il CISP e il cliente può assumere qualsiasi forma, comprese le seguenti:

- contratto unico;
- insieme di documenti, per esempio un contratto di base per i servizi con i relativi allegati (consensi per il trattamento dati, accordi sul livello di servizio, termini del servizio, politiche di sicurezza ecc.);
- termini e condizioni online standard.

### 4.3 Sicurezza

**Requisito per l'Incaricato del trattamento:**

Tenendo conto delle più recenti convenzioni in materia, i costi di applicazione, la natura, l'ambito, il contesto e le finalità del trattamento, nonché il rischio della diversa probabilità e gravità dei diritti e delle libertà delle persone fisiche, **sia l'incaricato che il responsabile del trattamento** devono mettere in pratica misure tecniche e organizzative che garantiscano un livello di sicurezza adeguato al rischio (come previsto dal punto 1 dell'Art. 32 del GDPR).

**Requisito per il CISP:**

**(a) Misure di sicurezza**

Il CISP adotterà e manterrà adeguate misure tecniche e organizzative relativamente alle infrastrutture dei data center, ai server e alle apparecchiature di rete del CISP e ai software host che sono sotto il suo controllo e che vengono utilizzati per fornire il suo servizio (**Rete del CISP**). Tali misure tecniche e organizzative dovrebbero (a) essere concepite per aiutare i clienti a proteggere i dati personali dal trattamento non autorizzato, la perdita, l'accesso a o la rivelazione realizzati in maniera accidentale o illecita e (b) per attribuire le responsabilità del CISP in materia di sicurezza, come illustrato nell'Allegato A (Responsabilità per la sicurezza).

**Precisazione:**

I servizi di infrastruttura cloud sono agnostici a livello dei contenuti. Offrono le stesse misure tecniche e organizzative e di sicurezza a tutti i clienti, indipendentemente dal loro trattamento dei dati personali o dalla natura, dall'ambito, dal contesto e dalle finalità del trattamento per il quale il cliente sta utilizzando il servizio.

Allo stesso tempo, il CISP non è l'unico responsabile della sicurezza nell'uso da parte del cliente del servizio di infrastruttura cloud. Ci sono alcuni aspetti chiave della sicurezza che sono di responsabilità del cliente (e non del CISP). Per esempio, il cliente (e non il CISP) è responsabile per la sicurezza dei sistemi operativi guest, le applicazioni ospitate nel servizio, i dati trasferiti e archiviati, le credenziali del cliente per effettuare il login al servizio e le politiche sulle autorizzazioni per il personale del cliente che utilizza il servizio.

L'Allegato A (Responsabilità in materia di sicurezza) definisce la responsabilità in materia di sicurezza

(a) del CISP e (b) del cliente nell'ambito del servizio di infrastruttura cloud.

I clienti devono rivedere (a) le informazioni rese disponibili dal CISP in relazione alla sicurezza dei dati nell'uso dei servizi (si veda la seguente Sezione *5*, Requisiti di trasparenza), (b) la configurazione prescelta dal cliente per il servizio di infrastruttura cloud e l'utilizzo delle caratteristiche e dei controlli disponibili per il servizio di infrastruttura cloud e (c) le misure di sicurezza che il cliente metterà in pratica riguardo agli aspetti della sicurezza che sono sotto la sua responsabilità e prenderà una decisione indipendente che, insieme a tali misure, consenta di fornire un adeguato livello di sicurezza per il trattamento che il cliente intende compiere utilizzando il servizio. Tale decisione deve basarsi sulla natura, l'ambito, il contesto e le finalità del trattamento desiderato dal cliente.
Dato che è il cliente a decidere quale trattamento effettuerà mediante il servizio (per esempio, con quali dati e scopi), sarà solo ed esclusivamente il cliente a decidere quale livello di sicurezza è più "adatto" ai dati personali che sono oggetto dell'archiviazione e del trattamento svolti utilizzando il servizio. Il CISP non è nella posizione di prendere tale decisione perché non monitora, limita né controlla quale tipo di trattamento verrà messo in atto dal cliente attraverso l'uso del servizio.

### (b) Programma per la sicurezza informatica

Il CISP osserverà un programma per la sicurezza informatica con lo scopo di (a) identificare i rischi ragionevolmente prevedibili e interni per la sicurezza della Rete del CISP e (b) ridurre al minimo i rischi per la sicurezza, anche grazie a valutazioni dei rischi e a test periodici.

Il CISP designerà uno o più membri del proprio personale come coordinatori e responsabili del programma di sicurezza informatica.

### (c) Valutazione continua

Il CISP condurrà revisioni periodiche sulla sicurezza della Rete del CISP e sull'adeguatezza del suo programma di sicurezza informatica. Il CISP può scegliere di rivedere il proprio programma per la sicurezza informatica alla luce di uno o più standard del settore relativi alla sicurezza. Il CISP valuterà in maniera continua la sicurezza della Rete del CISP per stabilire se si richiedono misure per la sicurezza aggiuntive o diverse per la difesa dai nuovi rischi per la sicurezza o sulla base dei risultati delle revisioni periodiche effettuate dal CISP stesso.

Il CISP può modificare i propri standard per la sicurezza di volta in volta, durante tutta la durata del Contratto di servizio, per offrire per lo meno lo stesso livello di sicurezza dichiarato dagli standard di sicurezza del CISP a partire dalla data di entrata in vigore del Contratto di servizio.

### 4.4 Trasferimento di dati personali verso paesi terzi

**Requisito per l'Incaricato del trattamento:**

Sia il **responsabile del trattamento** che l'incaricato del trattamento devono garantire che qualsiasi trasferimento di dati personali che siano oggetto del trattamento verso paesi terzi verrà effettuato solamente se si verificano le condizioni specifiche illustrate dalla normativa dell'UE applicabile in materia di protezione dei dati (come previsto dall'Art. 44 del GDPR).

**Requisito per il CISP:**

**(a) Luogo**

Il servizio di infrastruttura cloud fornisce al cliente la possibilità di scegliere di utilizzare il servizio per immagazzinare ed elaborare i propri dati all'interno del SEE.

**(b) Informazioni**

Il CISP fornirà al cliente le informazioni riguardo la regione e il paese in cui i dati vengono archiviati e trattati da o per conto del CISP, anche qualora il CISP affidi parte del trattamento a terze parti.

Per ragioni di sicurezza, è necessario indicare solamente un luogo generico (per esempio, la città o la regione). Tale descrizione generica dovrebbe per lo meno consentire al cliente di identificare quale Stato membro dell'UE eserciti giurisdizione sul trattamento da lui eseguito utilizzando il servizio.

Qualora fosse necessario assolvere a obblighi stabiliti da un'autorità di vigilanza competente, ai sensi della normativa applicabile in materia di utilizzo da parte del cliente del servizio e purché le informazioni siano protette da adeguati obblighi di riservatezza vincolanti per le autorità, il CISP deve comunicare all'autorità di vigilanza competente l'indirizzo esatto delle infrastrutture corrispondenti.

Nel caso di servizi realizzabili indifferentemente in molti luoghi diversi all'interno della Rete del CISP, i CISP dovranno rendere le informazioni facilmente accessibili da parte del cliente, permettendogli di selezionare i luoghi della Rete del CISP in cui i suoi dati verranno gestiti.

**(c) Livello di protezione**

Il CISP adotterà o renderà disponibile ai clienti uno standard di conformità riconoscibile sulla base

della normativa dell'UE applicabile in materia di protezione dei dati relativamente al lecito trasferimento dei dati personali verso il paese pertinente (comprensivo, ad esempio, delle Clausole contrattuali standard dell'UE, delle Norme societarie vincolanti o dello Scudo UE-USA per la privacy, che disciplina il trasferimento di dati personali verso gli Stati Uniti d'America) se:

i. il cliente trasferisce i dati che si trovano all'interno del SEE, oggetto di archiviazione mediante l'utilizzo del servizio del CISP, in qualsiasi paese al di fuori di esso al quale la Commissione europea non abbia riconosciuto un adeguato livello di tutela dei dati personali; o qualora

ii. il CISP venga autorizzato ad accedere ai dati archiviati utilizzando il suo servizio che si trova all'interno del SEE da un paese di cui al precedente punto (i).

### 4.5 Subincarico del trattamento

**Requisito per l'Incaricato del trattamento:**

**L'incaricato del trattamento** non deve coinvolgere un altro incaricato del trattamento senza la previa autorizzazione scritta, specifica o generica, da parte del responsabile del trattamento. In caso di autorizzazione scritta generica, l'incaricato del trattamento deve informare il responsabile del trattamento delle modifiche che intende apportare, lasciando al responsabile del trattamento la possibilità di opporsi (come previsto dal punto 2 dell'Art. 28 del GDPR).

**L'incaricato del trattamento** deve imporre ai suoi subincaricati i medesimi obblighi richiesti dalla normativa dell'UE applicabile in materia di protezione dei dati presenti nel contratto stipulato con il responsabile del trattamento. **L'incaricato del trattamento** deve rimanere pienamente responsabile per l'assolvimento degli obblighi da parte dei subincaricati nei confronti del responsabile del trattamento (come previsto dal punto 4 dell'Art. 28 del GDPR).

**Requisito per il CISP:**

### (a) Consenso

Nel rispetto della normativa applicabile, il CISP deve ottenere il consenso del cliente prima di autorizzare la terza parte subincaricata ad accedere ed elaborare i dati del cliente.

Il consenso del cliente può essere generalmente accordato mediante il Contratto di servizio. Nello specifico, il Contratto di servizio può delineare i casi e le condizioni in cui il CISP è autorizzato ad affidarsi a subincaricati per svolgere attività specifiche del trattamento per conto del cliente senza la necessità di ottenere aggiuntivi consensi da parte di quest'ultimo.

Qualora il cliente si opponesse alla partecipazione di un subincaricato, può avvalersi del recesso libero immediato del Contratto di servizio o, mediante decisione consensuale tra il cliente e il CISP, può porre subito fine al servizio fornito dal CISP per mezzo del relativo subincaricato, o a parte di esso.

### (b) Informazioni

Il CISP deve mantenere una lista attualizzata dei subincaricati autorizzati dal CISP ad accedere ai dati dei clienti. Tale lista deve comprendere il luogo e il subincaricato ed essere facilmente accessibile al cliente al momento dell'accettazione del Contratto di servizio e per tutta la durata dello stesso. È necessario fornire solamente un luogo generico (per esempio, la città o la regione). Tale descrizione generica dovrebbe per lo meno consentire al cliente di identificare quale Stato membro dell'UE eserciti giurisdizione sul trattamento da lui eseguito utilizzando il servizio.

Prima di autorizzare l'accesso ai dati dell'utente a un nuovo subincaricato, il CISP renderà disponibile al cliente le informazioni di cui sopra riguardanti il nuovo subincaricato.

### (c) Disposizioni per il subincarico

Il CISP imporrà al suo subincaricato gli stessi obblighi contrattuali per la protezione dei dati stabiliti all'interno del Contratto di servizio stipulato tra il CISP e il cliente.

Nei confronti del suo subincaricato, il CISP deve mettere in atto modalità operative che consentano di fornire un livello di protezione dei dati equivalente a quello stabilito dal Contratto di servizio. Il CISP deve essere in grado di dimostrare al cliente, per mezzo di una prova documentale idonea, che tali misure siano state adottate.

Il CISP deve limitare il trattamento dei dati dell'utente da parte del subincaricato alla misura necessaria a consentire la fornitura o il mantenimento dei servizi.

Il CISP resta responsabile per l'ottemperanza ai suoi obblighi in materia di protezione dei dati derivanti dal Contratto di servizio e per qualsiasi atto od omissione del subincaricato che configuri una violazione da parte del CISP di qualsivoglia obbligo stabilito dal Contratto di servizio.

Fatte salve le disposizioni di cui alle precedenti lettere (a) e (c), nonché quanto previsto dalla normativa applicabile, ai CISP è consentito di rivolgersi liberamente a subincaricati o fornitori (ivi compresi i fornitori di energia, apparecchiature, mezzi di trasporto, servizi tecnici, carrier IP, fornitori di transito e di hardware ecc.) per l'adempimento agli obblighi derivanti dal Contratto di servizio senza dover richiedere l'autorizzazione previa del cliente, purché i subincaricati e i fornitori non siano autorizzati ad accedere né a elaborare i dati del cliente.

### 4.6 Prova di conformità

**Requisito per l'Incaricato del trattamento:**

**L'incaricato del trattamento** deve rendere disponibile al responsabile del trattamento tutte le informazioni necessarie per dimostrare la propria ottemperanza agli obblighi sulla protezione dei dati e permettere revisioni e ispezioni da parte del responsabile del trattamento o di un revisore da lui nominato (come previsto dal punto 3, lettera h, dell'Art. 28 del GDPR).

**Requisito per il CISP:**

#### (a) Informazioni

I CISP devono fornire informazioni sufficienti riguardo i controlli sulla sicurezza messi in atto relativamente ai servizi resi disponibili ai clienti affinché questi ultimi possano ragionevolmente verificare la conformità del CISP agli obblighi sulla sicurezza previsti dal Contratto di servizio.

Qualora le informazioni non siano confidenziali né sensibili, verranno rese disponibili ai clienti mediante una procedura diretta (per esempio, per mezzo del sito web del CISP). Nel caso in cui le informazioni siano riservate, il CISP può renderle disponibili ai clienti su richiesta; tuttavia, potrebbe essere necessario che questi ultimi stipulino un accordo di non divulgazione ritenuto valido dal CISP. Il CISP, a sua esclusiva discrezione, può scegliere di non divulgare specifiche informazioni altamente sensibili.

I CISP possono richiedere ai clienti di pagare un costo aggiuntivo per ottenere le informazioni. Tale costo aggiuntivo dovrà essere ragionevole e non dovrà impedire ai clienti di accedere alle informazioni riguardanti i controlli di sicurezza relativi al servizio.

Il CISP può pubblicare le informazioni attuali sulla disponibilità del servizio e gli aggiornamenti riguardanti la sicurezza e i dettagli relativi alla conformità dei servizi sul proprio sito web.

Il CISP deve fornire un sistema (gratuitamente o a un costo ragionevole) affinché i clienti che hanno domande su questioni relative alla protezione dei dati e alla sicurezza del servizio possano richiedere di contattare il personale del CISP o un suo rappresentante designato attualmente incaricato di rispondere a tali quesiti. I sistemi dovrebbero essere idonei e proporzionati al servizio di infrastruttura cloud in questione e possono assumere la forma di numeri di telefono, indirizzi e-mail, sistemi chat o di qualsiasi altro metodo che permette al cliente di mettersi in contatto con i rappresentanti del CISP corrispondenti. Per adempiere a tale obbligo non è necessario accedere a, o conoscere, i dati del cliente.

**(b) Revisione**

Oltre ai requisiti sulle informazioni di cui sopra, i CISP possono avvalersi di revisori indipendenti terze parti per verificare l'idoneità dei controlli di sicurezza che vengono svolti sul servizio.

Qualora vengano offerte dal CISP, tali revisioni:

- verranno effettuate conformemente a uno standard di sicurezza riconosciuto (tra cui, per esempio, la norma ISO 27001);
- verranno realizzate periodicamente come previsto dallo standard applicabile;
- verranno effettuate da professionisti della sicurezza terze parti attendibili e indipendenti;
- si concluderanno con una relazione sulle revisioni.

Qualora il CISP ricorresse a revisori indipendenti terze parti per verificare l'idoneità dei controlli sulla sicurezza relativi al servizio, su richiesta scritta del cliente, il CISP può fornire a quest'ultimo una copia della relazione del revisore in modo tale che il cliente, il revisore del cliente e le autorità di vigilanza competenti, che abbiano giurisdizione sul cliente, possano ragionevolmente revisionare e verificare la conformità del CISP agli obblighi sulla sicurezza scaturiti dal Contratto di servizio. Il CISP può scegliere di addebitare ai clienti un costo aggiuntivo per la fornitura della relazione sulle revisioni purché tale costo non costituisca un deterrente.

La relazione rappresenta un'informazione confidenziale del CISP. Prima di consegnare la relazione al cliente, il CISP può chiedergli di stipulare un accordo di non divulgazione ritenuto valido dal CISP.

**Precisazione:**

Il Codice non richiede al CISP di autorizzare il cliente, o qualsiasi terza parte, a condurre una revisione nella sede dei locali o delle infrastrutture del CISP. I servizi di infrastruttura cloud sono ambienti multilocatari. Ciò significa che i dati di potenzialmente tutti i clienti del CISP possono essere ospitati negli stessi locali o infrastrutture. L'accesso fisico alle infrastrutture del CISP da parte di un singolo cliente o terze parti presuppone un rischio potenziale per la sicurezza di tutti i clienti del CISP, i cui dati vengono ospitati all'interno degli stessi locali e infrastrutture. Tale rischio può essere tenuto sotto controllo se, al posto di una revisione in loco, i clienti utilizzassero le informazioni fornite dal CISP per controllare ragionevolmente l'ottemperanza del CISP agli obblighi derivanti dal Contratto di servizio.

### 4.7 Richieste del titolare dei dati

**Requisito per l'Incaricato del trattamento:**

Tenendo conto della natura del trattamento, l'**incaricato del trattamento** deve assistere il responsabile del trattamento con misure tecniche e organizzative atte a permettergli, ove possibile, di adempiere all'obbligo di rispondere alle richieste basate sui diritti del titolare dei dati (come previsto dal punto 3, lettera e, dell'Art. 28 del GDPR).

**Requisito per il CISP:**

Il CISP darà al cliente la possibilità di rettificare, cancellare, circoscrivere o recuperare i propri dati. Il cliente può utilizzare tale facoltà per adempiere ai suoi obblighi e soddisfare le richieste derivanti dall'esercizio dei diritti del titolare dei dati.

Il CISP può fornire al cliente la possibilità di rettificare, cancellare, circoscrivere o recuperare i propri dati (a) come parte del servizio o (b) consentendo ai clienti di progettare e mettere in atto soluzioni proprie utilizzando il servizio.

**Precisazione:**

Oltre a mettere a disposizione del cliente la possibilità di rettificare, cancellare, circoscrivere o recuperare i propri dati, il CISP non è tenuto a fornire ulteriore assistenza al cliente riguardo alle richieste dei titolari dei dati. Questo perché è il cliente, e non il CISP, a essere il responsabile della gestione dei dati elaborati dal cliente per mezzo del servizio. Pertanto, il CISP non è a conoscenza di quali dati dei clienti siano oggetto di upload al servizio e, nello specifico, di chi siano i titolari di tali dati.

### 4.8 Il personale del CISP

**Requisito per l'Incaricato del trattamento:**

Gli **incaricati del trattamento** devono garantire che le persone da esso autorizzate al trattamento dei dati personali si siano impegnate a mantenere il riserbo o siano vincolate dall'obbligo legale di riservatezza corrispondente (come previsto dal punto 3, lettera b, dell'Art. 28 del GDPR).

**Requisito per il CISP:**

*Riservatezza:*

Il CISP imporrà adeguati obblighi contrattuali di riservatezza a tutti i membri del personale autorizzati dal CISP ad accedere ai dati del cliente.

*Controlli di accesso:*

Il CISP metterà in pratica e manterrà controlli di accesso e politiche per limitare il trattamento dei dati dei clienti a quei membri del personale del CISP che hanno l'esigenza di elaborare i dati dei clienti per fornirgli i servizi. Nel momento in cui il personale del CISP non avrà più bisogno di elaborare i dati dei clienti, il CISP revocherà prontamente i privilegi di accesso del personale.

### 4.9 Applicazione della legge/richieste delle autorità competenti

**Requisito per l'Incaricato del trattamento:**

Gli **incaricati del trattamento** possono dare applicazione a una sentenza giudiziaria o a una decisione amministrativa riguardo al trasferimento o alla rivelazione di dati personali richiesta da un paese terzo esclusivamente sulla base di un accordo internazionale (ad esempio, il Trattato bilaterale di assistenza giudiziaria, o MLAT) tra il paese terzo e l'UE o uno Stato membro (come previsto dall'Art. 48 del GDPR).

**Requisito per il CISP:**

Il CISP non rivelerà i dati del cliente agli organismi preposti all'applicazione della legge di un paese terzo a meno che sia necessario al fine di rispettare una sentenza giudiziaria, un ordine o una richiesta validi e giuridicamente vincolanti. Il CISP non rivelerà un numero maggiore di dati di quello strettamente necessario al rispetto della sentenza giudiziaria, dell'ordine o della richiesta pertinenti.

Qualora il CISP ricevesse una sentenza giudiziaria, un ordine o una richiesta validi e giuridicamente vincolanti da qualsiasi forza dell'ordine o autorità governativa affinché riveli i dati del cliente, a meno che sia vietato dalla legge, il CISP informerà il cliente prima della divulgazione per fornirgli la possibilità di tutelarsi rispetto a tale divulgazione.

Il CISP può disporre di linee guida pubbliche da utilizzare qualora organismi preposti all'applicazione della legge richiedano informazioni al CISP e può redigere relazioni almeno annuali sui tipi e il volume di richieste di informazioni elaborate dal CISP.

### 4.10 Violazione dei dati

**Requisito per l'Incaricato del trattamento:**

Gli **incaricati del trattamento** sono tenuti a notificare la violazione dei dati al responsabile del trattamento senza indebiti ritardi non appena ne vengono a conoscenza (come previsto dal punto 2 dell'Art. 33 del GDPR).

Tenendo conto della natura del trattamento e delle informazioni a disposizione dell'incaricato, l'**incaricato del trattamento** deve assistere il responsabile del trattamento nell'ottemperanza ai suoi obblighi di notifica della violazione dei dati all'autorità di vigilanza e ai titolari dei dati (come previsto dal punto 3, lettera f, dell'Art. 28 del GDPR).

**Requisito per il CISP:**

*Piano per la gestione degli incidenti riguardanti la sicurezza*

Il CISP deve adottare un piano per la gestione degli incidenti di sicurezza che indichi nel dettaglio le procedure che consentono di identificare e contrastare gli incidenti di sicurezza di cui il CISP venga a conoscenza.

Tale piano comprenderà:

- una guida per stabilire quali tipi di incidenti devono essere notificati al cliente sulla base del potenziale impatto sui dati.
- una guida su come gli incidenti devono essere affrontati;
- l'indicazione dettagliata delle informazioni che devono essere rese disponibili al cliente a seguito della violazione dei dati.

*Notifica della violazione dei dati*

*Ambito e tempistiche della notifica*

Qualora il CISP venga a conoscenza dell'accesso non consentito a qualsiasi dato personale dei clienti per mezzo delle apparecchiature o delle infrastrutture del CISP dando luogo alla perdita, rivelazione o alterazione di tali dati, il CISP notificherà l'accaduto al cliente senza nessun indebito ritardo.

*Contenuto della notifica*

La notifica (i) descriverà la natura della violazione della sicurezza, (ii) illustrerà le conseguenze della violazione, (iii) esporrà le misure messe in atto o proposte dal CISP in risposta all'incidente e (iv) fornirà un punto di contatto presso il CISP.

### 4.11 Cancellazione e restituzione dei dati personali

**Requisito per l'Incaricato del trattamento:**

In base alla decisione del responsabile del trattamento, l'**incaricato del trattamento** deve cancellare o restituire tutti i dati personali al responsabile del trattamento (cancellandone le copie esistenti) alla conclusione della fornitura del servizio (come previsto dal punto 3, lettera g, dell'Art. 28 del GDPR).

**Requisito del CISP:**

Il CISP fornirà al cliente la possibilità di recuperare e cancellare i dati del cliente. Il cliente può utilizzare tale facoltà per recuperare o cancellare i propri dati alla conclusione della fornitura del servizio.

In base al tipo di servizio, il CISP può fornire al cliente la possibilità di recuperare e cancellare i propri dati (a) come parte del servizio o (b) permettendo la creazione e l'applicazione di soluzioni proprie utilizzando il servizio.

**Precisazione:**

Il CISP non gestisce né sceglie di cancellare i dati del cliente al suo posto. Inoltre il CISP non è tenuto a fornire al cliente assistenza relativamente alla facoltà di quest'ultimo di ripristinare o cancellare i propri dati. Pertanto, spetta al cliente gestire la cancellazione e il ripristino dei dati utilizzando il servizio, tenendo conto di qualsiasi procedura a cui la risoluzione o la scadenza del Contratto di servizio abbia dato luogo.

# 5 Requisiti di trasparenza

I clienti devono essere in grado di poter eseguire accertamenti attendibili sui rischi per la sicurezza e sull'impatto sulla protezione dei dati relativamente ai dati personali elaborati attraverso i servizi di infrastruttura cloud.

Il CISP può offrire assistenza al cliente nel raggiungimento di tale obiettivo garantendo trasparenza riguardo alle misure per la sicurezza messe in atto dal CISP per proteggere i suoi servizi. Per fornire la trasparenza adeguata, il CISP perseguirà i 6 obiettivi seguenti:

1. La stipula di un Contratto di servizio con ripartizione della responsabilità tra il CISP e il cliente per la sicurezza del servizio.

2. Un'informativa di alto livello sugli obiettivi e gli standard di sicurezza relativi al servizio che comprendano, per lo meno, la Confidenzialità, la Disponibilità e l'Integrità.

3. Informazioni sul modello e la gestione del servizio che aiutino i clienti a comprendere le possibili minacce e le vulnerabilità che potrebbero derivare dal loro uso del servizio.

4. Informazioni attestanti i processi e i criteri per la gestione del rischio del CISP relativamente al servizio.

5. Informazioni sulle misure di sicurezza adottate dal CISP per il servizio.

6. Documentazione assicurativa sulla copertura del sistema di gestione della sicurezza informatica del CISP.

Le sottosezioni seguenti descrivono i passi che il CISP deve seguire per garantire un adeguato livello di trasparenza per ciascun servizio per il quale si dichiara l'adesione al Codice.

Il CISP può raggiungere tali obiettivi mettendo in atto un sistema per la gestione della sicurezza informatica che copra tutti e 6 gli obiettivi. Il Codice incentiva i CISP a mettere in pratica tali sistemi per la gestione della sicurezza informatica sulla base di uno o più standard del settore riconosciuti.

Fatti salvi i requisiti specificati all'interno del Contratto di servizio, il CISP può scegliere di comunicare le informazioni riferite nella Sezione 5 (Requisiti di trasparenza) ai propri clienti:

- fornendo informazioni riguardanti la sicurezza e le pratiche di controllo del CISP, e/o
- ottenendo certificazioni del settore e/o attestati di terze parti indipendenti, e/
- fornendo certificati, relazioni e altra documentazione direttamente ai clienti.

Qualora il CISP ritenga che le informazioni siano a carattere riservato, il CISP può renderle disponibili al cliente su richiesta; tuttavia, potrebbe essere necessario che il cliente stipuli prima un accordo di non divulgazione ritenuto valido dal CISP.

### 5.1 Contratto di servizio con ripartizione della responsabilità tra il CISP e il Cliente per la sicurezza del servizio

Il Contratto di servizio dovrebbe stabilire le responsabilità del CISP e del cliente relative alla sicurezza per tutta la durata del Contratto di servizio, a patto che il cliente resti responsabile per qualsiasi aspetto della sicurezza che non venga coperto dal Contratto di servizio.

Oltre al Contratto di servizio, il CISP può scegliere di rendere disponibile per la consultazione ulteriore

documentazione riguardante il servizio che descrive la ripartizione delle responsabilità per la sicurezza tra il CISP e il cliente. Per esempio, il CISP può fornire una griglia che descriva le responsabilità di entrambe le parti in base al loro controllo condiviso dell'ambiente informatico e dei controlli durante l'utilizzo del servizio.

### 5.2 Informativa di alto livello sugli obiettivi e gli standard di sicurezza relativi al servizio

Il CISP deve indicare (a) gli obiettivi per cui le misure di sicurezza messe in atto dal CISP per il servizio sono state create e, eventualmente, (b) gli standard che il CISP seguirà nel momento in cui metterà in atto tali misure di sicurezza.

Il CISP può modificare gli standard di sicurezza applicabili di volta in volta a patto che il servizio continui a offrire per lo meno lo stesso livello di sicurezza illustrato negli standard di sicurezza alla data di entrata in vigore del Contratto di servizio.

Il CISP informerà i clienti qualora il servizio di infrastruttura cloud sia stato creato dal CISP in modo tale da assistere i clienti adempiendo a uno standard o a un requisito legale riconosciuti applicabili a un tipo specifico di trattamento (per esempio, il trattamento di dati a carattere sanitario). Tali informazioni possono essere comunicate dal CISP ai clienti all'interno del Contratto di servizio, una descrizione del servizio o mediante il sito web del CISP o altro materiale pubblicamente disponibile.

### 5.3 Informazioni sul modello e sulla gestione del servizio

Il CISP dovrebbe fornire ai clienti informazioni sull'infrastruttura a loro resa disponibile e su come viene utilizzata per fornire il servizio (per esempio, le infrastrutture, la rete, l'hardware e il software operativo che supporta la fornitura e l'uso dei servizi).

Queste informazioni comprendono, ad esempio:

- L'architettura di alto livello dell'infrastruttura
- Il luogo generico delle infrastrutture che ospitano il CISP
- I subincaricati autorizzati dal CISP ad accedere ai dati dei clienti
- Le caratteristiche della sicurezza del servizio
- Opzioni che il cliente può utilizzare per incrementare la sicurezza del servizio

### 5.4 Informazioni attestanti i processi e i criteri per la gestione del rischio del CISP

Il CISP dovrebbe fornire informazioni ai clienti che attestino l'esistenza e l'idoneità del piano di gestione dei rischi del CISP per assistere i clienti nell'inclusione dei controlli del CISP nella propria gestione dei rischi. Tali informazioni possono, ad esempio, includere le valutazioni del rischio interne ed esterne svolte o incaricate dal CISP e comprese in una o più relazioni delle revisioni.

Il Codice incentiva il CISP a seguire una metodologia per la valutazione dei rischi basata su standard del settore riconosciuti.

## 5.5 Informazioni sulle misure di sicurezza adottate dal CISP per la prestazione del servizio

Il CISP deve fornire informazioni sufficienti riguardo alle misure di sicurezza in atto per i servizi resi disponibili ai clienti al fine di offrirgli assistenza nel comprendere i controlli del servizio che sono utilizzati e le modalità con cui i controlli sono stati approvati.

Tali informazioni sono volte ad aiutare i clienti a valutare se possono utilizzare e configurare i servizi in modo tale da ottenere un livello di sicurezza idoneo ai fini del trattamento che il cliente intende svolgere mediante l'uso dei servizi.

Nello specifico, il CISP dovrebbe descrivere:

- i processi di sicurezza, fisici e operativi, per la rete e le infrastrutture del server sotto la gestione del CISP; e
- le caratteristiche relative alla sicurezza e i controlli disponibili per l'utilizzo e la configurazione del servizio da parte dei clienti.

Queste informazioni comprendono, ad esempio:

- la sicurezza fisica e ambientale;
- la sicurezza della rete;
- la gestione della continuità delle attività;
- la gestione delle modifiche; e
- le caratteristiche dell'account relative alla sicurezza.

### 5.6 Documentazione assicurativa sulla copertura del sistema di gestione della sicurezza delle informazioni del CISP

Il CISP deve fornire le informazioni sufficienti riguardo al sistema di gestione della sicurezza informatica per i servizi resi disponibili ai clienti affinché questi ultimi possano ragionevolmente verificare la conformità del CISP agli obblighi sulla sicurezza previsti dal Contratto di servizio, illustrati nella Sezione 4.6 (Protezione dei dati, Prova di conformità) del presente Codice.

# 6 Adesione

I CISP per poter dichiarare la propria adesione al Codice devono soddisfare tutti requisiti del Codice per ogni servizio compreso nella sua dichiarazione e possono utilizzare i Marchi di conformità (come stabilito nella sottostante Sezione 6.2). I CISP non possono dichiarare di aderire solamente in parte ai Requisiti del Codice né escluderne specifiche sezioni.

I CISP che hanno dichiarato di aderire al Codice si impegnano a rispettare la Sezione 7 (Governance). Qualora un CISP non soddisfi i Requisiti del Codice, sarà oggetto dei meccanismi esecutivi illustrati nella Sezione 7 (Governance). Le misure di cui sopra non escludono qualsiasi sanzione eventuale da parte delle autorità di vigilanza competenti in base alla normativa dell'UE applicabile in materia di protezione dei dati.

### 6.1 Dichiarazione di adesione al Codice per un servizio

#### (a) <u>Dichiarazioni di adesione</u>

Per poter utilizzare i Marchi di conformità per un servizio, il CISP deve completare e inviare una dichiarazione di adesione (**Dichiarazione di adesione**) in conformità con le linee guida per l'adesione al Codice redatte dal CCTF e approvate dal Comitato esecutivo (**Linee guida per l'adesione al Codice**). L'attuale formulario della Dichiarazione di adesione è incluso nell'Allegato B. Tale elemento potrà essere attualizzato di volta in volta da parte del CCTF. La Segreteria pubblicherà e si occuperà di mantenere aggiornata la versione della Dichiarazione di adesione e le Linee guida di adesione al Codice all'interno del Registro pubblico del CISPE.

La Dichiarazione di adesione conferma che il servizio soddisfa i Requisiti del Codice.

Il CISP può scegliere tra le due seguenti procedure per supportare la propria Dichiarazione di adesione:

- Certificazione rilasciata da un revisore indipendente terza parte; o

- autodichiarazione del CISP.

A ciascuno dei due casi di Dichiarazioni di adesione corrisponde un diverso Marchio di conformità. Entrambe le procedure vengono illustrate nel dettaglio nelle seguenti sezioni (b) e (c).

La Segreteria dovrà rivedere la Dichiarazione di adesione in base alle Linee guida per l'adesione al Codice. Entro 40 giorni a partire dalla ricezione della Dichiarazione di adesione alla Segreteria, quest'ultimo dovrà notificare al CISP se la Dichiarazione di adesione è completa.
Se la Dichiarazione di adesione è incompleta, la Segreteria può richiedere al CISP di fornire i documenti o le informazioni richieste per completare la propria Dichiarazione di adesione.

Se la Dichiarazione di adesione è completa, la Segreteria deve includere la Dichiarazione di adesione nel Registro pubblico del CISPE entro 10 giorni lavorativi dalla data in cui la Segreteria ne comunica al CISP l'accettazione.

Una volta che la Dichiarazione di adesione viene inclusa nel Registro pubblico del CISPE:

- il CISP è autorizzato a utilizzare la Dichiarazione di adesione e il relativo Marchio di conformità, come illustrato nella sottostante Sezione 6.2, esclusivamente per i servizi coperti dalla Dichiarazione di adesione, purché resti valida e soggetta a qualsiasi misura esecutiva di cui alla Sezione 7.2 (Reclami ed esecuzione); e

- qualora una qualsiasi modifica del servizio comporti un aggiornamento del materiale allegato all'attuale Dichiarazione di adesione del CISP, è necessario che (i) il CISP informi prontamente la Segreteria e (ii) cooperi con la Segreteria fornendo il materiale aggiornato.

**(b) <u>Certificazione rilasciata da revisori indipendenti terze parti</u>**

<u>Procedura</u>

L'adesione ai Requisiti del Codice di uno o più servizi del CISP avviene presentando uno o vari certificati validi, relazioni di revisioni, attestati, dichiarazioni di applicazione o una documentazione equivalente che soddisfi tutti i Requisiti di adesione al Codice relativamente agli specifici servizi, elaborati da un revisore indipendente terza parte (**Certificato**). Tali requisiti rappresentano dei comportamenti atti a proteggere la sicurezza tecnica e operativa dei dati e che, come viene specificato all'interno delle Linee guida per l'adesione al Codice (**Requisiti del Codice verificabili**), nel settore vengono considerati verificabili.

I CISP che optano per questa procedura devono inviare alla Segreteria uno o più certificati che soddisfino tutti i Requisiti del Codice verificabili, allegando la propria Dichiarazione di adesione, in conformità con le Linee guida per l'adesione al Codice. I CISP devono inviare anche qualsiasi altra informazione di supporto che sia specificata all'interno delle Linee guida per l'adesione al Codice relativamente ai requisiti del CISP e che non rientri fra i Requisiti del Codice verificabili.

I CISP devono ottenere il Certificato rivolgendosi a una o più aziende di professionisti in contabilità e revisione, qualificate e attendibili, affinché eseguano una verifica o elaborino ulteriori relazioni o certificati di conformità per i servizi, seguendo una o più norme o schemi di certificazione per soddisfare tutti i Requisiti del Codice verificabili. Tali relazioni o certificati redatti da uno o più revisori andranno a costituire il Certificato, in base a quanto stabilito dalla presente sezione del Codice.

Qualora il CISP possieda già un certificato o una relazione per un servizio che soddisfa i requisiti del paragrafo precedente, il CISP può far valere tale certificato o relazione esistenti come Certificato per dimostrare che uno o più servizi aderiscono ai Requisiti del Codice verificabili senza dover effettuare una nuova revisione per ottenere un nuovo certificato o relazione.

Per l'ottenimento del certificato, il CCTF può consigliare specifiche aziende di professionisti in revisione e contabilità, così come norme o schemi di certificazione del settore. In tal caso, la Segreteria pubblicherà e manterrà aggiornata nel Registro pubblico del CISPE una lista di aziende, norme e schemi di certificazione. Tuttavia, ciò non impedisce al CISP di rivolgersi ad altre aziende o di ricorrere ad altre norme o schemi di certificazione.

Rinnovo

La Dichiarazione di adesione ottenuta per mezzo del Certificato è valida solamente per un anno a partire dalla data di inclusione nel Registro pubblico del CISPE.

Tuttavia, qualora né il servizio relativo al Certificato originale né il Codice siano stati modificati in modo sostanziale dal momento in cui il Certificato è stato emesso, il CISP può automaticamente estendere la validità della propria Dichiarazione di adesione per un altro anno in maniera gratuita, confermando la continuità dell'esattezza del Certificato e supportando le informazioni fornite (se presenti) alla Segreteria.

Negli altri casi, per continuare a utilizzare il Marchio di conformità, i CISP che si affidano alla Dichiarazione di adesione mediante Certificato devono rinnovare tale Dichiarazione di adesione ogni anno.

### (c) Autodichiarazione del CISP

Procedura

I CISP possono indicare che uno o più servizi aderiscono ai Requisiti del Codice completando

un'autodichiarazione, in conformità con le Linee guida per l'adesione al Codice.

I CISP che scelgono questa procedura devono inviare un Certificato di adesione alla Segreteria allegando qualsiasi informazione di supporto richiesta dalle Linee guida per l'adesione al Codice.

Rinnovo

La Dichiarazione di adesione ottenuta per mezzo dell'autodichiarazione è valida solamente per un anno a partire dalla data di inclusione nel Registro pubblico del CISPE.

Per continuare a utilizzare il Marchio di conformità, i CISP che si affidano alla Dichiarazione di adesione ottenuta con l'autocertificazione devono rinnovare tale Dichiarazione di adesione ogni anno.

### 6.2 Marchi di conformità

Il CCTF creerà dei marchi di conformità da utilizzare come simbolo pubblico indicante la conformità del servizio ai Requisiti del Codice (**Marchi di conformità**). I Marchi di conformità verranno approvati dal Comitato esecutivo.

Per aumentare la trasparenza nei confronti dei clienti, il CCTF creerà almeno due Marchi di conformità visivamente diversi per differenziare i CISP che hanno dimostrato la loro adesione ai Requisiti del Codice tramite: (a) una certificazione rilasciata da un revisore indipendente terza parte o (b) l'autodichiarazione da parte del CISP.

Il CCTF creerà e revisionerà le linee guida per l'utilizzo dei Marchi di conformità da parte dei CISP (**Linee guida per l'utilizzo dei marchi di conformità**). La Segreteria pubblicherà e manterrà aggiornata la versione delle Linee guida per l'utilizzo dei Marchi di conformità all'interno del Registro pubblico del CISPE.

Una volta che la Dichiarazione di adesione del CISP viene inclusa nel Registro pubblico del CISPE, il CISP può ritenersi autorizzato a usare il Marchio di conformità per tutto il periodo in cui la sua Dichiarazione di adesione resterà valida e purché il CISP utilizzi i Marchi di conformità: (a) esclusivamente per i servizi indicati nella Dichiarazione di adesione e (b) conformemente alle Linee guida per l'utilizzo del Marchio di conformità.

Qualora il CISP fornisca diversi servizi di infrastruttura cloud e non tutti siano coperti dalla Dichiarazione di adesione, il CISP deve garantire che il proprio utilizzo del Marchio di conformità identifichi inequivocabilmente i singoli servizi indicati nella Dichiarazione di adesione del CISP.

# 7 Governance

## 7.1 Assetto della governance

La governance del Codice è di responsabilità dell'Associazione di provider di servizi di infrastrutture cloud europei (**CISPE**). Lo schema sottostante fornisce una visione dell'assetto attuale del CISPE, comprensiva dei suoi organi chiave, la loro composizione e le rispettive responsabilità fondamentali.

| **Assemblea generale** |
|---|
| **Rappresentanza**: a ciascuna organizzazione partecipante spetta un rappresentante nell'Assemblea generale con diritto di voto. Non vi è limite al numero di organizzazioni partecipanti.<br><br>**Ammissibilità**: per essere ammessa come partecipante all'Assemblea generale, l'organizzazione deve (a) fornire ai clienti un servizio di infrastruttura cloud all'interno del SEE, (b) il servizio deve consentire ai clienti di scegliere se utilizzare il servizio per archiviare ed elaborare i propri dati completamente nel SEE e deve (c) dimostrare di avere almeno un servizio che aderisce al Codice entro 6 mesi dalla prima partecipazione all'Assemblea generale.<br><br>**Responsabilità fondamentali:** eleggere i rappresentanti del Comitato esecutivo e adottare le modifiche al Codice. Inoltre almeno il 10% dei membri, congiuntamente, può proporre al Comitato esecutivo delle modifiche del Codice. |
| **Comitato esecutivo** |
| **Rappresentanza**: dai 5 ai 10 rappresentanti, ciascuno dei quali proveniente da un diverso membro dell'Assemblea generale. I rappresentanti del Comitato vengono eletti dall'Assemblea generale.<br>**Ammissibilità**: per essere ammesso a presentare un candidato alle elezioni del Comitato esecutivo, un membro deve essere<br>(a) un membro fondatore o (b) (i) ricavare una parte sostanziale delle proprie entrate da servizi di infrastrutture cloud e (ii) possedere o esercitare un controllo effettivo sull'infrastruttura informatica fisica sottostante tali servizi di infrastrutture cloud.<br>**Responsabilità fondamentali:** approvare (a) l'ammissione di nuovi membri nell'Assemblea generale, (b) i marchi di conformità, (c) la procedura per i reclami relativi al Codice, (d) azioni esecutive derivanti dalla non conformità di servizi per i quali si dichiara l'adesione al Codice, (e) le linee guida per l'adesione al Codice e (f) le revisioni e le modifiche del Codice.<br>Nomina: (a) i rappresentanti del CCTF senza diritto di voto, (b) il Comitato per i reclami, (c) la Segreteria e (d) gli Osservatori. |
| **Unità operativa del Codice di condotta (CCTF)** |
| **Rappresentanza**: ciascuna organizzazione che fornisca almeno un servizio dichiarato aderente al Codice (che sia o meno un membro dell'Assemblea generale) può nominare un rappresentante nel CCTF con diritto di voto. Ciascun membro dell'Assemblea generale e del Comitato esecutivo può nominare rappresentanti nel CCTF senza diritto di voto (per esempio, esponenti del mondo accademico o esperti, rappresentanti di associazioni di utenti di servizi di infrastrutture cloud o rappresentanti della Commissione europea). Qualsiasi terza parte (compresi gli utenti finali) che desideri disporre di un rappresentante senza diritto di voto può inviare una richiesta scritta al Consiglio di amministrazione richiedendo un invito.<br>**Ammissibilità**: i rappresentanti devono provare: (a) la propria esperienza relativamente al cloud computing o sulla protezione dei dati e/o (b) avere conoscenze riguardo i modelli di business per il cloud computing.<br>**Responsabilità fondamentali:** valutare il Codice sulla base delle modifiche alla normativa dell'UE applicabile in materia di protezione dei dati, proporre al Comitato esecutivo modifiche al Codice, creare le linee guida per l'adesione al Codice, esprimere un'opinione non vincolante sulle proposte di modifica del Codice presentate dal Consiglio di amministrazione, consigliare revisori per le verifiche, norme e schemi di certificazione idonei come prova di adesione al Codice da parte degli enti, creare i marchi di conformità e mettere e a punto linee guida per l'uso dei marchi di conformità. |

| | | |
|---|---|---|
| **Comitato per i reclami**<br>**Rappresentanza:** la nomina proviene dal Comitato esecutivo.<br><br>**Responsabilità fondamentali:** (a) valutare i reclami riguardo la non conformità dei servizi rispetto al Codice e (b) adottare azioni esecutive nei confronti dei CISP non conformi e, se necessario, consigliare azioni esecutive al Comitato esecutivo. | **Segreteria Rappresentanza:** la nomina proviene dal Comitato esecutivo.<br><br>**Responsabilità fondamentali:** esaminare le dichiarazioni di adesione al Codice, pubblicare e mantenere attualizzate le informazioni sul Registro pubblico del CISPE, svolgere le mansioni amministrative del CISPE. | **Osservatori**<br><br>Il Comitato esecutivo può invitare dei rappresentanti che non hanno vincoli con i membri dell'Assemblea generale come partecipanti osservatori senza diritto di voto. |

## 7.2 Reclami ed esecuzione

### (a) Comitato per i reclami

Il Comitato esecutivo nominerà un Comitato per i reclami. Il Comitato per i reclami avrà le seguenti responsabilità: (a) valutare i reclami riguardo la non conformità dei servizi indicati nelle Dichiarazioni di adesione ai Requisiti del Codice da parte dei CISP e (b) adottare azioni esecutive nei confronti dei CISP non conformi e, se necessario, consigliare azioni esecutive al Comitato esecutivo.

### (b) Procedura per i reclami

Il Comitato per i reclami proporrà al Comitato esecutivo delle norme e una procedura per creare, decidere, impugnare e comunicare i risultati dei reclami riguardanti la conformità di servizi indicati nelle Dichiarazioni di adesione dei CISP rispetto ai Requisiti del Codice (**Procedura per i reclami**).

Una volta approvata dal Comitato esecutivo, il Comitato per i reclami pubblicherà, metterà in pratica, amministrerà e revisionerà regolarmente la Procedura per i reclami. La Segreteria pubblicherà e manterrà aggiornate le informazioni sulla Procedura per i reclami all'interno del Registro pubblico del CISPE.

Un membro del CISPE, un cliente o un'autorità di vigilanza competente può presentare un reclamo al Comitato per i reclami conformemente alla Procedura per i reclami. Il Comitato per i reclami deve rivedere e prendere una decisione sul reclamo in base alla Procedura per i reclami.

### (c) Esecuzione

Qualora la decisione finale del Comitato per i reclami deliberasse che il CISP è non conforme ai Requisiti del Codice, il Comitato per i reclami può:

- richiedere al CISP di rimediare entro tempi ragionevoli affinché possa divenire conforme al Codice; e

- per i casi di reiterata non conformità, o qualora il CISP non sia riuscito a prendere i provvedimenti richiesti (in alcun modo o non nei tempi stabiliti), può consigliare al Comitato esecutivo che la Dichiarazione di adesione del CISP venga sospesa o revocata per il servizio non conforme.

Nel caso in cui la Dichiarazione di adesione del CISP venga sospesa o revocata:

- la Segreteria dovrà prontamente rimuovere tali servizi dalla Dichiarazione di adesione del CISP presente sul Registro pubblico del CISPE;
- il Comitato per i reclami dovrà specificare, entro tempi ragionevoli, a partire da quando il CISP dovrà smettere di utilizzare il Marchio di conformità relativamente al servizio pertinente; e
- il CISP dovrà smettere di utilizzare il Marchio di conformità relativamente al servizio pertinente entro i tempi specificati dal Comitato per i reclami.

In caso di sospensione, tali misure devono essere rispettate fino a quando la sospensione non viene ritirata.

Le misure esecutive di cui sopra sono:

- le sole e uniche modalità in cui il CISP può porre rimedio alla non conformità ai Requisiti del Codice; e
- non pregiudicano in alcun modo i diritti dei clienti previsti dalla normativa dell'UE applicabile in materia di protezione dei dati né il Contratto di servizio.

La facoltà del cliente di presentare un reclamo non implica nessun diritto o rimedio del cliente nei confronti del CISP o del CISPE relativamente al Codice.

Il CISPE non si assume alcuna responsabilità riguardante la conformità al Codice da parte del CISP. Il CISPE non sarà altresì responsabile nei confronti di alcuna parte per qualsivoglia ragione o ipotesi di responsabilità per qualsiasi danno o perdita derivante da un'azione od omissione del CISPE o di un CISP relativamente al Codice.

### 7.3 Revisione del Codice e delle Linee guida

#### (a) Revisione del Codice

Il CCTF continuerà a rivedere il Codice sulla base delle modifiche alla normativa dell'UE applicabile in materia di protezione dei dati, specie con l'entrata in vigore GDPR.

Il CCTF deve aspirare a realizzare una completa revisione del Codice ogni due anni per poter

prendere in considerazione i nuovi sviluppi giuridici e tecnologici, come pure l'evoluzione delle migliori pratiche del settore.

Il Comitato esecutivo può dare inizio a una revisione specifica del Codice da parte del CCTF a seguito di una richiesta congiunta recapitata al CCTF da parte di almeno due membri del Comitato esecutivo. Il Comitato esecutivo può dare luogo a tale revisione di sua iniziativa o perché gli è stato richiesto da:

- almeno il 10% dei membri dell'Assemblea generale;
- un'autorità di vigilanza competente nell'esercizio delle sue funzioni ufficiali; o
- un'associazione che rappresenta gli interessi degli utenti di un servizio di infrastruttura cloud che agisca in veste ufficiale.

**(b) Modifiche al Codice**

A seguito della revisione, il CCTF può consigliare al Comitato esecutivo di apportare delle modifiche al Codice.

Le modifiche al Codice devono essere adottate dal CISPE prima che entrino in vigore.

Affinché possa essere adottata dal CISPE, qualsiasi modifica al Codice deve:

- essere presentata al Comitato esecutivo e all'Assemblea generale;
- essere approvata dal Comitato esecutivo; e
- essere adottata dall'Assemblea generale con un'apposita delibera.

Prima dell'approvazione del CISPE, il Comitato esecutivo può decidere di inviare una modifica al Codice affinché venga presa in considerazione e commentata a:

- un'autorità di vigilanza competente; e/o
- un'associazione che rappresenta gli interessi degli utenti di un servizio di infrastruttura cloud.

Non appena possibile, dopo la modifica del Codice da parte del CISPE, la Segreteria deve pubblicare una versione aggiornata del Codice nel Registro pubblico del CISPE.

I CISP sono tenuti a rinnovare o a riconfermare le proprie Dichiarazioni di adesione entro un anno a partire dalla pubblicazione della versione aggiornata del Codice sul Registro pubblico del CISPE. Qualora un CISP dichiari che il suo servizio è conforme ai Requisiti del Codice presentando un Certificato e allegando la propria Dichiarazione di adesione, può far valere un certificato esistente

per dimostrare che il servizio aderisce alla versione aggiornata del Codice senza dover effettuare una nuova revisione per ottenere un nuovo certificato o relazione.

# ALLEGATO A

Responsabilità in materia di sicurezza

**Introduzione**

Il presente Allegato stabilisce le responsabilità in materia di sicurezza (a) del CISP e (b) del cliente nell'ambito del servizio di infrastruttura cloud.

Il CISP è responsabile per il servizio di infrastruttura cloud che fornisce e non per i sistemi e le applicazioni sviluppate dal cliente utilizzando il servizio di infrastruttura cloud, i quali restano di responsabilità dei clienti.

## (1) Gestione della sicurezza informatica

### (a) Responsabilità del CISP

Il CISP deve disporre di una gestione a livello dirigenziale chiara e offrire assistenza sulla sicurezza del servizio.

Il CISP deve porre in essere un insieme di politiche per la sicurezza informatica approvate dai dirigenti che disciplinino la sicurezza del servizio.

Il CISP deve mettere in pratica un sistema di gestione della sicurezza informatica o misure equivalenti. L'ambito del sistema per la gestione della sicurezza informatica deve comprendere il servizio.

Il CISP designerà uno o più membri del proprio personale come coordinatori e responsabili del sistema di gestione della sicurezza informatica.

### (b) Responsabilità dei clienti

Il cliente deve disporre di un punto di contatto per suoi i clienti che si occupi delle questioni in materia di sicurezza relativamente al loro uso del servizio di infrastruttura cloud.

Il cliente deve svolgere una valutazione dei rischi per verificare l'idoneità del servizio di infrastruttura cloud per le attività di trattamento dei dati che il cliente desidera effettuare in conformità con la normativa dell'UE applicabile in materia di protezione dei dati.

## (2) Sicurezza delle risorse umane

### (a) Responsabilità del CISP

Il CISP deve porre in essere una struttura organizzativa per gestire l'applicazione della sicurezza informatica ai servizi del CISP con ruoli e responsabilità chiaramente definiti.

**(b) Responsabilità dei clienti**

Il cliente è l'unico responsabile per il suo personale e per qualsiasi terza parte acceda o utilizzi i servizi di infrastruttura cloud forniti al cliente (ivi compresi, ma non limitatamente a, contraenti, agenti e utenti finali).

**(3) <u>Gestione dell'accesso degli utenti</u>**

**(a) Responsabilità del CISP**

Il CISP deve fornire al cliente un sistema di gestione per il controllo degli accessi per il servizio di infrastruttura cloud come parte del servizio. Il sistema di gestione per il controllo degli accessi deve includere account nominativi, accessi e password basati sui ruoli o altri strumenti per l'autenticazione.

Il CISP non è responsabile per le soluzioni di accesso ai sistemi e le applicazioni utilizzate dal cliente attraverso il servizio di infrastruttura cloud.

**(b) Responsabilità dei clienti**

Il cliente è l'unico responsabile per l'uso e la configurazione dei sistemi di gestione per il controllo degli accessi forniti dal CISP. Il cliente deve essere responsabile per l'assegnazione dei diritti di accesso a personale idoneo.

Il cliente è responsabile per le soluzioni di accesso ai sistemi e alle applicazioni utilizzate dal cliente attraverso il servizio di infrastruttura cloud.

**(4) <u>Sicurezza fisica e ambientale</u>**

**(a) Responsabilità del CISP**

Il CISP deve applicare e attualizzare in maniera costante delle misure di sicurezza fisiche e ambientali per il servizio di infrastruttura cloud, create per offrire assistenza ai clienti nel proteggere i propri dati contro il trattamento non autorizzato, la perdita accidentale o illecita, l'accesso o la divulgazione.

**(b) Responsabilità dei clienti**

I clienti devono rivedere (a) le informazioni rese disponibili dal CISP relative alla sicurezza fisica e ambiente del servizio, (b) la configurazione del servizio prescelta dai clienti e l'uso delle

caratteristiche e dei controlli disponibili relativamente al servizio di infrastruttura cloud e (c) le misure di sicurezza che il cliente può mettere in atto per gli aspetti della sicurezza che sono sotto la sua responsabilità ed effettuare una valutazione indipendente per stabilire se l'insieme delle misure fornisce un livello di sicurezza adeguato al trattamento che il cliente realizzerà attraverso i servizi.

**(5) Server fisici e apparecchiature**

**(a) Responsabilità del CISP**

Il CISP è l'unico responsabile per lo sviluppo, l'operatività e la sicurezza di qualsiasi hardware fisico utilizzato per fornire il servizio di infrastruttura cloud e per qualsivoglia configurazione necessaria alla fornitura del servizio.

**(b) Responsabilità dei clienti**

Il cliente è l'unico responsabile per la gestione della corretta configurazione di qualsiasi sistema e applicazione da lui sviluppata sul servizio di infrastruttura cloud.

**(6) Gestione della protezione contro i malware**

**(a) Responsabilità del CISP**

Il CISP deve utilizzare una protezione contro i malware per i sistemi sensibili (per esempio, per i sistemi che sono comunemente colpiti o bersaglio di attacchi) che fanno parte del servizio di infrastruttura cloud.

**(b) Responsabilità dei clienti**

Il Cliente è responsabile per la gestione della protezione contro i malware per i sistemi e le applicazioni da lui utilizzate attraverso il servizio di infrastruttura cloud.

**(7) Gestione delle vulnerabilità**

**(a) Responsabilità del CISP**

Il CISP deve definire il livello di coinvolgimento (la ripartizione dei compiti tra il CISP, il ritardo tra il patch e l'applicazione del patch ecc.) relativamente al servizio di infrastruttura cloud.

**(b) Responsabilità dei clienti**

Il Cliente è responsabile per la gestione delle vulnerabilità dei sistemi e delle applicazioni

utilizzate dal cliente e ospitate dal servizio di infrastruttura cloud.

## (8) Registrazione e sorveglianza

### (a) Responsabilità del CISP

Il CISP deve fornire al cliente la sorveglianza (ad esempio livello, ambito, report, interfaccia, API) e strumenti per la registrazione (per esempio, accesso, registrazioni e durata delle registrazioni) relativamente al servizio di infrastruttura cloud.

### (b) Responsabilità dei clienti

Il cliente è l'unico responsabile per l'uso e la configurazione degli strumenti per la sorveglianza e la registrazione forniti dal CISP.

## (9) Vita utile delle apparecchiature

### (a) Responsabilità del CISP

Il CISP, prima di eliminare definitivamente il supporto di memoria utilizzato per archiviare i dati del cliente, deve realizzare una procedura di disattivazione del supporto di memoria. La procedura di disattivazione verrà realizzata in conformità con le pratiche standard del settore create per garantire che i dati del cliente non possano essere ripristinati dal tipo di supporto di memoria corrispondente attraverso alcuno strumento di ripristino dei dati o delle informazioni o mezzi analoghi.

### (b) Responsabilità dei clienti

I clienti devono rivedere (a) le informazioni rese disponibili dal CISP in relazione alla disattivazione del supporto di memoria, (b) la configurazione prescelta dal cliente per il servizio e l'utilizzo delle caratteristiche e dei controlli disponibili relativamente al servizio di infrastruttura cloud, e le misure di sicurezza che il cliente metterà in pratica per gli aspetti della sicurezza sotto la sua responsabilità, e dovranno svolgere una valutazione indipendente del fatto che l'insieme di tali misure fornisca un livello di sicurezza adeguato al trattamento che verrà realizzato attraverso i servizi.