ISO/IEC 27018:2025, Sicurezza delle informazioni, cibersicurezza e protezione della privacy: Linee guida per la protezione delle informazioni di identificazione personale (PII) nei cloud pubblici che agiscono come responsabili del trattamento di PII (3a edizione, 2025-08)

Protezione delle PII nel cloud pubblico

36 requisiti. Per questa norma non esiste un certificato accreditato. Versione di 07/2026.

ISO/IEC 27018 non è una norma di sistema di gestione, bensì un insieme di linee guida con controlli aggiuntivi che si innestano su ISO/IEC 27002:2022. Non esiste un certificato accreditato autonomo per ISO/IEC 27018. I controlli vengono recepiti nella Dichiarazione di applicabilità di un sistema ISO/IEC 27001, e il certificato viene quindi rilasciato in base a ISO/IEC 27001 con riferimento a ISO/IEC 27018. La norma si rivolge al fornitore di un servizio cloud pubblico che tratta informazioni di identificazione personale per conto dei propri clienti del servizio cloud. Un'organizzazione che si limita a utilizzare servizi cloud non assume questo ruolo e dovrebbe valutare in modo ragionevole i requisiti nei confronti dei propri fornitori, non di se stessa. Per Leanshift questa checklist è quindi soprattutto una griglia di valutazione dei fornitori. Ogni punto può essere posto al fornitore come domanda e messo per iscritto tramite l'accordo sul trattamento dei dati ai sensi dell'articolo 28 del RGPD. Il risultato di una tale valutazione è una registrazione interna di conformità o un profilo di valutazione del fornitore, non un certificato. Sulla numerazione: i punti da A.2 a A.12 seguono i principi sulla privacy dell'allegato A della norma, le voci numerate come A.11.6 sono i controlli aggiuntivi ivi elencati. Le voci numerate come 8.10 o 5.34 rimandano a controlli di ISO/IEC 27002:2022 che la norma rende specifici per il cloud. Le voci con il suffisso "(Grundsatz)", che significa principio, derivano dal principio del punto stesso, nei casi in cui l'allegato A non prevede un controllo aggiuntivo dedicato.

Azienda	Data	Redatto da

A.2 Consenso e scelta 2

A.2.1 **Il fornitore del servizio cloud supporta il cliente del servizio cloud nel soddisfare i diritti degli interessati, quali accesso, rettifica, cancellazione e opposizione. Le responsabilità e i termini sono stabiliti contrattualmente.** Documento

Come si dimostra: Come evidenza serve l'accordo sul trattamento dei dati ai sensi dell'articolo 28 del RGPD con una clausola di assistenza per i diritti degli interessati, insieme agli strumenti tecnici presenti nel servizio stesso: funzioni di esportazione, correzione ed eliminazione, oppure una procedura di supporto documentata con un termine di risposta. Domanda al fornitore: quale funzione o procedura offrite affinché possiamo evadere una richiesta di accesso o cancellazione entro un mese?

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.2 (Grundsatz) **Le informazioni di identificazione personale dei clienti del servizio cloud vengono trattate esclusivamente sulla base delle istruzioni documentate del cliente. L'ottenimento del consenso degli interessati resta compito del cliente in qualità di titolare del trattamento, e il fornitore non lo anticipa.**

Come si dimostra: Come evidenza serve la clausola sulle istruzioni nell'accordo sul trattamento dei dati, unita alla prova che il fornitore non fa un uso secondario dei dati, ad esempio l'informativa sulla privacy del servizio e la documentazione del prodotto. Domanda al fornitore: trattate in qualche modo i dati dei nostri clienti al di fuori delle nostre istruzioni, ad esempio per il miglioramento del prodotto o l'addestramento di modelli?

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.3 Legittimità e specificazione della finalità 2

A.3.1 **La finalità per cui il fornitore tratta le informazioni di identificazione personale è limitata all'erogazione del servizio concordato ed è indicata nel contratto. Non si effettua alcun trattamento per finalità proprie del fornitore.** Documento

Come si dimostra: Come evidenza serve l'accordo sul trattamento dei dati che indica oggetto, natura, finalità e durata del trattamento, nonché le categorie di interessati ai sensi dell'articolo 28, paragrafo 3, del RGPD. Domanda al fornitore: fornite l'allegato contrattuale che descrive in modo esaustivo la finalità del trattamento? Per le organizzazioni piccole è sufficiente l'addendum standard sul trattamento dei dati del fornitore, purché contenga queste informazioni.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.3.2 **Le informazioni di identificazione personale affidate al fornitore non vengono utilizzate per pubblicità, marketing o altre finalità commerciali proprie del fornitore senza consenso espresso preventivo. L'erogazione del servizio non è subordinata a tale consenso.**

Come si dimostra: Come evidenza serve una clausola contrattuale esplicita che escluda l'uso commerciale secondario, insieme alle condizioni di servizio. Domanda al fornitore: confermate per iscritto che i dati dei clienti non vengono utilizzati per pubblicità, profilazione o addestramento di modelli di IA? Se manca questo impegno, il servizio non è idoneo per le informazioni di identificazione personale.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.4 Limitazione della raccolta 1

A.4 (Grundsatz) **Oltre ai dati che il cliente inserisce nel servizio, il fornitore non raccoglie ulteriori informazioni di identificazione personale per finalità proprie, come telemetria, profili d'uso o analisi dei contenuti. I dati operativi e i metadati raccolti sono indicati e motivati.**

Come si dimostra: Come evidenza serve un elenco dei dati che il servizio registra oltre ai dati di contenuto (log di accesso, telemetria, dati diagnostici), con finalità e periodo di conservazione, insieme a una schermata dell'impostazione che disattiva la telemetria opzionale. Domanda al fornitore: quali dati di utilizzo, telemetria e diagnostica raccogliete in aggiunta, a cosa li utilizzate e possiamo disattivare tale raccolta?

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.5 Minimizzazione dei dati 2

A.5.1 **I file temporanei creati durante il trattamento delle informazioni di identificazione personale, come memoria di lavoro, cache o registri di rollback, vengono cancellati in modo sicuro entro un periodo definito.**

Come si dimostra: Come evidenza serve una procedura operativa o di cancellazione con un periodo di conservazione dichiarato per i dati temporanei, supportata dalla configurazione del sistema, ad esempio un TTL della cache o un'attività di pulizia pianificata con il relativo log di esecuzione. Domanda al fornitore: dopo quanto tempo vengono cancellati cache, file temporanei e stati intermedi, e come viene monitorato ciò?

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

8.11 **Ovunque le operazioni, i test o il supporto non richiedano dati reali, le informazioni di identificazione personale vengono mascherate, pseudonimizzate o anonimizzate. Il volume di dati trattati resta limitato a quanto effettivamente necessario per il servizio.**

Come si dimostra: Come evidenza serve una regola su quali ambienti possono accedere ai dati reali, insieme a schermate o script del mascheramento utilizzato nei sistemi di test e sviluppo. Domanda al fornitore: i vostri team di supporto e sviluppo lavorano con dati di produzione e, in tal caso, con quali garanzie? Per le organizzazioni piccole è sufficiente una regola secondo cui i sistemi di test funzionano esclusivamente con dati campione generati.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.6 Limitazione dell'uso, della conservazione e della divulgazione 3

A.6.1 **Quando il fornitore riceve una richiesta giuridicamente vincolante di divulgazione di informazioni di identificazione personale, ad esempio da un'autorità pubblica, ne informa preventivamente il cliente del servizio cloud, nella misura consentita dalla legge.**

Come si dimostra: Come evidenza serve una clausola contrattuale di notifica e un processo interno per le richieste delle autorità con un responsabile designato. Domanda al fornitore: ci notificate prima di consegnare i dati, e pubblicate un rapporto di trasparenza sulle richieste delle autorità? Un rapporto di trasparenza aggiornato costituisce un'evidenza solida.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.6.2 **Quando il fornitore divulga informazioni di identificazione personale a terzi, registra l'evento in modo che sia tracciabile: chi ha ricevuto i dati, quando è avvenuto, quali dati erano coinvolti e su quale base si fonda la divulgazione.** Documento

Come si dimostra: Come evidenza serve un registro delle divulgazioni o una cronologia dei ticket con questi campi, anche se non contiene voci. Un registro vuoto ma tenuto è accettabile ed è la via pratica per le organizzazioni piccole. Domanda al fornitore: tenete un registro delle divulgazioni di dati, e possiamo ottenerne estratti?

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

8.10 **Le informazioni di identificazione personale vengono cancellate al termine del periodo di conservazione concordato o alla fine del contratto, incluse le copie conservate nei backup dopo il relativo ciclo di rotazione.**

Come si dimostra: Come evidenza serve un concetto di cancellazione con periodi di conservazione per categoria di dati, il periodo di conservazione dei backup e un log o una conferma di cancellazione. Domanda al fornitore: per quanto tempo i nostri dati permangono nei vostri backup dopo la cessazione, e riceviamo conferma scritta della loro cancellazione?

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.7 Accuratezza e qualità 2

A.7 (Grundsatz) **Il fornitore non modifica di propria iniziativa le informazioni di identificazione personale che gli sono state affidate. Le correzioni e gli aggiornamenti vengono effettuati esclusivamente su istruzione del cliente del servizio cloud o tramite funzioni gestite direttamente dal cliente.**

Come si dimostra: Come evidenza servono le funzioni di modifica del servizio insieme alla relativa cronologia delle modifiche, oltre alla clausola sulle istruzioni nell'accordo sul trattamento dei dati. Domanda al fornitore: possiamo correggere i record autonomamente, e ogni modifica viene registrata in modo tracciabile?

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

8.13 **L'integrità delle informazioni di identificazione personale è protetta durante l'archiviazione, la trasmissione e il ripristino. Esistono backup e la loro ripristinabilità è stata testata.**

Come si dimostra: Come evidenza serve la configurazione dei backup, i meccanismi di checksum o integrità, e almeno un test di ripristino documentato all'anno con data e risultato. Domanda al fornitore: con quale frequenza testate i ripristini, e quale tempo di recupero garantite nel livello di servizio?

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.8 Apertura, trasparenza e informativa 2

A.8.1 **L'utilizzo di subfornitori che trattano informazioni di identificazione personale viene comunicato prima della conclusione del contratto. Le modifiche all'elenco vengono notificate al cliente con anticipo sufficiente, in modo che il cliente possa opporsi o recedere.** Documento

Come si dimostra: Come evidenza serve un elenco aggiornato dei subresponsabili del trattamento, pubblicato o reso disponibile contrattualmente, con nome, paese e finalità del trattamento, insieme a una regola di notifica ai sensi dell'articolo 28, paragrafo 2, del RGPD. Domanda al fornitore: dove troviamo il vostro elenco di subresponsabili, con quanto anticipo notificate le modifiche, e come possiamo opporci?

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.8 (Grundsatz) **Prima della conclusione del contratto, il fornitore mette a disposizione informazioni comprensibili su come vengono trattate le informazioni di identificazione personale, quali garanzie sono in atto e in quali giurisdizioni avviene il trattamento.**

Come si dimostra: Come evidenza servono l'informativa sulla privacy, un documento tecnico sulla sicurezza, una pagina del trust center e l'accordo sul trattamento dei dati comprensivo delle misure tecniche e organizzative come allegato. Domanda al fornitore: fornite l'elenco aggiornato delle misure tecniche e organizzative come allegato contrattuale, non solo come materiale di marketing?

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.9 Partecipazione individuale e accesso 2

A.9 (Grundsatz) **Il servizio fornisce al cliente del servizio cloud gli strumenti tecnici per evadere autonomamente le richieste di accesso, rettifica e cancellazione degli interessati, ad esempio tramite funzioni di esportazione, ricerca ed eliminazione.**

Come si dimostra: Come evidenza serve la documentazione del prodotto relativa alle funzioni di esportazione ed eliminazione, supportata da una prova interna: elaborare una richiesta di accesso dall'inizio alla fine e annotare quanto tempo richiede. Domanda al fornitore: possiamo individuare, esportare ed eliminare tutti i dati relativi a una singola persona senza il vostro supporto?

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

5.34 **Quando il cliente non è in grado di gestire autonomamente una richiesta di un interessato, il fornitore presta assistenza entro un termine concordato. Le richieste che gli interessati inviano direttamente al fornitore vengono inoltrate al cliente anziché essere evase dal fornitore.**

Come si dimostra: Come evidenza serve la relativa clausola nell'accordo sul trattamento dei dati con un termine di risposta concreto, insieme a una cronologia di ticket di supporto come esempio reale. Domanda al fornitore: quale termine garantite per l'assistenza sui diritti degli interessati, e quanto costa?

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.10 Responsabilizzazione 4

A.10.1 **Le violazioni che coinvolgono informazioni di identificazione personale vengono segnalate al cliente del servizio cloud senza ingiustificato ritardo, indicando la portata, i dati interessati, la causa e le misure adottate. Viene definito un processo di notifica con responsabilità e termini.** Documento

Come si dimostra: Come evidenza serve il piano di risposta agli incidenti con la relativa catena di escalation, il termine contrattuale di notifica (24-48 ore funziona nella pratica, in modo che il cliente possa comunque rispettare il termine di 72 ore ai sensi dell'articolo 33 del RGPD) e i registri di incidenti passati o di un'esercitazione. Domanda al fornitore: entro quale termine segnalate un incidente, tramite quale canale, e quali informazioni fornite insieme alla segnalazione?

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.10.2 **Le politiche di sicurezza, le procedure operative e i relativi registri vengono conservati per un periodo definito, in modo che il trattamento possa essere ricostruito a posteriori.** Documento

Come si dimostra: Come evidenza serve una regola di conservazione con la cronologia delle versioni delle politiche, ad esempio tramite un registro documentale o un sistema di controllo delle versioni con la data di approvazione. Domanda al fornitore: per quanto tempo conservate le versioni delle politiche e i relativi registri, e vi accediamo in caso di audit?

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.10.3 **Esiste un accordo definito per la restituzione, il trasferimento e la distruzione delle informazioni di identificazione personale al termine del contratto, che specifica formati, termini e trattamento delle copie.** Documento

Come si dimostra: Come evidenza serve la clausola di uscita nell'accordo sul trattamento dei dati, insieme a una conferma di cancellazione dopo la fine del contratto. Domanda al fornitore: in quale formato ed entro quale termine riceviamo indietro i nostri dati, quando vengono distrutte tutte le copie, e riceviamo conferma scritta?

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

5.35 **L'efficacia delle garanzie viene verificata in modo indipendente a intervalli regolari, ad esempio tramite audit interni, test di penetrazione o rapporti di assurance di terze parti. I risultati vengono messi a disposizione del cliente del servizio cloud in forma adeguata.**

Come si dimostra: Come evidenza serve un certificato ISO/IEC 27001 con una Dichiarazione di applicabilità che includa i controlli di ISO/IEC 27018, oppure un rapporto SOC 2, insieme a sintesi aggiornate dei test di penetrazione. Domanda al fornitore: fornite il certificato, il suo ambito di applicazione e la conferma che ISO/IEC 27018 sia riflessa nella Dichiarazione di applicabilità? Verificare se l'ambito copre realmente il servizio utilizzato.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.11 Sicurezza delle informazioni 13

A.11.1 **Chiunque abbia accesso a informazioni di identificazione personale è vincolato alla riservatezza, sia esso dipendente diretto o collaboratore esterno.** Documento

Come si dimostra: Come evidenza servono accordi o impegni di riservatezza firmati che restano validi dopo la cessazione del rapporto. Domanda al fornitore: tutto il personale e i fornitori di servizi con accesso ai dati sono vincolati per iscritto alla riservatezza?

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.11.2 **Le stampe e le altre copie cartacee contenenti informazioni di identificazione personale vengono create solo quando strettamente necessario. La portata consentita è disciplinata da una regola.**

Come si dimostra: Come evidenza serve una regola sulla gestione delle stampe, che nei data center consiste tipicamente in un divieto generale di stampa nelle aree in cui si trovano dati dei clienti. Domanda al fornitore: i dati dei clienti vengono mai stampati nelle vostre operazioni e, in tal caso, a quali condizioni?

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.11.3 **I ripristini dai backup vengono autorizzati preventivamente e registrati, indicando la persona che ha avviato il ripristino e i dati interessati.** Documento

Come si dimostra: Come evidenza serve il log dei ripristini con marca temporale, autore e ambito, generato solitamente in modo automatico dallo strumento di backup. Domanda al fornitore: registrate ogni ripristino, e possiamo consultare tali log in caso di audit?

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.11.4 **I supporti di archiviazione contenenti informazioni di identificazione personale che lasciano le sedi sono protetti contro l'accesso non autorizzato e la perdita, di norma tramite cifratura e un registro di trasporto.**

Come si dimostra: Come evidenza serve la prova della cifratura (cifratura completa del supporto), i registri di trasporto e consegna, e un inventario dei supporti. Domanda al fornitore: i supporti contenenti dati dei clienti lasciano mai le vostre sedi, ad esempio per i backup, e come vengono protetti durante il trasporto?

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.11.5 **L'uso di supporti e dispositivi portatili non cifrati per le informazioni di identificazione personale è vietato o limitato a eccezioni giustificate con approvazione documentata.**

Come si dimostra: Come evidenza serve una politica sui supporti rimovibili unita all'applicazione tecnica, ad esempio la cifratura obbligatoria dei dispositivi o il blocco delle porte USB tramite la gestione dei dispositivi. Domanda al fornitore: il personale può copiare dati dei clienti su dispositivi non cifrati, e cosa lo impedisce tecnicamente?

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.11.6 **Le informazioni di identificazione personale trasmesse su reti pubbliche vengono cifrate. I meccanismi utilizzati riflettono lo stato dell'arte attuale.**

Come si dimostra: Come evidenza serve la configurazione TLS (versione del protocollo aggiornata, nessun cifrario obsoleto) e un test esterno della configurazione documentato in un rapporto. Pratico per le organizzazioni piccole: eseguire una scansione TLS gratuita una volta all'anno e archiviare il risultato. Domanda al fornitore: quale cifratura di trasporto applicate obbligatoriamente, ed è attiva la cifratura dei dati a riposo?

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.11.7 **I documenti cartacei contenenti informazioni di identificazione personale vengono distrutti in modo da escludere qualsiasi ricostruzione.**

Come si dimostra: Come evidenza servono distruggidocumenti con un livello di sicurezza adeguato o certificati di distruzione rilasciati da un fornitore di servizi che opera secondo la norma DIN 66399 o una norma equivalente. Domanda al fornitore: come distruggete i documenti cartacei relativi ai clienti, e sono conservati i certificati di distruzione?

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.11.8 **Gli identificativi utente sono assegnati in modo univoco a una sola persona e non vengono né riassegnati né condivisi. Gli account condivisi esistono solo in eccezioni giustificate e con tracciabilità aggiuntiva.**

Come si dimostra: Come evidenza serve un elenco utenti del sistema di identità privo di account di gruppo, insieme alla regola secondo cui le attività amministrative vengono svolte tramite un account personale. Domanda al fornitore: il vostro personale operativo lavora con account personali, ed è obbligatoria l'autenticazione a più fattori?

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.11.9 **Il fornitore è in grado di indicare in qualsiasi momento quali persone o ruoli sono autorizzati ad accedere alle informazioni di identificazione personale, e mantiene aggiornata tale panoramica.** Documento

Come si dimostra: Come evidenza serve una panoramica dei diritti di accesso per ruolo, supportata da una revisione periodica degli accessi con data e risultato. Per le organizzazioni piccole è sufficiente un'esportazione semestrale dell'elenco utenti, con relativa approvazione. Domanda al fornitore: quanti membri del vostro personale possono accedere ai nostri dati, e con quale frequenza lo verificate?

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.11.10 **Gli account utente vengono gestiti lungo l'intero ciclo di vita: creazione, modifica e disattivazione tempestiva quando qualcuno lascia l'organizzazione o cambia ruolo.**

Come si dimostra: Come evidenza serve una procedura di attivazione e disattivazione con una checklist, insieme ai log degli account disattivati con marca temporale. Domanda al fornitore: entro quale termine revocate l'accesso al personale che lascia l'organizzazione, e come lo documentate?

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.11.11 **Gli obblighi di sicurezza e privacy del fornitore sono fissati contrattualmente, comprese le misure tecniche e organizzative, il carattere vincolante delle istruzioni del cliente e il diritto di audit del cliente.** Documento

Come si dimostra: Come evidenza serve l'accordo sul trattamento dei dati firmato ai sensi dell'articolo 28 del RGPD, con l'allegato delle misure e un diritto di audit o di informazione. Domanda al fornitore: fornite l'accordo sul trattamento dei dati firmato, compresi i relativi allegati, non un semplice rimando alle condizioni generali di servizio?

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.11.12 **I subfornitori che trattano informazioni di identificazione personale sono soggetti almeno agli stessi obblighi del fornitore stesso. La loro selezione e il monitoraggio continuativo sono disciplinati da un processo definito.**

Come si dimostra: Come evidenza serve il trasferimento degli obblighi nei contratti con i subfornitori (articolo 28, paragrafo 4, del RGPD) e una valutazione dei fornitori con data. Domanda al fornitore: come valutate i vostri subfornitori, e quali evidenze richiedete loro?

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.11.13 **Prima del riutilizzo dello spazio di archiviazione, viene garantito che nessun dato di utenti precedenti resti accessibile, né su supporti fisici né in ambienti virtualizzati.**

Come si dimostra: Come evidenza serve la procedura di sanificazione o sovrascrittura applicata alla liberazione dello spazio di archiviazione, i registri di distruzione dei supporti e la separazione tra tenant descritta nel documento di architettura. Domanda al fornitore: come garantite che lo spazio di archiviazione riutilizzato non contenga dati residui di altri clienti?

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.12 Conformità in materia di privacy 3

A.12.1 **I paesi in cui vengono archiviate e trattate le informazioni di identificazione personale sono indicati e noti al cliente del servizio cloud. Le modifiche alle sedi di archiviazione vengono notificate.** Documento

Come si dimostra: Come evidenza serve la panoramica delle sedi e delle regioni del fornitore, presente nel contratto o nella documentazione, insieme a una schermata dell'impostazione della regione del servizio utilizzato. Domanda al fornitore: in quali paesi risiedono i nostri dati, da quali paesi vi si accede, ad esempio per il supporto, e possiamo fissare la regione?

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.12.2 **I trasferimenti di informazioni di identificazione personale verso paesi terzi sono noti, motivati e coperti da garanzie adeguate.** Documento

Come si dimostra: Come evidenza servono le clausole contrattuali standard o una decisione di adeguatezza, supportate da una valutazione d'impatto del trasferimento, che per le organizzazioni piccole può essere breve: categorie di dati interessate, paese di destinazione, rischio, misure aggiuntive adottate. Domanda al fornitore: su quale base giuridica trasferite i dati verso paesi terzi, e quali misure supplementari applicate?

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

5.31 **I requisiti legali e contrattuali applicabili al trattamento delle informazioni di identificazione personale sono identificati e mantenuti aggiornati al variare del quadro giuridico. Vengono valutati i conflitti tra giurisdizioni.**

Come si dimostra: Come evidenza serve una panoramica dei requisiti applicabili (RGPD, normativa nazionale, obblighi settoriali specifici) con un responsabile e una data di revisione. In un'organizzazione piccola è sufficiente un elenco di una pagina, rivisto annualmente. Domanda al fornitore: voi o i vostri subfornitori siete soggetti a giurisdizioni che consentono alle autorità di accedere ai nostri dati, e come gestite questa situazione?

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione