BOLLINOCARE – VALUTAZIONE IMPATTO G.D.P.R.

RESPONSABILE DEL TRATTAMENTO			
Denominazione	Bollino IT S.p.A. a socio unico		
Partita Iva	06344961211		
Indirizzo	Via delle Industrie, 31		
Città	Napoli	Cap	80147
Legale Rappresentante	Ruggiero Bollino		
Data Protection Officer	Francesco Donato – DNTFNC83H28F839N f.donato@bollino.com		

Scopo del documento

Il presente documento ha lo scopo di consentire ai clienti di Bollino IT S.p.A. in qualità di Titolari del Trattamento di ottenere le informazioni necessarie ad effettuare la propria valutazione di impatto come prescritto dal Reg UE 2016/679.

Il documento è da considerarsi un supporto tecnico, come prescritto dalla normativa ogni valutazione è condotta dal Titolare del trattamento secondo le metodologie e le considerazioni che riterrà più idonee.

Contesto

Panoramica del trattamento

Quali sono le responsabilità connesse al trattamento?

BollinoCare è un applicativo fornito come servizio SaaS (Software as Service) in ambiente Cloud Azure; in quanto tale sono individuate diverse responsabilità connesse al trattamento da parte di diversi attori:

- Sono interessati finali del trattamento i pazienti delle strutture sanitarie che utilizzano il sistema ed i cui dati sono effettivo oggetto del trattamento da parte delle ulteriori parti interessate del processo
- Titolare del Trattamento del dato sanitario è la struttura sanitaria che utilizza BollinoCare in qualità di cliente di Bollino IT Spa a socio unico.
- Bollino IT è responsabile del trattamento per quanto attiene la manutenzione del software, gli aggiornamenti, la conservazione del dato, la gestione dei canali comunicativi, la gestione del server con riferimento alle attività direttamente

eseguibili da Bollino IT, il ripristino, i trattamenti effettuati dall'applicativo per le finalità contrattualmente definite (es. raggruppamento, estrazione dati, consegna a norma di legge alle strutture statali e ministeriali di riferimento quali ASL territoriali, Ministero della salute, Ministero Economica e Finanza, etc...)

- Microsoft si configura quale sub-responsabile del trattamento in ragione del rapporto contrattuale che sussiste tra Bollino IT e Microsoft Azure per l'architettura a supporto del funzionamento di BollinoCare.

Al fine di meglio identificare i ruoli, con riferimento ai servizi SaaS, sussiste tra Titolare del Trattamento e Responsabile del Trattamento un Data Processing Agreement per il quale il Titolare del Trattamento si configura quale Cloud Service Costumer (CSC), ovvero Cliente del Servizio Cloud mentre il Responsabile del Trattamento si configura quale Cloud Service Provider (CSP) ovvero Fornitore del Servizio Cloud.

Ci sono standard applicabili al trattamento?

UNI EN ISO 9001:2015
UNI EN ISO 13485:2016
UNI EN ISO 27001:2017
Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017,
Relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio
UNI CEN ISO/TR 14969 Dispositivi medici. Sistemi di gestione della qualità Guida all'applicazione della ISO 13485
UNI CEI EN ISO 14971 dispositivi medici. Applicazione della gestione dei rischi ai dispositivi medici
Regolamento (UE) 2017/745 relativo ai dispositivi medici – Allegato VIII
MedDev 2.4/1 rev. 9 – Classificazione

Quali sono le finalità di trattamento?

Il software ha una finalità definita contrattualmente con il cliente; è lo stesso cliente in qualità di titolare del trattamento che ha la responsabilità di garantire legittimità, specificità e rendere espliciti gli scopi del trattamento nei confronti dei propri pazienti. Il trattamento dei dati ha lo scopo di gestire il processo sanitario dal punto di vista IT, nel rispetto dei requisiti connessi alla normativa sui Dispositivi Medici in vigore.

Per quanto attiene l'accesso da parte di Bollino IT al software ed ai DB contenenti dati di natura personale, questo è specifico per le finalità contrattuale, esplicito poiché previsto dai requisiti di assistenza ed aggiornamento del software e legittimo poiché necessario per l'erogazione del servizio contrattuale. Tutto il personale di Bollino, in tal senso, è opportunamente e formalmente incaricato al trattamento (ovvero individuato ai sensi dell'art. 29 del GDPR) ed i relativi accessi sono memorizzati sui file di log che consentono idonea tracciabilità.

Quali sono le categorie di interessati?

Sono interessati del trattamento i pazienti della struttura sanitaria che si configura quale Titolare del Trattamento

Quali categorie di dati personali sono trattati?

Il software tratta dati personali e particolari categorie di dati personali (ovvero dati idonei a rilevare lo stato di salute) dei pazienti del titolare del trattamento. Sono trattati anche dati connessi alle condizioni di esenzione del paziente (anch'essi genericamente rientranti i particolari categorie di dati personali) e dati di natura amministrativa per il relativo processo di fatturazione, avvenga esso in regime privato o in regime di accreditamento con il Sistema Sanitario Nazionale.

Accessibilità dei dati da parte del Responsabile

Il Responsabile del Trattamento potrà accedere a tali dati esclusivamente tramite propri dipendenti e collaboratori all'uopo incaricati per finalità di natura manutentiva del sistema, previa richiesta assistenza da parte del Titolare del Trattamento. Per quanto attiene l'accesso da parte di Bollino IT al software ed ai DB contenenti dati di natura personale, questo è specifico per le finalità contrattuali, esplicito poiché previsto dai requisiti di assistenza ed aggiornamento del software e legittimo poiché necessario. Tutto il personale di Bollino, in tal senso, è opportunamente e formalmente incaricato al trattamento (ovvero individuato ai sensi dell'art. 29 del GDPR) ed i relativi accessi sono memorizzati sui file di log che consentono idonea tracciabilità.

Basi legali per il trattamento

BOLLINOCARE – VALUTAZIONE IMPATTO G.D.P.R.

L'applicativo è utilizzabile su base contrattuale; la liceità del trattamento lato cliente è una sua responsabilità in qualità di Titolare del Trattamento ed è suo onere garantire chiara ed idonea informazione sulle modalità di trattamento dei dati dei pazienti

Gli obblighi di Bollino IT in qualità di Responsabile del Trattamento sono in vigore per la durata del rapporto contrattuale tra le parti; nei casi in cui il rapporto contrattuale non fosse attivo, ovvero fosse sospeso per inadempienze amministrative, il processo di assistenza e manutenzione è da considerarsi sospeso, al pari del Ruolo di Responsabile del Trattamento di Bollino IT.

Misure di sicurezza connesse al trattamento implementate dal Responsabile del Trattamento

Crittografia

I dati sono conservati nel sistema in forma anonima e crittografata. Ogni eventuale perdita o copia della base dati ne rende impossibile la lettura.

Il Data Base che ospita i dati è Microsoft SQL Server con *[la presente informazione è omessa poiché non resa pubblica da Bollino IT S.p.A. I Titolari del trattamento possono richiedere il dettaglio all'azienda]*, per assicurare la crittografia dell'intera base dati.

Per le password di autenticazione è utilizzato un algoritmo *[la presente informazione è omessa poiché non resa pubblica da Bollino IT S.p.A. I Titolari del trattamento possono richiedere il dettaglio all'azienda]* non reversibile per calcolare l'hash della parola chiave. Il flusso dati avviene esclusivamente su *[la presente informazione è omessa poiché non resa pubblica da Bollino IT S.p.A. I Titolari del trattamento possono richiedere il dettaglio all'azienda]* con certificato specifico rilasciato da ente certificatore *[la presente informazione è omessa poiché non resa pubblica da Bollino IT S.p.A. I Titolari del trattamento possono richiedere il dettaglio all'azienda]* e rinnovato annualmente.

Anonimizzazione

Sebbene non sia prevista una procedura di anonimizzazione, è previsto l'inserimento di anagrafiche in modalità anonima senza obbligo di inserimento di dati identificativi del paziente da parte del Titolare del Trattamento.

Partizionamento

Il partizionamento è applicato su 3elementi: dati applicativi, logging attività e files.
I dati applicativi risiedono su un unico database; i dati di tracciamento delle attività (blackbox) vengono archiviati su un database *[la presente informazione è omessa poiché non resa pubblica da Bollino IT S.p.A. I Titolari del trattamento possono richiedere il dettaglio all'azienda]* fornito in cloud dalla piattaforma ufficiale e quindi completamente separati dall'ambiente applicativo Azure. I file prodotti (referti, moduli, etc....) sono archiviati sempre sulla piattaforma Azure, ma tramite i servizi di storage documentale offerti dalla stessa piattaforma.

Controllo degli accessi logici

Gli accessi avvengono mediante comunicazione sicura HTTPS (protocollo SSL) di credenziali di accesso (User e Password). Tutti gli accessi sono registrati con idonei file di log per permettere la tracciabilità delle attività e delle connessioni all'applicativo.

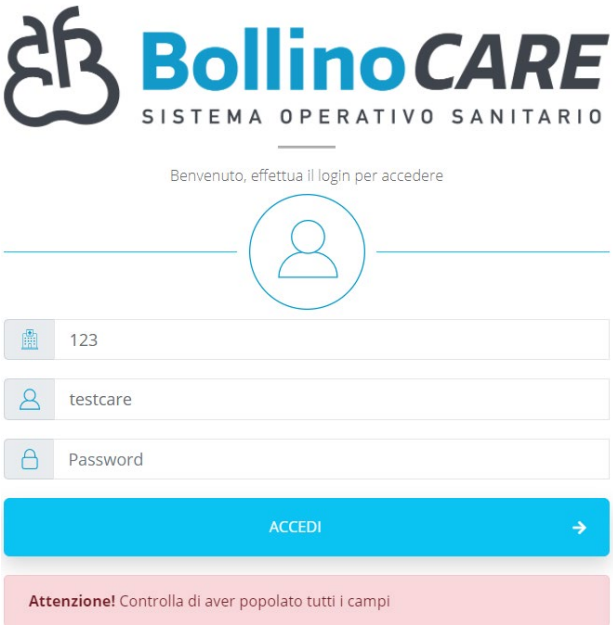
Di default i diritti di accesso sono minimi ed è responsabilità del Titolare del Trattamento settare le varie utenze secondo le proprie policy ed il proprio meccanismo di gestione dei diritti.

Per quanto attiene l'accesso del personale di Bollino IT, con finalità contrattuali di assistenza e manutenzione, anche questo è idoneamente tracciato al fine di garantire il Titolare del Trattamento in merito agli accessi effettuati da Bollino; altresì anche le utenze di Bollino IT sono divise secondo logiche di need to know e least privilege per minimizzare i rischi connessi alle attività.
Le regole di composizione della password prevedono:
1. La password deve essere lunga almeno 8 caratteri.
2. Deve rispettare almeno 3 dei seguenti requisiti:
   - contenere almeno una lettera minuscola
   - contenere almeno una lettera maiuscola
   - contenere almeno un numero
   - contenere almeno uno dei seguenti caratteri speciali: (~!@#$%^&*()_+-={}|[]"\+:;'<>?,./)
3. La stessa password non può più essere riutilizzata
4. La password scade ogni 90 giorni

In fase di immissione della password, la scrittura della stessa è resa non visibile a schermo di default, in modo da garantire che non possa essere sottratta, ad esempio, in ambiente promiscuo con la visualizzazione a schermo.

BOLLINOCARE – VALUTAZIONE IMPATTO G.D.P.R.

In presenza di errori di log in, o di mancata compilazione dei campi, il sistema genera un messaggio di errore che indica genericamente il fallimento del login, senza specificare se è relativo alla password o all'utenza.



Il Titolare del Trattamento gestisce autonomamente i diritti di accesso e le policy. BollinoCare consente diversi livelli di impostazione in ragione delle specifiche esigenze del Titolare del Trattamento. L'impostazione di base di un'utenza è settata sul "least privilege" per garantire sempre anche la privacy by default. Il Titolare del trattamento può incrementare i diritti del

singolo profilo in funzione delle specifiche esigenze "need to know" per garantire l'operatività della risorsa e le giuste esigenze di accesso, visualizzazione o modifica

Tracciabilità

Le attività degli utenti, a partire dall'autenticazione fino alle innumerevoli tipologie di operazioni chiave di inserimento, modifica ed eliminazione dei dati sono tracciate su un database esterno a quello applicativo. In particolare, si tratta di un database di tipo *[la presente informazione è omessa poiché non resa pubblica da Bollino IT S.p.A. I Titolari del trattamento possono richiedere il dettaglio all'azienda]* fornito dalla piattaforma ufficiale. L'accesso è governato da token di autenticazione configurabili e configurati esclusivamente tramite il pannello amministrativo della piattaforma Azure.

Minimizzazione dei dati

Il principio di minimizzazione dei dati raccolti in fase di accettazione e gestione diagnostica del paziente è responsabilità del Titolare del Trattamento in ragione delle proprie e specifiche valutazioni sia di carattere amministrativo che sanitario (es. contenuti anamnestici all'interno di un referto).

Per quanto riguarda i dati gestiti da Bollino IT mediante BollinoCare il sistema web è progettato per registrare i dati minimi necessari all'accesso e gestione della navigazione (minimizzazione dei dati).

Al termine di una attività sono conservati esclusivamente i dati di log delle attività di accesso e nessun ulteriore dato sensibile.

Vulnerabilità

Bollino IT adotta il Risk Thinking come specifica metodologia operativa. Per tanto l'approccio orientato alle vulnerabilità aziendali e del software fa parte della logica aziendale sin dalla fase di progettazione, passando per lo sviluppo, il testing, la produzione ed installazione al cliente, l'assistenza e la manutenzione. Tale approccio è validato dalla certificazione ISO 27001 ottenuta dall'azienda a valle di verifica condotta da ente terzo qualificato e indipendente.

BOLLINOCARE – VALUTAZIONE IMPATTO G.D.P.R.

Con riferimento a BollinoCare è stato, sin dal principio, elaborato un documento di Sviluppo e Manutenzione del Software Sicuro che evidenzia con metodologia DREAD i livelli di rischio implicito e le contromisure atte alla gestione delle relative vulnerabilità considerate

Lotta contro il malware

I data center sono protetti a cura del Sub Responsabile Microsoft (Azure). L'opzione Microsoft Defender per il cloud è attiva sul server sql.

Sicurezza dei siti web

Il sito web che espone la piattaforma bollino.care è protetto con certificato ed accessibile solo con protocollo *[la presente informazione è omessa poiché non resa pubblica da Bollino IT S.p.A. I Titolari del trattamento possono richiedere il dettaglio all'azienda].* Non sono adoperati cookie di alcun tipo per evitare l'archiviazione, anche temporanea, di eventuali informazioni sui dispositivi locali che accedono ai servizi.

Backup

Il backup del database può essere programmato in maniera personalizzata per ogni istanza di database. Il comportamento predefinito è il backup in linea degli ultimi 7 giorni che può essere ripristinato ad un punto qualsiasi in questo arco di tempo. La modifica delle policy di frequenza, mantenimento in linea e distribuzione geografica può essere modificata in ogni momento.

I documenti archiviati tramite il servizio di storage documentale di Azure mantengono il backup in linea degli ultimi 30 giorni. Inoltre, gli archivi sono replicati con opzione di Ridondanza locale.

Manutenzione

Bollino IT è responsabile del trattamento per quanto attiene la manutenzione del software, gli aggiornamenti, la conservazione del dato, la gestione dei canali comunicativi, la gestione del server con riferimento alle attività direttamente eseguibili da Bollino IT, il ripristino, i trattamenti effettuati dall'applicativo per le finalità contrattualmente definite (es. raggruppamento, estrazione dati, consegna a norma di legge alle strutture statali e ministeriali di riferimento quali ASL territoriali, Ministero della salute, Ministero Economica e Finanza, etc...)

Microsoft si configura quale sub-responsabile del trattamento in ragione del rapporto contrattuale che sussiste tra Bollino IT e Microsoft Azure per l'architettura a supporto del funzionamento di BollinoCare.

Contratto con il Responsabile del Trattamento

I SLA forniti dal Sub Responsabile del Trattamento (gestore dei data center) sono chiari, disponibili e contrattualmente completi nella documentazione standard di fornitura. Altresì al seguente link https://learn.microsoft.com/it-it/compliance/regulatory/gdpr-dpia-azure e relativi rimandi interni, sono disponibili tutte le informazioni di natura tecnica utili a comprendere sia le modalità del Sub Responsabile per fornire idonee garanzie circa le modalità di trattamento, sia la gestione dinamica delle variazioni applicate dal Sub Responsabile in termini procedurali e dei controlli connessi ai requisiti contrattuali garantiti Gli SLA sono formalizzati https://azure.microsoft.com/it-it/support/legal/sla/

Sicurezza dei canali informatici

Il trasferimento dei dati tra i server avviene in modalità sicura e criptata attraverso protocollo *[la presente informazione è omessa poiché non resa pubblica da Bollino IT S.p.A. I Titolari del trattamento possono richiedere il dettaglio all'azienda]*

Controllo degli accessi fisici

Azure è costituito da un'infrastruttura del Data Center distribuita a livello globale, che supporta migliaia di servizi online e che si estende su più di 100 strutture altamente protette in tutto il mondo.
L'infrastruttura è progettata per avvicinare le applicazioni agli utenti in tutto il mondo, mantenendo la residenza dei dati e fornendo ai clienti opzioni complete per la conformità e la resilienza. Azure ha 58 regioni in tutto il mondo ed è disponibile in 140 paesi/regioni.
Un'area è un set di Data Center interconnessi tramite una rete di grandi dimensioni e resiliente. La rete include la distribuzione del contenuto, il bilanciamento del carico, la ridondanza e la crittografia del livello di collegamento dati per impostazione predefinita per tutto il traffico di Azure all'interno di un'area o in viaggio tra aree. Con un numero di aree globali superiore rispetto a qualsiasi altro provider di servizi cloud, Azure offre la flessibilità necessaria per distribuire le applicazioni dove necessario.
Le aree di Azure sono organizzate in aree geografiche. Un'area geografica di Azure assicura il rispetto dei requisiti di residenza, sovranità, conformità e resilienza entro limiti geografici.

BOLLINOCARE – VALUTAZIONE IMPATTO G.D.P.R.

Le aree geografiche consentono ai clienti con esigenze specifiche a livello di residenza dei dati e conformità di mantenere vicini i propri dati e le proprie applicazioni. Le aree geografiche offrono la tolleranza di errore per resistere a un errore completo dell'area tramite la connessione all'infrastruttura di rete a capacità elevata.
Le zone di disponibilità sono località separate fisicamente entro un'area di Azure. Ogni zona di disponibilità è costituita da uno o più Data Center dotati di impianti indipendenti per l'energia, il raffreddamento e la rete. Le zone di disponibilità consentono di eseguire applicazioni cruciali con disponibilità elevata e replica a bassa latenza.
La figura seguente mostra come l'infrastruttura globale di Azure associa l'area e le zone di disponibilità con gli stessi limiti di residenza dei dati per assicurare disponibilità elevata, ripristino di emergenza e backup.

Microsoft adotta un approccio a più livelli per la sicurezza fisica per ridurre il rischio che utenti non autorizzati ottengano l'accesso fisico ai dati e alle risorse dei Data Center. I Data Center gestiti da Microsoft hanno estesi livelli di protezione: accedere all'approvazione nel perimetro della struttura, nel perimetro dell'edificio, all'interno della compilazione e sul pavimento del Data Center. I livelli di sicurezza fisica sono:

- Richiesta di accesso e approvazione. È necessario richiedere l'accesso prima di arrivare al Data Center. Viene richiesto di fornire una motivazione aziendale valida per la visita, ad esempio ai fini di controllo o di conformità. Tutte le richieste sono approvate su una base di necessità di accesso a cura dei dipendenti Microsoft. La base di necessità di accesso consente di mantenere il numero di persone necessarie per completare un'attività nei Data Center per il livello minimo. Una volta che viene concessa l'autorizzazione da parte di Microsoft, un singolo può accedere solo all'area discreta del Data Center per la quale ha presentato richiesta in base alla motivazione aziendale approvata. Le autorizzazioni sono limitate a un determinato periodo di tempo, dopodiché scadono.
- Perimetro della struttura. Quando si arriva a un Data Center, sarà necessario passare attraverso un punto di accesso ben definito. In genere, le altezze delle staccionate fatte in acciaio e cemento includono ogni singolo centimetro del perimetro. Esistono fotocamere digitali intorno ai Data Center, con un team di protezione che monitora costantemente i video.
- Ingresso della struttura. L'ingresso del Data Center è occupato dai responsabili della sicurezza professionale che sono stati sottoposti a rigorose verifiche di training e idoneità. I responsabili della sicurezza pattugliano periodicamente il Data Center e monitorano costantemente anche i video delle fotocamere digitali all'interno del Data Center.

- All'interno della struttura. Dopo essere entrati nella struttura, è necessario superare l'autenticazione a due fattori con dati biometrici per continuare a spostarsi all'interno del Data Center. Se l'identità dell'utente è convalidata, è possibile entrare solo nella parte del Data Center per la quale è stata ottenuta l'autorizzazione. Si può rimanere lì solo per la durata del tempo approvato.
- Piano del Data center. È possibile accedere solo al piano per il quale è stata ottenuta l'autorizzazione. Viene richiesto di passare attraverso uno screening di rilevamento dei metalli su tutto il corpo. Per ridurre il rischio che dati non autorizzati entrino o escano dal datacenter a nostra insaputa, solo i dispositivi approvati possono entrare nel data center. Inoltre, le videocamere monitorano la parte anteriore e posteriore di ogni rack del server. Lo screening di rilevamento dei metalli su tutto il corpo viene ripetuto quando si esce dal piano del Data Center. Per lasciare il Data Center, viene richiesto di passare attraverso un'analisi aggiuntiva di sicurezza.

Ai visitatori viene richiesto di restituire i badge all'uscita di qualsiasi struttura Microsoft.

Sicurezza dell'hardware

Azure usa vari metodi per la ridondanza e la tolleranza di errore per proteggere i clienti da errori hardware localizzati. Gli errori locali possono includere problemi con un computer server Archiviazione di Azure che archivia parte dei dati per un disco virtuale o errori di unità SSD o unità disco rigido (HDD) su tale server. Gli errori dei componenti hardware isolati possono verificarsi durante le normali operazioni.
Azure è progettato per essere resiliente a questi errori. Le emergenze gravi possono causare errori o l'inaccessibilità di molti server di archiviazione o persino un intero data center. Anche se le macchine virtuali e i dischi sono normalmente protetti da errori localizzati, sono necessari passaggi aggiuntivi per proteggere il carico di lavoro da errori irreversibili a livello di area, ad esempio un'emergenza grave, che può influire sulle macchine virtuali e sui dischi. Oltre a potenziali errori della piattaforma, è possibile che si verifichino problemi con un'applicazione o i dati dei clienti. Ad esempio, è possibile che una nuova versione dell'applicazione apporti accidentalmente una modifica ai dati che ne causa l'interruzione. In tal caso, è consigliabile ripristinare una versione precedente dell'applicazione e dei dati che contenga l'ultimo stato valido noto. A questo scopo, sono necessari backup regolari.
Per il ripristino di emergenza a livello di area, è necessario eseguire il backup dei dischi delle macchine virtuali IaaS (Infrastructure as a Service) in un'area diversa.
Le macchine virtuali di Azure e i dischi gestiti sono progettati per essere resilienti agli errori hardware comuni.

Una VM è costituita principalmente da due parti: un server di calcolo e i dischi persistenti. Entrambi influiscono sulla tolleranza di errore di una VM.
Se nel server host di calcolo di Azure che ospita la VM si verifica un errore hardware (eventualità rara), Azure è progettato per il ripristino automatico della VM in un altro server. In questo scenario il computer viene riavviato e la macchina virtuale viene riavviata dopo qualche tempo. Azure rileva automaticamente tali errori hardware e avvia il ripristino per garantire che la macchina virtuale del cliente sia disponibile il prima possibile.
Per quanto riguarda il disco gestito, la durabilità dei dati è fondamentale per una piattaforma di archiviazione permanente. I clienti di Azure hanno applicazioni aziendali importanti in esecuzione su IaaS e dipendono dalla persistenza dei dati. La progettazione della protezione di Azure per questi dischi IaaS prevede tre copie ridondanti dei dati archiviate localmente. Queste copie offrono una durabilità elevata rispetto agli errori locali. In caso di errore di uno dei componenti hardware che contiene il disco, la VM non subisce ripercussioni, perché sono disponibili due copie aggiuntive per supportare le richieste del disco. Non si verificano problemi anche in caso di errore contemporaneo di due componenti hardware che supportano un disco, un'eventualità rara.
Per assicurarsi di mantenere sempre tre repliche, Azure crea automaticamente una nuova copia dei dati in background se una delle tre copie diventa non disponibile. Non dovrebbe essere quindi necessario usare RAID con i dischi di Azure per ottenere la tolleranza di errore. Una semplice configurazione di tipo RAID 0 dovrebbe essere sufficiente per lo striping dei dischi, se necessario, per creare volumi più elevati.
Grazie a questa architettura, Azure ha offerto in modo costante una durabilità di livello aziendale per i dischi IaaS, con una percentuale di frequenza di errori annualizzata pari a zero, ovvero la migliore del settore.

Gli errori hardware localizzati nell'host di calcolo o nella piattaforma di archiviazione possono talvolta causare l'indisponibilità temporanea della macchina virtuale coperta dal contratto di servizio di Azure per la disponibilità delle macchine virtuali.

Per proteggere i carichi di lavoro dell'applicazione dall'inattività causata dalla mancata disponibilità temporanea di un disco o di una VM, i clienti possono usare i set di disponibilità. Due o più macchine virtuali in un set di disponibilità offrono la ridondanza per l'applicazione. Azure crea quindi queste VM e questi dischi in domini di errore separati con diverso tipo di alimentazione, diverse risorse di rete e diversi componenti del server.

A causa di questi domini di errore separati, gli errori hardware localizzati in genere non influiscono su più macchine virtuali nel set contemporaneamente. La presenza di domini di

errore separati offre una disponibilità elevata per l'applicazione. È consigliabile usare i set di disponibilità quando è necessaria la disponibilità elevata.

Politica di tutela della privacy

Bollino applica alla propria organizzazione una rigida politica di Information Security come evidenziato dall'ottenimento della certificazione ISO 27001 da ente esterno, indipendente ed accreditato. Con riferimento al sub responsabile Microsoft Azure, Come specificato dalle Condizioni dei servizi online (https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=46) e dall'Addendum relativo alla protezione dei dati personali (https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=67), Microsoft, in qualità di responsabile del trattamento dei dati, elabora i dati dei clienti solo per fornire i Servizi Online al cliente.

Integrare la protezione della privacy nei progetti

Bollino IT è soggetto certificato ISO 27001 con il seguente campo di applicazione: "Progettazione sviluppo, installazione ed assistenza prodotti software usati in ambito sanitario. Commercializzazione, installazione ed assistenza di dispositivi medici per imaging radiologico. Servizi di conservazione documenti informatici". L'estensione del campo di applicazione evidenzia come l'azienda intenda applicare principi di Information Security (ivi inclusi quelli relativi alla privacy) a tutti i processi aziendali e non solo ad una parte di essi o a determinate fasi di lavoro. La sicurezza delle informazioni è quindi requisito fondamentale sin dalle fasi di progettazione delle attività condotte da Bollino IT.

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

Bollino IT ha attiva una propria procedura per la gestione dei data breach. Nello specifico, su BollinoCare, solo il Titolare del Trattamento ha la possibilità di rilevare i data breach mediante le attività di monitoraggio che vorrà condurre. Bollino IT, secondo i compiti del Titolare del Trattamento, e secondo procedura interna ha attivo un processo che preveda l'assistenza al Titolare del Trattamento (per quanto di propria competenza) e, ove Bollino dovesse riscontrare un Data Breach durante le attività di assistenza e manutenzione, è tenuto a comunicarlo al Titolare del Trattamento senza ingiustificato ritardo e comunque entro 24 ore da quando ha appreso dell'evento.

Per quanto riguarda Azure, Microsoft lavora costantemente per fornire servizi altamente sicuri e di livello aziendale per i clienti Microsoft, ma gli incidenti di sicurezza sono una realtà

inevitabile che deve essere gestita in modo accurato e rapido. In questo documento viene fornita una panoramica sul modo in cui Microsoft gestisce gli incidenti di sicurezza utilizzando metodi e tecnologie già provati e veri per ridurre al minimo il loro potenziale impatto. Un incidente di sicurezza si riferisce a qualsiasi accesso illecito ai dati dei clienti archiviati nelle attrezzature di Microsoft o nelle strutture di Microsoft, o all'accesso non autorizzato a tali attrezzature o strutture che potrebbero causare la perdita, la divulgazione o l'alterazione dei dati dei clienti. Gli obiettivi di Microsoft per rispondere agli incidenti di sicurezza sono proteggere i dati dei clienti e i servizi online di Microsoft.

I team di sicurezza dei servizi online Microsoft e i vari team di servizio lavorano insieme e prendono lo stesso approccio agli incidenti di sicurezza:

- Preparazione
- Rilevamento e analisi
- Contenimento, eliminazione e ripristino
- Attività post-evento imprevisto

L'approccio di Microsoft alla gestione di un incidente di sicurezza è conforme al National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61. Microsoft ha diversi team dedicati che lavorano insieme per prevenire, monitorare, rilevare e rispondere a incidenti di sicurezza.

Gestione del personale

Tutto il personale di Bollino IT, in relazione agli specifici ruoli e mansioni, è incaricato al trattamento dei dati inteso come soggetto individuato secondo art. 29 del GDPR. Tale nomina prevede, inoltre clausola NDA e vincolo alla segretezza anche a valle di eventuale modifica dell'autorizzazione e/o cessazione del rapporto di lavoro del soggetto autorizzato

Integrità dei dati

Integrità dei dati acquisiti: si riferisce alla loro correttezza e alla loro accuratezza. Gli utenti autorizzati sono responsabili dell'introduzione corretta dei dati, ma essi spesso possono commettere errori. BollinoCare aiuta gli utenti a trovare un errore appena immesso e a correggere errori dopo che sono stati inseriti. Inoltre mantengono l'integrità di ogni record nel database nei seguenti modi:

- applicando dei controlli di campo: un campo potrebbe essere un valore numerico, una lettera maiuscola, o uno di un insieme specifico di caratteri. Il controllo assicura

che un valore cada in specifici limiti. Questi controlli prevengono semplici errori verificabili durante l'immissione di dati;

- applicando controlli di accesso: solo chi ha l'autorizzazione almeno per visualizzare i dati può accedere al sistema. Il livello successivo, ossia la possibilità di modificare i dati, dev'essere gestito in modo da consentire la modifica dei dati solo a chi è autorizzato e in modo da evitare conflitti
- mantenendo un log delle modifiche: ossia una lista di tutte le modifiche fatte sui dati (inserimento, cancellazione, modifica o semplice visualizzazione)

Redazione	Approvazione
	BOLLINO IT S.p.A. A SOCIO UNICO Via delle Industrie, 31 - 80147 N. Tel. 081 5592819 - Fax 081 559 Part. IVA 0 6 3 4 4 9 6