Nextbit S.r.l., nell'ambito dei servizi di fatturazione elettronica per la PA e per le Aziende, ha applicato le seguenti misure tecniche ed organizzative per la protezione dei dati personali:

Misure di sicurezza organizzative

Policy e Disciplinari utenti	Sono in essere dettagliate policy e disciplinari, ai quali tutta l'utenza con accesso ai sistemi informativi ha l'obbligo di conformarsi, finalizzate a garantire comportamenti idonei ad assicurare, in fase di assistenza tecnica, il rispetto dei principi di riservatezza, disponibilità ed integrità dei dati nell'utilizzo delle risorse informatiche.
Autorizzazione e istruzioni *accessi logici*	Nextbit ha in essere specifiche procedure per la definizione e autorizzazione dei profili di accesso, configurati nel rispetto del principio di minimizzazione necessario all'esecuzione delle mansioni assegnate. I profili di autorizzazione sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Tali profili sono oggetto di controlli periodici finalizzati alla verifica della sussistenza delle condizioni per la conservazione dei profili attribuiti.
Procedura per Incident Management & Data Breach	Nextbit ha implementato un'apposita procedura finalizzata alla gestione degli eventi e degli incidenti con un potenziale impatto sui dati personali che definisce ruoli e responsabilità, il processo di rilevazione (presunto o accertato), l'applicazione delle azioni di contrasto, la risposta e il contenimento dell'incidente / violazione nonché le modalità attraverso le quali effettuare le comunicazioni delle violazioni di dati personali.
Formazione	Nextbit eroga periodicamente ai propri collaboratori coinvolti nelle attività di Trattamento corsi di formazione sulla corretta gestione dei dati personali
Data Protection Officer	Nextbit ha individuato e nominato un professionista per il ruolo di Data Protection Office affinchè monitori e verifichi tutte le procedure per la gestione dei Dati Personali

Misure di sicurezza tecniche

Privacy by Design	Policy per la gestione delle credenziali con scadenza e complessità; Permessi utente a livello di funzionalità in modo granulare;
Crittografia	Crittografia dei dati in transito utilizzando protocolli sicuri come TLS/SSL per proteggere le comunicazioni tra il client e il server. Crittografia dei dati a riposo per proteggere le informazioni sensibili memorizzate nel database con algoritmo AES 128bit
Isolamento dei Dati	Isolamento logico dei dati dei singoli clienti per evitare l'accesso non autorizzato da parte di altri utenti; Implementazione di controlli di accesso granulari per limitare l'accesso solo alle risorse autorizzate per ciascun utente.
Protezione dell'infrastruttura	L'ambiente di produzione dei servizi FEPA è un'infrastruttura puramente basata sul cloud, ospitata in datacenter forniti da terzi.
Monitoraggio e Logging	Monitoraggio continuo delle attività del sistema e registrazione degli eventi di sicurezza per rilevare e rispondere tempestivamente alle minacce; Analisi dei log per identificare comportamenti anomali o potenziali violazioni della sicurezza.
Piano di Continuità Operativa e Disaster Recovery (RCO e RCT)	Ci impegniamo a garantire elevati standard di continuità operativa. L'RCO rappresenta il nostro impegno per ripristinare il servizio nel minor tempo possibile in caso di interruzione, minimizzando l'impatto sulle attività dei nostri clienti. Il nostro obiettivo è mantenere un RCO il più breve possibile e comunque non superiore al giorno lavorativo successivo all'evento. Inoltre, ci preoccupiamo di proteggere i dati dei nostri clienti garantendo un basso Punto di Ripristino Operativo (RPO), che rappresenta il limite massimo di tempo entro il quale possono essere accettati perdite di dati in caso di incidente. Attraverso rigorose procedure di backup e ripristino, ci impegniamo a mantenere l'RPO entro 1 ora." I servizi sono erogato attraverso una infrastruttura logica ridondata. Per ogni servizio sono presenti due risorse che lo erogano o in bilanciamento di carico o in modalità Attivo Passivo: Tutte le macchine virtuali sono replicate su un altro datacenter giornalmente e il backup dei dati è orario.
Sicurezza perimetrale	L'infrastruttura è protetta da sistema Firewall munito di IPS e Web Application Firewall.
Antivirus	L'intera infrastruttura è protetta da sistema antivirus/antimalware con EDR.

Aggiornamenti	Il software viene aggiornato periodicamente (mediamente almeno una volta al mese) con rilasci applicativi e bugfix. L'infrastruttura è costantemente aggiornata sia a livello di sistemi operativi che di applicativi di supporto al sistema.
Amministratori di Sistema	Gli operatori amministratori di sistema utilizzano credenziali specifiche e sono stati nominati e gestiti come prevede il Provvedimento del Garante per la protezione dei Dati Personali sugli amministratori di sistema.
Lettere di autorizzazione e istruzioni documentate	I soggetti autorizzati e quelli designati sono istruiti sulle modalità di trattamento da eseguire.
Backup	I salvataggi vengono fatti su due datacenter diversi in modalità crittografata con frequenza oraria. Uno dei backup avviene su infrastruttura S3 in modalità immodificabile. La retention del backup è di 15 giorni oltre alla conservazione del primo backup del primo sabato dei precedenti 3 mesi e del primo sabato dei precedenti 2 anni.
Analisi dei rischi	Analisi dei rischi per tutte le attività di trattamento ogni volta intervenga una modifica normativa, procedurale o di contesto al fine di valutare se le misure applicate possano essere migliorate.
Segregazione	I server virtuali che compongono l'infrastruttura risultano segregati e il collegamento tra i vari servizi viene ispezionato da sistema IPS.
Deception Technology	Le reti segregate all'interno delle quali sono collegate schede di rete di un sistema di Honeypot permettono di individuare comportamenti anomali all'interno del perimetro dell'infrastruttura.