

Politica per la Gestione della Qualità, per la Sicurezza delle Informazioni & per la Cybersicurezza

Il presente documento descrive la Politica del Sistema di Gestione Integrato della qualità, della sicurezza delle informazioni e della cybersicurezza di ZPay S.r.l.

La società è stata fondata nel 2021 da Dojo S.r.l., società del Gruppo Zucchetti, ed è un istituto di pagamento, autorizzato da Banca d'Italia, il cui scopo è fornire servizi finanziari, integrabili con i gestionali del Gruppo Zucchetti.

Tali servizi si articolano in esecuzione di operazioni di pagamento, emissione di strumenti di pagamento e/o convenzionamento di operazioni di pagamento, servizi di disposizione di ordini di pagamento nonché servizi di informazione sui conti, come meglio precisati nella sezione "Servizi" del sito web.

La Società risulta conforme, nello specifico, alle disposizioni di seguito indicate:

- ISO/IEC 27001:2022 e Linee Guida 27017:2015 e 27018:2019;
- ISO/IEC 9001:2015 / AMD 1:2024;
- Digital Operational Resilience Act (DORA), Regolamento n. 2554/2022;
- D. Lgs 138/2024, che recepisce la Direttiva UE NIS2, Network and Information Security, n. 2555/2022;
- Determina ACN n. 164179 del 14 aprile 2025.

Il Sistema di Gestione Integrato è applicato alla *"Sviluppo software, assistenza, ed erogazione servizi per istituti di pagamento"*.

La sicurezza, la salvaguardia del patrimonio informativo e la garanzia della massima soddisfazione del Cliente, costituiscono condizione imprescindibile per il raggiungimento degli obiettivi di business di ZPAY S.r.l.

A tal fine, lo svolgimento delle attività aziendali deve sempre avvenire garantendo adeguati livelli di disponibilità, integrità e riservatezza delle informazioni; ciò anche attraverso l'implementazione di un formale *"Sistema di Gestione Integrato della Qualità e della Sicurezza delle Informazioni"* (SGI) in linea con i requisiti attesi dalle parti interessate e nel rispetto delle normative vigenti.

Inoltre, Zpay si impegna a garantire la piena conformità al Regolamento (UE) 2022/2554 (DORA), adottando misure e controlli idonei a rafforzare la resilienza operativa digitale, gestire i rischi informatici nonché assicurare la sicurezza dei servizi di pagamento erogati ai propri clienti.

In aggiunta, la società si sta adattando alle prescrizioni normative richieste dalla Direttiva NIS2 e dalla Determina ACN al fine di garantire elevati standard di sicurezza informatica, prevenire incidenti, mitigare i rischi legati alle reti e ai sistemi informativi e assicurare la continuità operativa dei servizi di pagamento.

Infine, la società provvederà a adattarsi alla nuova versione della LG 27018:2025.

La Direzione ha pertanto implementato un Sistema di Gestione integrato per la Qualità e la Sicurezza delle informazioni, ispirandosi ai seguenti principi:

- **Focalizzazione sul cliente:** ZPAY dipende dai propri clienti e pertanto cerca di soddisfare le loro esigenze presenti e future, soddisfare i loro requisiti e mirare a superare le loro stesse aspettative;
- **Chiara definizione dei ruoli e responsabilità:** ZPAY definisce in modo chiaro le responsabilità del personale e degli utenti in relazione ai requisiti dei propri sistemi di gestione;
- **Coinvolgimento e consapevolezza del personale:** ZPAY è consapevole che le persone, a tutti i livelli, costituiscono l'essenza dell'organizzazione ed il loro pieno coinvolgimento permette di porre le loro capacità al servizio dell'organizzazione;
- **Approccio per processi:** ZPAY favorisce un approccio per processi al fine di perseguire i risultati desiderati con maggior efficienza;
- **Miglioramento:** il miglioramento continuo delle prestazioni complessive sono un obiettivo permanente di ZPAY;
- **Processo decisionale basato sulle evidenze:** il sistema di gestione è costituito da un insieme di informazioni documentate, come prescritto dalle Norme UNI EN ISO;
- **Rapporti di reciproco beneficio con i fornitori:** ZPAY ed i suoi fornitori sono interdipendenti ed un rapporto di reciproco beneficio migliora, per entrambi, la capacità di creare valore.

Gli obiettivi della Politica Aziendale di ZPAY sono:

- Ricercare la completa soddisfazione delle esigenze ed aspettative delle Parti Interessate rilevanti;
- Monitorare costantemente il contesto interno ed esterno in cui opera;
- Rispettare le leggi e le disposizioni vigenti, i requisiti contrattuali, le norme e le procedure aziendali;
- Soddisfare i propri obblighi di conformità, garantendo allo stesso tempo di applicare tutte le misure di controllo necessarie;
- Mantenere un elevato standard qualitativo dei prodotti;
- Proteggere le informazioni e i dati personali da accessi non autorizzati;
- Minimizzare il rischio di perdita e/o indisponibilità dei dati trattati, pianificando e gestendo le attività a garanzia della continuità di servizio;
- Proteggere le risorse informative e i dati personali all'interno dell'ambiente Cloud;
- Sviluppare e mantenere un Sistema di Gestione Integrato quale strumento per realizzare gli obiettivi, rispettare gli impegni assunti, promuovere il miglioramento continuo dei processi aziendali,
- Riesaminare periodicamente la Politica, gli Obiettivi, i traguardi e relativi programmi di attuazione ed il Sistema di Gestione Aziendale e darne adeguata visibilità all'interno dell'azienda;
- Realizzare Audit Interni al fine di assicurare il rispetto dei requisiti del Sistema di gestione Integrato adottando tutte le azioni correttive necessarie;
- Potenziare l'attività di informazione, formazione e addestramento, coinvolgendo tutti gli operatori e rendendoli consapevoli dei loro obblighi individuali e dell'importanza di ogni loro azione per il raggiungimento dei risultati attesi e della loro responsabilità;
- Monitorare periodicamente l'efficacia del Sistema di gestione Integrato, anche attraverso il riesame da parte della Direzione;
- Sensibilizzare i fornitori ed appaltatori alle tematiche di qualità, sicurezza delle informazioni e richiedere il rispetto delle politiche adottate dall'Azienda;
- Specificamente alle piattaforme Cloud, ZPAY si impegna a rispettare i seguenti requisiti:

- i requisiti di base di sicurezza delle informazioni applicabili alla progettazione e realizzazione del servizio cloud;
- rischi derivanti da insider autorizzati;
- accesso agli asset del cliente del servizio cloud da parte del personale del fornitore di servizi cloud;
- procedure di controllo degli accessi, ad esempio, autenticazione forte per accesso amministrativo ai servizi cloud;
- comunicazioni ai clienti del servizio cloud durante il change management;
- sicurezza della virtualizzazione;
- accesso e protezione dei dati dei clienti del servizio cloud;
- gestione del ciclo di vita degli account del cliente del servizio cloud;
- comunicazione delle violazioni e condivisione delle informazioni linee guida per aiutare le indagini e la scientifica.

La Direzione di ZPAY è convinta che il processo di miglioramento continuo costituisca l'elemento fondamentale per raggiungere l'eccellenza nel coniugare la crescita aziendale, con elevati standard di qualità ed efficienza dei servizi erogati.

Tutto il personale di ZPAY, i fornitori o terze parti sotto contratto, che rientrano nel campo di applicazione sopracitato, sono responsabili dell'attuazione della presente politica con il supporto della Direzione che l'ha approvata.

La Direzione di ZPAY sostiene i principi ed obiettivi per il SGI e supporta in modo pieno e completo il programma per la loro attuazione e mantenimento, fornendo le risorse necessarie.

La presente politica viene riesaminata dalla Direzione regolarmente o in caso di cambiamenti significativi che influenzano i sistemi, al fine di garantire l'idoneità, l'adeguatezza e l'efficacia.

La presente Politica è comunicata alle parti interessate e sarà oggetto di revisione a breve termine al fine di garantire la piena conformità con quanto previsto dal D.Lgs. 138/2024, di recepimento della Direttiva (UE) 2022/2555 – NIS2 (Network and Information Security) nonché alla Determina ACN n. 164179 del 14 aprile 2025.

Milano, 03.09.2025

Il Legale Rappresentante


