INFORMATIVA SULLA PRIVACY DI NEXI

INDICE

1 LA PRIVACY DELL'UTENTE È FONDAMENTALE PER IL GRUPPO NEXI.

Nexi mette al centro della propria attività il rapporto con il cliente prevedendo, fin dalla fase di progettazione e realizzazione dei propri servizi, tutte le misure organizzative, tecniche e di sicurezza necessarie per salvaguardare i dati personali dei soggetti coinvolti nella loro gestione (clienti, personale dipendente e fornitori), nel pieno rispetto delle previsioni del Regolamento UE 2016/679 (GDPR) e adottando le più recenti "best practices" per l'utilizzo dei sistemi informativi che sono alla base del buon funzionamento dei servizi stessi.

Il nostro scopo, infatti, è conquistare e aumentare, ogni giorno, la fiducia dei nostri clienti, sulla base dei seguenti principi fondamentali della privacy:

- Trasparenza: forniamo informazioni trasparenti sulla raccolta e l'uso dei dati;
- Sicurezza: proteggiamo i dati a noi affidati tramite strumenti di sicurezza avanzati;
- Controllo: il cliente ha il controllo della sua privacy tramite strumenti di facile utilizzo e opzioni di scelta chiare.
- Reporting: forniamo periodica informativa sulle eventuali segnalazioni per violazioni sulla privacy all'interno della Dichiarazione consolidata di carattere non Finanziario ai sensi del D.Lgs. 254/2016.

Nexi opera nell'ambito dei servizi di pagamento e della gestione di moneta elettronica e, pertanto offre alla propria clientela e alla clientela delle Banche e Società partner, servizi di Issuing e di Acquiring per l'uso delle carte di pagamento (es. gestione delle transazioni), nonché servizi correlati all'attività bancaria (es. gestione bonifici).

I riferimenti ai servizi Nexi presenti in questa informativa includono l'uso di siti Web, app, server e dispositivi diversi, resi disponibili alla clientela per l'erogazione degli stessi.

Con questa informativa Nexi intende illustrare le finalità e le relative modalità di trattamento dei dati personali all'interno dalle Società del Gruppo.

2 DATI PERSONALI RACCOLTI DA NEXI

Nexi raccoglie i dati del cliente sia direttamente dallo stesso (c.d. raccolta di dati presso l'interessato) sia da fonti terze (ad esempio, banche *partner* per la vendita dei servizi ai clienti finali, circuiti nazionali e internazionali di pagamento, etc.).

Nel primo caso, Nexi raccoglie i dati del cliente sia in fase di sottoscrizione dei contratti (ad es. dati personali comuni - identificativi e di contatto, economico/finanziari – IBAN e carta di pagamento, ecc.) che, successivamente, in base ed in seguito all'utilizzo dei servizi erogati (ad es. dati transazionali, di autenticazione alle app Nexi, ecc.), nonché dell'assistenza richiesta dal cliente per eventuali chiarimenti necessari o per la segnalazione di problematiche riscontrate nell'uso dei servizi erogati.

Nexi acquisisce i dati della clientela anche da terze parti, sia per ottemperare ad obblighi di legge, ad esempio, da basi dati pubbliche o private autorizzate (es. Registro delle Imprese, Cerved) in fase di censimento del cliente ai sensi delle vigenti norme in materia di

antiriciclaggio, sia nell'ambito della normale operatività, ad esempio dai Circuiti di pagamento nazionali (PagoBancomat) e internazionali (Visa, MasterCard, ecc.), per l'autorizzazione e la contabilizzazione delle operazioni effettuate.

Nexi, infine, raccoglie i dati di navigazione degli utenti del proprio sito istituzionale, dei portali e delle app attraverso l'uso dei cookie, sia Tecnici, Analitici o Statistici, che per loro natura non richiedono il consenso, sia di Profilazione con finalità di marketing che, al contrario dei primi, per essere installati richiedono il consenso esplicito dell'utente.

3 MODALITÀ DI UTILIZZO DEI DATI PERSONALI

Nexi raccoglie e tratta i dati e le informazioni necessarie all'erogazione dei propri servizi e all'esecuzione dei relativi adempimenti di legge, per i quali non è necessario acquisire il consenso del soggetto interessato.

Per determinati tipi di attività, ad esempio per azioni di marketing, Nexi acquisisce un esplicito consenso da parte dei soggetti interessati.

In alcuni casi, i dati possono essere utilizzati senza consenso dell'interessato, al fine di effettuare analisi statistiche e analisi quantitative e qualitative anche per gestire specifiche esigenze di Nexi (legittimo interesse) tra cui, a titolo esemplificativo, l'analisi dell'operatività della propria clientela al fine di adeguare la propria offerta al mercato di riferimento, l'analisi delle prestazioni dei propri applicativi, la ricerca di nuove soluzioni tecnologiche per migliorare l'esperienza del cliente, ecc. Gli output derivanti dalle analisi sono di tipo aggregato, utilizzati da Nexi per esaminare e identificare i trend andamentali dei prodotti e/o servizi erogati, studiare e sviluppare nuovi prodotti e/o servizi e per migliorare le attività promozionali allineate alle esigenze e alle aspettative della clientela.

Nexi potrebbe utilizzare i dati e le informazioni raccolte anche per finalità diverse da quelle per i quali sono stati raccolti, ad esempio per azioni di marketing, garantendo l'applicazione dei principi stabiliti dalla normativa privacy vigente, in particolare l'obbligo di informare l'interessato di tali altre finalità e dei suoi diritti, compreso il diritto di opporsi.

Il trattamento dei dati personali per le suddette finalità, per la natura dei servizi erogati, include prevalentemente metodi di trattamento automatizzati, ma non prescinde da trattamenti manuali, svolte da personale opportunamente autorizzato; le due modalità si completano vicendevolmente per l'erogazione dei servizi stessi.

I trattamenti automatizzati si basano sull'uso delle migliori tecnologie reperibili sul mercato e sull'adozione di molteplici sistemi di sicurezza (es. firewall, credenziali, token, ecc.) per evitare la perdita o l'indisponibilità, anche involontaria e/o temporanea, dei dati personali trattati; allo scopo, Nexi si è dotata di apposite procedure interne per lo sviluppo iniziale e l'implementazione degli applicativi, basate su più livelli autorizzativi per l'attivazione in ambiente di produzione, in grado di garantire il raggiungimento di tale obiettivo.

I trattamenti manuali si basano sull'applicazione di procedure definite da Nexi per il proprio personale e per il personale delle terze parti a cui le Società del gruppo possono ricorrere, supportati da costanti sessioni di formazione, generale e specialistica, erogata, sia a distanza che in aula, in funzione delle mansioni assegnate.

I dati sono trattati prevalentemente in modalità elettronica; tuttavia, permangono trattamenti di documenti cartacei, ad esempio con riferimento alla gestione di reclami e contestazioni, ecc.

Nexi condivide i dati personali acquisiti con fornitori che lavorano per suo conto, nominati responsabili del trattamento ai sensi dell'art. 28 del GDPR, o con altri Titolari autonomi del trattamento, sia per necessità operative (es. Circuiti di pagamento) che per obblighi di legge (es. Agenzia delle Entrate).

I fornitori devono trattare i dati esclusivamente per eseguire il mandato loro conferito da Nexi e informare Nexi stessa di tutte le modalità operative adottate per essere conforme al GDPR come, ad esempio, la tenuta di un proprio registro dei trattamenti, la nomina a responsabile di eventuali sub fornitori, le clausole contrattuali adottate per eventuali trasferimenti dei dati all'estero, ecc.. Tutti i fornitori, in ogni caso, sono soggetti a controlli periodici, da parte di Nexi, per la valutazione del rischio privacy.

4 MODALITÀ DI ACCESSO E CONTROLLO DEI DATI PERSONALI DEL SOGGETTO INTERESSATO

I soggetti interessati possono controllare i dati personali che Nexi ha raccolto ed esercitare i diritti relativi alla protezione dei dati contattando, tramite i canali tempo per tempo resi disponibili e pubblicizzati nella sezione Privacy del sito www.nexi.it, il Responsabile della protezione dei dati (Data Protection Officer) che Nexi ha identificato nel Responsabile della Funzione Compliance & AML.

Gli interessati, in particolare, possono chiedere l'accesso ai dati che li riguardano, la loro rettifica, l'integrazione o la loro cancellazione, la limitazione del trattamento nei casi previsti dall'art. 18 GDPR, nonché l'opposizione al trattamento ai sensi dell'art. 21 del GDPR.

Gli interessati, inoltre, possono esercitare il diritto alla portabilità dei propri dati ai sensi dell'art. 20 del GDPR, ovvero il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati, nonché, se tecnicamente fattibile, di trasmetterli ad altro titolare senza impedimenti.

Gli interessati, infine, hanno il diritto di proporre un reclamo all'Autorità Garante per la protezione dei dati personali.

5 CANCELLAZIONE DEI DATI

I dati acquisiti sono trattenuti da Nexi per il solo tempo necessario all'erogazione dei servizi per i quali sono stati archiviati e, pertanto, vengono cancellati al termine del loro specifico utilizzo, nel rispetto delle prescrizioni del GDPR e degli altri obblighi di legge (es. art. 2220 del Codice Civile in tema di gestione della documentazione contrattuale), di norma dopo 10 anni dalla cessazione del rapporto continuativo o prima, qualora tali dati siano serviti per specifiche attività quali, ad esempio, la gestione delle contestazioni verso i Circuiti di pagamento.

6 MISURE DI SICUREZZA

Per l'adeguata e sicura gestione dei dati personali raccolti, elaborati, conservati o trattati in altro modo dalla Società, Nexi ha definito un sistema di governance della Privacy che garantisce l'applicazione dei requisiti normativi tempo per tempo vigenti e delle misure di sicurezza adottate, nel rispetto del principio di accountability (ex art. 24 GDPR).

Il sistema di governance è costituito da Policy, Regolamenti, Procedure operative e Manuali che sono periodicamente aggiornati per recepire le più recenti disposizioni normative in ambito e in coerenza con l'assetto organizzativo della società.

Le misure di sicurezza adottate dalla Società sono di tipo organizzativo, procedurale e tecnico e sono prevalentemente disposte dalle preposte funzioni sotto la supervisione del DPO.

Con particolare riferimento alla definizione e implementazione di misure tecniche, la funzione Compliance e il DPO sono supportati dalla CISO Area, la Funzione aziendale responsabile del presidio delle tematiche in ambito information security, del governo dei processi di business continuity e security incident management, della verifica dell'applicazione degli standard e dei processi di sicurezza.

Le principali misure di sicurezza coprono tutti gli aspetti della sicurezza dei dati e delle informazioni, come normato dai principali standard di settore, quali ad esempio: sviluppo sicuro e manutenzione del software, gestione dei backup e del disaster recovery, gestione degli accessi logici e fisici, protezione dagli attacchi esterni (es. firewall, antimalware, ...), ecc.

Con riferimento ai trattamenti di dati e documenti cartacei, sono adottate misure di sicurezza ad hoc con particolare riferimento all'uso e alla conservazione sicura degli stessi (es. clean desk policy), alla protezione contro la perdita di integrità, alla dismissione a norma di legge al cessare della loro utilità e necessità, ecc.

La definizione delle misure di sicurezza avviene adottando un approccio risk-based, nel rispetto dei principi di accountability, di privacy by design e by default, e tenendo in considerazione anche altri standard e normative di settore applicabili quali, ad esempio, le

richieste di sicurezza previste dalla certificazione PCI-DSS conseguita dalla Società, in quanto spesso sovrapponibili e reciprocamente compensative. Dette misure sono riesaminate e aggiornate qualora necessario, per garantire che i trattamenti siano effettuati conformemente alla normativa privacy vigente.

Ultimo Aggiornamento: 31 marzo 2021