POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

Informazioni sul documento				
Revisione	**1**		Data	**17.04.2024**
scritto	GContri	Day spa	Data	10.09.2020
controllato	MMalizia	Day spa	Data	22.09.2020
approvato	MCBartolini	Day spa	Data	29.09.2020

Stato	BOZZA	**DEFINITIVO**	RITIRATO	
Classificazione	PUBLICO	**INTERNO**	RISERVATO	
Tipo	**GENERALE**	PERSONALE	PARTICOLARE	

Storia del documento

Rev.	Date	Stato	Redatto	Verificato	Approvato
0	29.09.2020	Prima emissione	GContri	Team Day	Dir Gen.
1	17.04.2024	Aggiornamento della Politica File rename a seguito del passaggio all'edizione 2022	GContri	Team Day	Dir Gen.

DAY considera come obiettivo primario la sicurezza delle informazioni.

Ciò significa implementare e mantenere un sistema di gestione delle informazioni sicuro così da garantire:

1. Riservatezza – informazioni accessibili solamente ai soggetti e/o ai processi debitamente autorizzati
2. Integrità – salvaguardia della consistenza dell'informazione da modifiche non autorizzate
3. Disponibilità – facilità di accesso alle informazioni necessarie
4. Controllo – garanzia che i processi e strumenti per la gestione dei dati siano sicuri e testati
5. Autenticità – provenienza affidabile dell'informazione
6. Privacy – garanzia di protezione e controllo dei dati personali.

DAY ha sviluppato un Sistema di Gestione della Sicurezza dell'Informazione (ISMS), seguendo i requisiti specificati della Norma UNI CEI EN ISO/IEC 27001:2017.
Il sistema è stato rivisto a marzo 2024 alla luce della nuova edizione della norma nel 27001:2022.

DAY ha inoltre ritenuto fondamentale estendere il sistema di gestione della sicurezza delle informazioni con lo schema ISO/IEC 27701, quale ulteriore impegno nella protezione dei dati personali gestiti nell'ambito delle proprie attività ed erogazione dei servizi.

La decisione e l'impegno di DAY nell'implementazione di un sistema di gestione delle informazioni esteso alla protezione dei dati personali, emerge dalla volontà di assicurare e garantire la massima tutela dei dati e delle informazioni presenti nella propria organizzazione, tenuto conto, fra gli altri, dei seguenti fattori:

a) la tipologia di servizi offerti. Si riportano di seguito i principali:

Buoni pasto

DAY è una Smart company da 30 anni leader nel mercato del Buono Pasto. L'offerta di DAY si è negli anni ampliata e diversificata, anche attraverso l'introduzione di nuovi modelli di business che hanno di fatto determinato un processo di *digital transformation*.

Tale processo si è reso necessario a fronte dell'evoluzione digitale del buono pasto, a seguito della maggiore diffusione dei buoni pasto elettronici rispetto a quelli cartacei, ormai marginali in termini di volumi.

Servizi Welfare

Tra i servizi offerti da DAY alle aziende clienti vi è una sempre maggiore diffusione dei Servizi Welfare, erogati tramite Piattaforma web dedicata, che interagisce anche con servizi di Partner esterni, con i quali Day ha concluso specifici accordi al fine di ampliare la propria offerta nei confronti dei clienti e dei beneficiari (dipendenti delle aziende clienti).

In considerazione della tipologia di dati trattati per l'erogazione di tali servizi (che vede coinvolti anche i dati sanitari dei beneficiari, di familiari e minori), DAY presta particolare attenzione all'analisi delle misure di sicurezza implementate nella Piattaforma.

Cadhoc

Anche i buoni Cadhoc, in ragione della tipologia di servizio e delle modalità di utilizzo (si tratta di buoni acquisto spendibili in una vasta rete di negozi o convertiti on line in buoni shopping di brand conosciuti, quali, ad esempio, Amazon, Decathlon, Unieuro, Zalando, etc.) hanno certamente inciso nel processo di digitalizzazione di DAY.

b) le indicazioni del Gruppo UP in merito alla sicurezza delle informazioni, che richiedono la necessità di mantenere livelli di sicurezza elevati e continuamente sottoposti a monitoraggio da parte del Gruppo stesso, attualmente governati secondo il framework NIST.

Ciò posto, il patrimonio informativo della DAY da tutelare è costituito dall'insieme delle informazioni localizzate nella sede centrale, in tutte le unità operative dell'azienda e presso i data center ove sono gestiti i dati aziendali.

La mancanza di adeguati livelli di sicurezza può comportare il danneggiamento dell'attività di DAY, la mancata soddisfazione del cliente, problematiche sotto il profilo del trattamento dei dati personali (lesioni dei diritti e delle libertà degli interessati), nonché il rischio di incorrere in sanzioni legate alla violazione delle normative vigenti nonché danni di natura economica, finanziaria e di immagine aziendale.

La politica per la sicurezza delle informazioni di DAY si applica a tutto il personale interno e alle terze parti che collaborano alla gestione delle informazioni ed a tutti i processi e risorse coinvolte nella progettazione, realizzazione, avviamento ed erogazione continuativa nell'ambito dei servizi.

La politica della sicurezza rappresenta l'impegno dell'organizzazione a garantire la sicurezza delle informazioni, degli strumenti fisici, logici ed organizzativi atti al trattamento delle informazioni in tutte le attività.

In tal senso, l'impegno della Direzione si attua tramite la definizione di una struttura organizzativa adeguata a:

- Stabilire i ruoli aziendali e le responsabilità per lo sviluppo e il mantenimento del ISMS
- Controllare che il ISMS sia integrato in tutti i processi aziendali, e che le procedure e i controlli siano sviluppati efficacemente
- Monitorare l'esposizione alle minacce per la sicurezza delle informazioni
- Attivare programmi per diffondere la consapevolezza e la cultura sulla sicurezza delle informazioni.

Gli obiettivi generali della DAY sono quindi:

- Garantire i migliori standard, ottimizzando e razionalizzando i processi e gli strumenti aziendali
- Garantire l'efficacia del sistema ISMS
- Garantire la soddisfazione degli utenti (clienti, beneficiari, fornitori, affiliati, partner) in relazione alla qualità delle informazioni.

Tutto il personale deve operare per il raggiungimento degli obiettivi di sicurezza nella gestione delle informazioni.

L'applicazione del sistema di gestione richiede pertanto piena partecipazione, impegno ed efficace interazione di tutte le risorse umane e tecnologiche. La continua crescita del livello di servizio verrà perseguita mediante il regolare riesame dello stesso, volto al monitoraggio degli obiettivi prestabiliti e al riconoscimento di eventuali aree di miglioramento.

La Direzione è impegnata per:

1. Attuare, sostenere e verificare periodicamente la presente Politica, a divulgarla a tutti i soggetti che lavorano per l'azienda o per conto di essa
2. Garantire le risorse necessarie per l'efficace protezione delle informazioni
3. Definire gli obiettivi in materia di sicurezza delle informazioni
4. Riesaminare periodicamente gli obiettivi e la Politica per la sicurezza delle informazioni per accertarne la continua idoneità.

In particolare, per tutti i sistemi sotto ISMS, l'organizzazione si impegna affinché:

- Le informazioni siano accessibili esclusivamente alle persone autorizzate, sia interne che esterne all'azienda, garantendo livelli di servizio e complessità compatibili con i requisiti funzionali dei sistemi interessati;
- Qualunque sia il formato delle informazioni trattate, sia garantita la loro disponibilità, integrità e riservatezza nel rispetto dei requisiti legislativi applicabili;
- Sia effettuato un monitoraggio costante nel cambiamento degli Asset e della tecnologia al fine di identificare tempestivamente nuove vulnerabilità;
- Sia effettuato un costante aggiornamento sui siti specializzati in tematiche di sicurezza e forum per la pronta individuazione di nuove tipologie di minacce;
- Sia prestata particolare attenzione alle variazioni dei requisiti normativi, contrattuali e alle relative priorità in relazione a nuovi sviluppi applicativi;
- Sia garantita la continuità operativa attraverso interventi mirati, sia organizzativi sia tecnologici, e che tali interventi siano definiti, costantemente aggiornati e periodicamente verificati;
- Tutto il personale sia addestrato sulla sicurezza, sia informato dell'obbligatorietà delle politiche aziendali in merito e sia sensibilizzato sulle conseguenze derivanti dalla violazione delle politiche aziendali;
- Siano effettuate valutazioni periodiche dell'efficacia del ISMS e della formazione del personale attraverso simulazioni nell'ambito di applicazione (test di penetrazione/intrusione sulla sicurezza logico-fisica, test di conoscenza delle policy e simulazioni di violazioni delle stesse);
- Siano introdotte metriche per la valutazione delle prestazioni del sistema;
- Siano separate le mansioni relative alle attività critiche (ad esempio sviluppo e collaudo con la produzione);
- Siano ridotti il più possibile i rischi alla fonte;
- Qualsiasi violazione della sicurezza, reale o presunta, sia comunicata ed investigata;
- Siano prontamente identificati e gestiti gli incidenti sulla sicurezza ed attivate le autorità competenti per quelli che hanno impatto su requisiti di legge violati;
- Sia evitato l'utilizzo di software non autorizzati;
- Siano effettuati riesami periodici del ISMS relativamente a:
    - verifica dell'attualità e dell'efficacia dei controlli applicati per le minacce e le vulnerabilità individuate nel piano del trattamento dei rischi
    - incidenza dei controlli attuati sull'efficacia gestionale
    - modifiche apportate dalla tecnologica (vulnerabilità nuove o modificate, riduzione dei rischi per nuove conoscenze acquisite in base al progresso tecnologico)
    - modifiche apportate alla configurazione dei sistemi sotto ISMS
    - rivalutazione periodica del rischio ed in particolare a monte e a valle di qualsiasi azione preventiva.

Inoltre, l'organizzazione s'impegna a mantenere la conformità con i requisiti legali e contrattuali in materia di protezione dei dati personali. Nella specie, l'organizzazione s'impegna a garantire la conformità alle seguenti norme:

- ISO/IEC 27001 – Sistema di Gestione per la Sicurezza delle Informazioni
- ISO/IEC 27701 – Standard per la protezione dei dati personali
- Regolamento (UE) 16/679 (GDPR)
- D.lgs. 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali (per le parti compatibili con il GDPR e non abrogate)
- D.lgs. 101/2018 - Adeguamento della normativa italiana al GDPR (Regolamento UE 2016/679)

Viene inoltre definita la metodologia di valutazione del rischio basata sulle linee guida della ISO/IEC 27005 ed individuati i parametri per il monitoraggio delle performance (Rif. ISMS.IT.5 - Obiettivi Sicurezza KPI.xsls).

La responsabilità dell'istituzione e della gestione del ISMS è assegnata al Responsabile della Sicurezza delle Informazioni

Bologna, 28 maggio 2024

Day Ristoservice S.P.A. Società Benefit
Vice Presidente e Direttore Generale
Mariacristina Bertolini