POLITICA AZIENDALE SULLA SICUREZZA DEI DATI PERSONALI

1. Premessa

La presente Politica è redatta in ottemperanza all'Art. 24, comma 2, del Regolamento (UE) n. 2016/679 (di seguito indicato per brevità come "Regolamento") che disciplina gli aspetti relativi alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione degli stessi.
La Politica definisce:

- i principi generali applicabili a **Febo S.p.A.** in qualità di Titolare del trattamento di dati personali e le misure generali adottate per ottemperare a tali principi;
- le responsabilità e i compiti delle funzioni operanti per conto della nostra azienda.

Il Responsabile del trattamento dei dati personali provvede, con cadenza almeno annuale, a rivedere la Politica e a valutare eventuali modifiche da apportare.
Eventuali modifiche derivanti da:

- cambiamenti organizzativi,
- emanazione o modifica della normativa di riferimento (ad es. provvedimenti del Garante Privacy)

sono approvate, su proposta del Responsabile del trattamento dati, dal Rappresentante Legale.

2. Principi e misure generali sul trattamento dei dati personali

La Politica identifica le principali misure individuate da **Febo S.p.A.** per assicurare il rispetto dei principi generali contenuti nel Regolamento, con particolare riguardo a:

- liceità del trattamento;
- diritti degli interessati;
- registro dei trattamenti e valutazione d'impatto sulla protezione dei dati;
- sicurezza dei trattamenti;
- gestione degli eventi di "data breach".

A tale riguardo **Febo S.p.A.**:

1. adotta processi, strumenti e controlli idonei, che consentano il pieno rispetto dei principi generali sul trattamento dei dati personali;
2. garantisce adeguati flussi informativi da e verso le funzioni aziendali, le strutture di controllo e operative;
3. assicura lo svolgimento delle attività di formazione del personale in materia di protezione dei dati personali, al fine di garantire il rispetto della normativa applicabile da parte di chiunque ponga in essere attività di trattamento dei dati personali all'interno della struttura aziendale sotto l'autorità del Titolare.

I trattamenti di dati personali delle diverse categorie di soggetti interessati (ad es. clienti, dipendenti, fornitori) svolti da **Febo S.p.A.** si fondano sui seguenti principi:

- liceità, correttezza e trasparenza: i dati personali sono raccolti e trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- limitazione della finalità: i dati personali sono raccolti e trattati per finalità determinate, esplicite e legittime;
- minimizzazione dei dati: i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- esattezza: i dati personali sono mantenuti esatti ed aggiornati e sono adottate misure ragionevoli per cancellare o rettificare, tempestivamente, i dati inesatti o superati;
- limitazione della conservazione ("data retention"): i dati personali sono conservati per un arco temporale non superiore al conseguimento delle finalità per cui sono stati raccolti;
- integrità e riservatezza: i dati personali sono trattati in modo da garantirne un'adeguata sicurezza, attraverso l'adozione di misure tecniche ed organizzative adeguate;
- privacy by design e privacy by default: gli aspetti in materia di protezione dei dati personali devono essere considerati fin dalle fasi di progettazione, implementazione e configurazione di tutte le tecnologie utilizzate per le operazioni di trattamento. **Febo S.p.A.** deve trattare, di default, solamente quei dati che siano necessari al perseguimento delle finalità del trattamento;
- responsabilizzazione ("accountability"): i trattamenti dei dati personali sono svolti secondo i principi che precedono e il loro rispetto è adeguatamente documentato.

2.1. Liceità del trattamento

I trattamenti di dati personali all'interno di **Febo S.p.A.** possono essere condotti esclusivamente sulla base di una o più delle seguenti condizioni:

- contratto di cui l'interessato è parte;
- obbligo legale cui è soggetta **Febo S.p.A.**;
- salvaguardia di interessi vitali del soggetto interessato;
- esplicito consenso dell'interessato;
- perseguimento di un legittimo interesse di **Febo S.p.A.**

2.1.1. Richiesta del consenso

Laddove il trattamento di dati personali si fondi sul consenso dell'interessato, la raccolta del consenso è effettuata tramite dichiarazione scritta ovvero, in casi particolari caratterizzati da minore rischiosità, in forma orale e documentata per iscritto. Qualora nel modulo utilizzato per la raccolta del consenso si trattino altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio chiaro e semplice in modo tale che la volontà dell'interessato sia liberamente espressa. Il consenso è revocabile in qualsiasi momento e la sua revoca non pregiudica la liceità del trattamento effettuato fino a quel momento.

2.1.2. Legittimo interesse

In alcuni casi (ad esempio svolgimento di marketing diretto), le procedure di **Febo S.p.A.** devono prevedere che il trattamento di dati personali possa essere effettuato al fine di perseguire un legittimo interesse di **Febo S.p.A.**
In ottemperanza al principio di accountability, in tali casi, le procedure devono prevedere che la valutazione circa il corretto bilanciamento tra gli interessi di **Febo S.p.A.** e i diritti dell'interessato sia adeguatamente documentata.

2.1.3. Trasferimento di dati all'estero

Il trasferimento di dati personali verso un paese terzo (non appartenente all'Unione Europea) o un'organizzazione internazionale può avere luogo senza autorizzazioni specifiche solo se la Commissione Europea ha deciso che il paese terzo o l'organizzazione internazionale garantisce un livello di protezione adeguato, sulla base di una serie di elementi (tra cui il rispetto dei diritti umani e delle libertà fondamentali, l'esistenza e l'effettivo funzionamento delle Autorità di controllo). In mancanza di una decisione di adeguatezza, l'azienda può trasferire i dati personali solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi.

2.2. Diritti degli interessati

2.2.1. Informativa sul trattamento

In conformità ai principi di trasparenza, correttezza, limitazione delle finalità e data retention, le procedure devono prevedere che ai soggetti interessati, all'atto della raccolta dei dati personali, vengano fornite chiare informative circa:

- l'identità del Titolare e del Responsabile del trattamento dei dati personali;
- le caratteristiche del trattamento (es. le finalità e la base giuridica dello stesso, il periodo di conservazione dei dati);
- i diritti del soggetto interessato.

Qualora i dati non siano stati ottenuti presso l'interessato, l'informativa indica anche la fonte da cui hanno origine i dati personali e se si tratta di dati provenienti da fonti accessibili al pubblico.

2.2.2. Diritti d'accesso, rettifica, cancellazione, probabilità e opposizione

Le procedure devono assicurare il rispetto del principio di esattezza e di data retention, prevedendo che ogni interessato abbia il diritto di ottenere:

1. la conferma che siano o meno in corso attività di trattamento di suoi dati personali e informazioni sulle caratteristiche del trattamento (es. finalità, categorie di dati personali, destinatari della comunicazione dei dati, diritti dell'interessato);
2. la rettifica di dati personali inesatti che lo riguardano, nonché la loro integrazione qualora siano incompleti;
3. la cancellazione, se sussistono alcune fattispecie, ad esempio se i dati non sono più necessari rispetto alle finalità per le quali sono stati raccolti, se l'interessato ha revocato il consenso o ha esercitato il diritto di opposizione al trattamento, oppure se i dati personali sono stati trattati illecitamente;
4. la portabilità dei dati oggetto del trattamento, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, qualora il trattamento si basi su un consenso legittimo e sia effettuato con mezzi automatizzati;
5. la cessazione del trattamento dei dati nel caso di trattamento effettuato sulla base del consenso dell'interessato.

Le procedure devono prevedere che, a seguito di ciascuna richiesta, si debbano fornire agli interessati le informazioni necessarie in forma concisa, accessibile ed usando un linguaggio semplice e chiaro, entro un mese (estendibile fino a due mesi, in casi di particolare complessità), anche in caso di diniego.

2.3. Registro dei trattamenti, analisi dei rischi, valutazione d'impatto e consultazione preventiva

Febo S.p.A. è tenuta a predisporre e aggiornare periodicamente un "Registro delle attività di trattamento" che identifichi le attività svolte in qualità di Titolare o di Responsabile del trattamento. Il Registro costituisce la mappatura di tutti i trattamenti effettuati e viene aggiornato periodicamente. Il Registro deve essere reso disponibile su richiesta all'Autorità di Controllo. Il Registro rappresenta la base per assicurare il rispetto dei principi generali sanciti dal Regolamento. Al fine di assicurare l'integrità e la riservatezza dei dati personali, per ciascuna attività di trattamento identificata nel Registro, viene effettuata un'analisi del rischio. Ove da tale analisi emerga che il trattamento possa comportare un livello di rischio elevato per i diritti e le libertà degli interessati, le procedure devono prevedere lo svolgimento di una valutazione di impatto sulla protezione dei dati (Data Protection Impact Assessment, di seguito "DPIA"), previo consulto con il Responsabile del trattamento dati.
In particolare, le procedure devono prevedere che, nel valutare la necessità di effettuare una DPIA su un determinato trattamento, si tenga conto:

1. del livello di rischio per i diritti e le libertà degli interessati,
2. dell'esistenza di un trattamento automatizzato (inclusa la profilazione);
3. del fatto che il trattamento sia effettuato su larga scala o
4. possa comportare la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

2.4. Sicurezza del trattamento

Per garantire un livello di sicurezza del trattamento dei dati adeguato al rischio, le procedure devono definire misure tecniche e organizzative, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi del trattamento e alla natura dei dati personali, in accordo ai principi di "privacy by design" e "privacy by default".
Queste misure possono comprendere:

- la pseudonimizzazione e la cifratura dei dati personali;
- la riservatezza e l'integrità dei sistemi e dei servizi di trattamento assicurate su base permanente;
- meccanismi di verifica e valutazione della loro efficacia.

Tenendo conto dei rischi presentati dal trattamento che derivano, in particolare, dalla distruzione, dalla perdita o dalla modifica non autorizzata di dati personali, le procedure devono definire le misure di sicurezza che possono garantire un adeguato livello di protezione dei dati personali di default e in via preventiva rispetto allo stesso trattamento dei dati personali.

2.5. Gestione degli eventi di "data breach"

Sempre al fine di assicurare il rispetto dei principi di integrità e riservatezza dei dati personali, laddove sia identificata una violazione di sicurezza, accidentale o illecita, che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata dei dati compromettendone la riservatezza, la disponibilità o l'integrità, le procedure devono assicurare, previo coinvolgimento del Responsabile del trattamento dati, che la notifica all'Autorità di Controllo avvenga entro 72 ore dal momento in cui sia stata ravvisata la violazione.
Tale notifica contiene:

- la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati;
- i dati di contatto del Responsabile del trattamento dati;
- le probabili conseguenze della violazione;
- le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e attenuarne i possibili effetti negativi.

Qualora la notifica non sia effettuata entro 72 ore, devono essere indicati i motivi del ritardo. Nei casi in cui la violazione possa comportare elevati rischi per i diritti e le libertà dei soggetti interessati, le procedure devono prevedere che - previo consulto con il Responsabile del trattamento dati - sia fornita agli interessati informativa sulla violazione senza ingiustificato ritardo. Tale comunicazione non è necessaria se comporterebbe uno sforzo sproporzionato oppure se sono state adottate misure tecniche ed organizzative adeguate alla tutela dei dati (es. cifratura).
Le procedure devono stabilire che:

1. la scelta della modalità di comunicazione dovrà tenere in considerazione l'accessibilità dei soggetti interessati a formati diversi, e, ove necessario, le diversità linguistiche dei destinatari; e
2. ciascuna violazione dei dati personali, sospetta o accertata, deve essere adeguatamente censita e documentata nel registro delle violazioni al fine di garantire il rispetto del principio di accountability.

Serravalle Pistoiese, 28/02 /2019