Guida per la protezione dei dati attraverso il principio della Privacy by Design e by Default

Introduzione

Quando ECOLOGICA SERVIZIO AMBIENTE 2000 SRL (qui di seguito "ECOLOGICA") sviluppa nuovi servizi per i suoi clienti o considera nuove attività di elaborazione dati (definite di seguito), in particolare implementando una nuova pratica aziendale, o tecnologia o sistema IT (ad esempio applicazioni, software, database, funzionalità) o modifica qualsiasi attività di elaborazione dati esistente, ci sono determinati requisiti che vengono rispettati in tema di protezione dei dati. La società ha ben presente che una protezione dei dati in base alla progettazione e per impostazione predefinita promuove la conformità alla privacy e alla protezione dei dati prima dell'avvio di un progetto.

Definizioni

Attività di elaborazione dati

Indica l'implementazione di nuove modifiche o modifiche a attività di elaborazione dati esistenti come lo sviluppo, la progettazione, la selezione e l'uso di sistemi IT che elaborano dati personali e / o trasferiscono dati personali.

Leggi sulla protezione dati personali

Indica il regolamento generale sulla protezione dei dati e qualsiasi altra legge, regolamento e normativa applicabile in materia di protezione delle persone in relazione al trattamento e alla libera circolazione dei dati personali in qualsiasi paese pertinente

Dati personali

Indica qualsiasi informazione da cui possa essere identificato una persona fisica, come il nome, l'indirizzo, la data di nascita, il numero di patente, il numero del conto bancario, i numeri delle carte di credito o di debito, informazioni sanitarie o mediche, numero di assicurazione o di identità o fotografia etc.

Pseudoanonimizzazione

Significa convertire i Dati personali in un modulo in cui le persone non possono più essere identificate da tali dati senza l'uso di ulteriori informazioni, a condizione che queste informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative per garantire che gli individui non vengano nuovamente identificati. Ad esempio, se ECOLOGICA dovesse conservare i nomi e i numeri di telefono dei clienti, questi dati potrebbero essere pseudonimizzati tenendo separati i nomi e i numeri di telefono e crittografando i nomi in modo che gli individui non possano più essere identificati a meno che i dati dei nomi non vengano decodificati e i due dataset siano ricombinati.

Dati sensibili

Indica informazioni riguardanti razza, origine etnica, affiliazione politica, appartenenza sindacale, genetica, dati biometrici (se utilizzati per scopi di identificazione), salute e orientamento sessuale.

Perché abbiamo bisogno di questa guida?

Questa guida è particolarmente rivolta alle situazioni in cui ECOLOGICA:

- Crea o integra sistemi IT che comprendono l'archiviazione o l'accesso ai dati personali.
- Progetta strategie che hanno implicazioni sulla privacy.
- Implementa un'iniziativa di condivisione dei dati personali (ad esempio, una nuova pratica aziendale che prevede la condivisione di dati personali).
- Utilizza dati personali esistenti per un nuovo scopo

Qualora si manifestassero circostanze in cui ECOLOGICA si sta impegnando in attività di elaborazione dei dati che possono presentare un rischio elevato per le persone interessate, potrebbe essere necessario anche aver bisogno di completare una valutazione dell'impatto sulla protezione dei dati ("DPIA").

Protezione dei dati by Design

Un approccio basato sulla protezione dei dati dalla fase di progettazione promuove la conformità alla privacy e alla protezione dei dati prima dell'avvio di un progetto. Quando decidere in che modo il trattamento dei Dati personali sarà eseguito in connessione con un nuovo progetto e durante l'elaborazione stessa, ECOLOGICA dovrebbe prendere in considerazione e incorporare adeguate misure di sicurezza e salvaguardie al fine di attuare i seguenti principi:

- Trasparenza: i dati personali devono essere trattati in modo equo, legale e trasparente.
- Scopo / restrizione: I dati personali devono essere ottenuti solo per uno o più scopi specificati, espliciti e leciti e non trattati in alcun modo incompatibili con tale scopo o con tali scopi.
- Riduzione dei dati: i dati personali devono essere adeguati, pertinenti e limitati a quanto necessario in relazione allo scopo per cui sono trattati. ECOLOGICA non dovrebbe elaborare più dati del necessario o elaborare i dati più a lungo del necessario.
- Qualità dei dati: i dati personali devono essere accurati e aggiornati. Dati personali imprecisi dovrebbero essere corretti o cancellati senza indugio (a seconda del contesto).
- Principio di Need-to-Know: i dati personali devono essere conservati in una forma che consenta l'identificazione degli interessati per un periodo non superiore a quello necessario per lo scopo per il quale sono trattati.
- Diritti sui dati: I dati personali devono essere trattati in conformità con i diritti degli interessati, quali il diritto di richiedere una copia dei dati personali detenuti da ECOLOGICA su di essi (richiesta di accesso), avere i loro dati corretti o cancellati, o opporsi a determinate attività di elaborazione.
- Riservatezza del trattamento: devono essere adottate misure tecniche e organizzative adeguate contro l'elaborazione non autorizzata o illecita di dati personali e contro la perdita accidentale o la distruzione o il danneggiamento dei dati personali.
- Trasferimento di dati: i dati personali non devono essere trasferiti in un paese / territorio al di fuori dell'EU, a meno che tale paese / territorio non assicuri un livello adeguato di protezione dei dati personali.

Regole

Ci sono una varietà di passaggi che ECOLOGICA può intraprendere per dimostrare di aver preso in considerazione la protezione dei dati in base alla progettazione in relazione a qualsiasi attività di elaborazione dei dati. Quali misure siano appropriate dipenderanno dal particolare progetto e dal probabile rischio per i Dati personali degli individui, ma le seguenti linee guida dovrebbero essere osservate:

- Effettuare penetration prima del lancio di qualsiasi nuovo sistema.
- Pseudonimizzare i dati personali ove possibile e praticabile.
- Assicurarsi che siano in atto processi di autenticazione per limitare l'accesso ai Dati personali.
- Condurre la dovuta diligenza sui fornitori di servizi di terze parti per verificare la loro conformità alle leggi sulla protezione dei dati.
- Utilizzare livelli appropriati di crittografia (ad esempio, la crittografia dovrebbe essere normalmente utilizzata per proteggere i dati personali sensibili).
- Condurre DPIA per le attività di elaborazione dei dati laddove vi sia la probabilità che tale attività possa o possa comportare un alto rischio per i diritti e le libertà delle persone.

Protezione dei dati by default

L'approccio standard di ECOLOGICA a tutte le attività di elaborazione dati dovrebbe essere:

- Per impostazione predefinita, vengono elaborati solo i Dati personali che sono necessari per ogni specifico scopo del trattamento;
- Per impostazione predefinita, i Dati personali non vengono conservati per un periodo di tempo superiore a quello necessario per lo scopo dell'elaborazione (consultare Registro dei trattamenti);
- Per impostazione predefinita, i Dati personali non sono resi accessibili a un numero indefinito di individui; tale accesso dovrebbe essere limitato utilizzando i controlli pertinenti all'interno dei sistemi IT e fornito al personale sulla base della necessità di conoscere solo per la loro funzione lavorativa.

Regole

Al fine di dimostrare che ECOLOGICA ha considerato la protezione dei dati per impostazione predefinita in relazione a qualsiasi attività di elaborazione dei dati, si rende necessario:

- Comunicare agli interessati lo scopo per cui i Dati personali sono raccolti, utilizzati e conservati. Questo dovrebbe essere fatto prima o al momento in cui i Dati personali vengono raccolti (ad esempio tramite la relativa informativa sulla privacy).
- Garantire che le tecniche di raccolta dei dati prevengano l'eccessiva raccolta di dati.
- Introdurre procedure e procedure di cancellazione appropriate per rimuovere i Dati personali dopo un determinato periodo di tempo, quando non è più necessario archiviare i Dati personali per gli scopi per cui sono stati raccolti.
- Astenersi dall'utilizzare, per quanto possibile, commenti di campo aperti per questionari e sondaggi interni.