Tel e Fax - +39 06 88805551
Web - www.lynxlab.com
Mail - info@lynxlab.com
Pec - lynx1@pec.it

LYNX s.r.l.
P.IVA 04854721000
C.C.I.A. RM812186 – Trib. 2552/95
Via Salaria 292 - 00199 Roma

GDPR Customer Care

ver 7 del 23/01/20

Documento riservato

Presentazione

Caso d'uso

L'azienda ABCWeb gestisce diverse applicazioni web che trattano i dati degli utenti. Quando è entrato in vigore il GDPR ha inserito un indirizzo di email in fondo alla pagina e il link alla pagina delle policy relative alla privacy.

Purtroppo questo non è sufficiente e genera ulteriori carichi di lavoro per ABCWeb:

- la societò non ha modo di monitorare le richieste che arrivano all'indirizzo

- non può esibire una prova del fatto che siano stato prese in carico entro 30 gg

- deve rispondere manualmente ad ogni utente che chiede notizie relativamente alla sua richiesta, andando a reperire le informazioni da altri servizi

Inoltre le policy cambiano, o sono diverse per le diverse applicazioni.

Descrizione

GDPR Customer Care è un'applicazione web pensata per la gestione semplificata delle richieste GDPR e delle policies relative alla privacy.

E' indipendente dalle applicazioni, dai contesti e dai siti, e permette di gestire la raccolta delle richieste, ma anche la loro evasione.

E' composto da due moduli pubblici (aperti agli utenti dell'azienda, dipendenti o clienti che siano) e due riservati al Manager GDPR

Consente di avere un'interfaccia web attraverso la quale gli utenti possono esercitare i loro diritti ai sensi del GDPR e da una dashboard dove il manger GDPR può gestire le richieste.

Consente inoltre di gestire in maniera centralizzata una o più Policy GDPR, anche differenziate per sito.

Tel e Fax - +39 06 88805551
Web - www.lynxlab.com
Mail - info@lynxlab.com
Pec - lynx1@pec.it

LYNX s.r.l.
P.IVA 04854721000
C.C.I.A. RM812186 – Trib. 2552/95
Via Salaria 292 - 00199 Roma

Moduli

1. Modulo di invio richiesta

Accesso: Pubblico

Permette di vedere le policy attuali, obbligatorie e non, e di effettuare una richiesta GDPR.

L'utente deve inserire nome cognome, email e *captcha*

Opzionalmente, può essere fatta una verifica dell'unicità dell'utente (ad esempio tramite la chiamata di un metodo di autenticazione del sistema informativo dell'azienda)

Se l'utente esiste ed è unico (oppure se non si attiva il controllo dell'unicità) l'utente può inserire la tipologia di richiesta con un testo di accompagnamento (ad es. le motivazioni della richiesta).

Quando la richiesta è inviata, il modulo genera un token di tipo *onetime* che viene riportato nel testo di un'email inviata all'indirizzo fornito, insieme alla url da visitare per la conferma.

Se l'utente visita la URL (cioè conferma la sua identità) si registra la richiesta come verificata e viene inviata una seconda email di conferma all'utente con il numero di pratica e un nuovo token.

2. Modulo per il controllo e l'evasione delle richieste GDPR

Accesso: Riservato al manager GDPR

Vengono mostrate le richieste:

- ricevute

- chiuse

con numero di pratica, utente, data, testo e la possibilità di eseguire due azioni:

- chiudi (annulla la richiesta, ad esempio perché non sussistono le condizioni)

- evadi (esegue un'azione predefinita ma configurabile, e poi chiude)

Le azioni predefinite sono, ad esempio, la visita di una URL (per esempio, l'endpoint di un API) o l'invio di un'email, con i parametri riempiti con i dati della richiesta. Se l'azione

remota restituisce un risultato, quel risultato può essere visualizzato.

Le azioni possono essere configurate direttamente dall'azienda.

3. Modulo per la verifica dello stato

Accesso: Pubblico

L'utente può verificare lo stato della sua richiesta: data, tipo, stato (aperto, chiuso)

La forma richiede l'inserimento del numero di pratica e di un token (che è quello inviato in precedenza).

4. Modulo per la gestione delle policy

Accesso: Riservato al manager GDPR

Permette la creazione, editing, cancellazione, attivazione della/e policies GDPR

Oltre all'editing, il modulo tramite API fornisce le policies aggiornate a tutte le applicazioni dell'azienda che ne fanno richiesta, in modo da evitare duplicati, versioni non allineate etc.

Configurazioni

Multisito

Tramite API, i moduli per l'utente finale (richiesta o verifica) possono se necessario essere moltiplicati e comunicare con il modulo Master di gestione delle richieste e con il modulo di gestione delle Policies.

In questo modo, più società di un gruppo (oppure più contesti applicativi con utenti separati) possono avere ognuna la sua interfaccia dedicata, mentre le richieste sono gestite in maniera centralizzata da un unico punto.

Modalità

GDPR Customer Care può essere installato presso il cliente, oppure fornito come servizio. In questo secondo caso, possiamo garantire connettività tramite HTTPS, la cifratura dei dati personali degli utenti a livello di database, chiavi crittografiche conservate in maniera sicura (es. AWS KMS).