UNIVERSITÉ TOULOUSE Jean Jaurès

Fiche de conseil juridique

22/12/2024

1. Informations générales

Ce document est la fiche de conseils juridiques et de sécurité du groupe 2A9 concernant la création du site de e-commerce de Nautic Horizon.
Le groupe 2A9 est composé de :

- GUILLUY Matt (Scrum Master)
- AMERI Mohammed
- CARDOUAT Alexi
- FUSI BELAID Thomas

L'objectif est de définir les mesures nécessaires pour assurer la conformité du site au RGPD, ce qui nous permettra d'identifier les tâches à accomplir lors du dernier sprint. Ce document sera adapté dans le cas de Nautic Horizon nous ne prendrons donc pas en compte certains cas comme les micro entreprises ou un entrepreneur individuel.

2. Mentions légales obligatoires

Voici la liste des mentions légales qui devront figurer sur notre site:

- Informations sur l'entreprise et l'hébergeur:
  - Dénomination sociale et forme juridique de l'entreprise
  - Adresse du siège social de l'entreprise
  - Numéro d'immatriculation au RCS
  - Numéro d'identification à la TVA
  - Coordonnées de contact: adresse mail et numéro de téléphone de contact
  - Identité de l'hébergeur du site: nom ou dénomination sociale, adresse, contact

- Les conditions générales de vente (CGV) qui servent à encadrer les relations commerciales :
  - Caractéristiques essentielles du bien ou du service
  - Prix TTC en euros
  - Frais, date et modalités de livraison
  - Modalités d'exécution du contrat
  - Modalités de paiement
  - Droit de rétractation (délais et conditions)
  - Garantie légale de conformité et garantie des vices cachés
  - Garantie commerciale et service après vente
  - Durée du contrat et conditions de résiliation, s'il y a lieu
  - Caution ou garantie à fournir par le client, s'il y a lieu
  - Durée minimale des obligations contractuelles du client, s'il y a lieu
  - Existence d'un code de conduite applicable au contrat, s'il y a lieu
  - Modalités de règlement des litiges : tribunal compétent et possibilité de recourir à un médiateur.

- Politique de cookies :
  - Mentionner l'utilisation de cookies
  - Décrire leur finalité
  - Expliquer les modalités d'acceptation et de refus

- Propriété intellectuelle
  - Indiquer les protections applicables au contenu du site (logo, images, texte, …)
  - Préciser que toute reproduction ou utilisation non autorisée est interdite

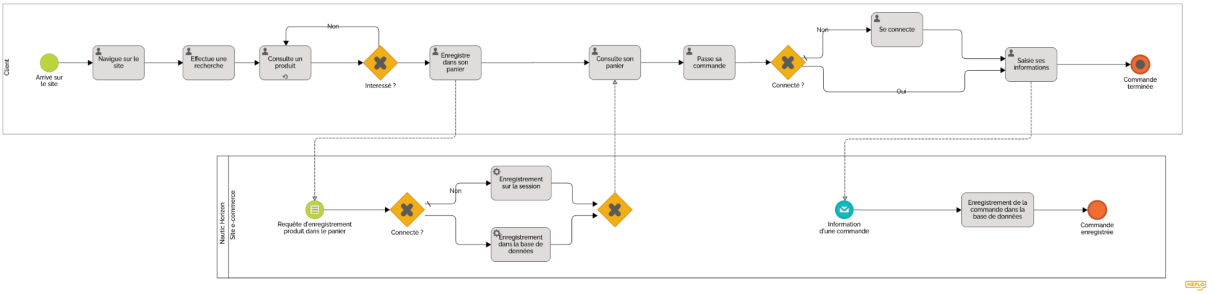
- Résiliation de contrat: possibilité de résilier son contrat par voie électronique

Mentions manquantes à ce jour:

- Tout sauf la dénomination sociale de l'entreprise et la note sur la propriété intellectuelle

3. Description du processus de vente en ligne

Diagramme de collaboration BPMN détaillant le processus de vente en ligne:



4. Protection des données

Liste des mesures applicables, de leurs modalités et de leurs priorités concernant la protection des données.

Mesure	**Modalités**	**Priorité**
Obtenir le consentement explicite des utilisateurs	Implémenter une case à cocher obligatoire pendant le processus d'inscription ou de création de compte, avec une mention claire indiquant que l'utilisateur accepte le traitement de ses données personnelles.	Must
Informer sur la collecte et l'utilisation des données	Ajouter une politique de confidentialité détaillant les droits des utilisateurs et les finalités du traitement dans les formulaires d'inscription et sur le site.	Must
Faciliter la gestion des données personnelles	Offrir aux utilisateurs la possibilité de consulter, rectifier ou supprimer leurs données personnelles via un formulaire dédié ou un tableau de bord accessible depuis leur compte.	Must
Assurer la sécurité des données sensibles	Activer le protocole HTTPS sur tout le site pour sécuriser les échanges de données. Utiliser un hachage sécurisé des mots de passe.	Must
Désigner un Délégué à la Protection des Données (DPO)	Nommer un DPO chargé de superviser la conformité avec les régulations de protection des données et de gérer les demandes des utilisateurs concernant leurs données.	Should
Informer sur les transferts de données	Indiquer clairement dans la politique de confidentialité les situations dans lesquelles des données peuvent être transférées à des partenaires ou à l'international, avec des garanties appropriées.	Should
Garantir la conservation limitée des données	Préciser dans les mentions légales la durée de conservation des données	Should

	personnelles et s’assurer que cette durée est conforme à la finalité du traitement.	

5. Sécurité des données

Liste des mesures applicables, de leurs modalités et de leurs priorités concernant la sécurité des données.

Mesure	**Modalités**	**Priorité**
Chiffrer les données sensibles	Utiliser un hachage sécurisé pour les mots de passe et garantir que les autres informations sensibles, comme les informations bancaires, sont cryptées à l’aide de protocoles modernes.	Must
Imposer le protocole HTTPS	Forcer l’utilisation du protocole HTTPS sur l’ensemble du site, afin de garantir la sécurité des échanges entre le navigateur de l’utilisateur et le serveur.	Must
Protéger contre les attaques XSS	Mettre en place une validation systématique des entrées utilisateurs pour éviter les injections malveillantes et utiliser des mécanismes comme l’échappement des caractères.	Must
Exiger des mots de passe complexes	Imposer des règles strictes concernant la création de mots de passe (au moins 8 caractères, incluant des majuscules, minuscules, chiffres et symboles).	Must
Utiliser un prestataire tiers pour le traitement des paiements	Ne jamais stocker localement les coordonnées bancaires des clients. Faire appel à des prestataires de paiement certifiés, comme PayPal, pour traiter les transactions financières.	Must
Limiter les tentatives de connexion	Mettre en place une protection contre les attaques par force brute, par exemple en limitant le nombre de tentatives de connexion et en appliquant un verrouillage temporaire après plusieurs échecs.	Should
Sécuriser l'accès aux données	Limiter l’accès aux données personnelles à des employés ou prestataires autorisés et mettre en œuvre une politique stricte	Should

	d’accès basée sur les rôles..	

6. Liste des US à ajouter

Concernant la protection des données :

US	Description	Priorité
US01	En tant qu’utilisateur, je veux qu’une case à cocher obligatoire apparaisse lors de l’inscription pour consentir au traitement des données personnelles.	Must
US02	En tant qu’utilisateur, je veux pouvoir consulter la politique de confidentialité et savoir clairement comment mes données seront utilisées, stockées et protégées.	Must
US03	En tant qu’utilisateur, je veux avoir un moyen facile de consulter, rectifier ou supprimer mes données personnelles à tout moment.	Must
US04	En tant qu’utilisateur, je veux que toutes les informations sensibles (comme mes mots de passe) soient protégées par un protocole HTTPS et un hachage sécurisé.	Must
US05	En tant qu’utilisateur, je veux être informé si mes données sont transférées à des partenaires ou en dehors de l'UE, avec des garanties adéquates.	Should
US06	En tant qu’entreprise, je veux qu’il soit précisé dans les mentions légales la durée de conservation de mes données personnelles.	Should

Concernant la sécurité des données:

US	Description	Priorité
US07	En tant qu’administrateur, je veux que les mots de passe et autres informations sensibles soient hachés et chiffrés avec des protocoles modernes pour garantir leur sécurité.	Must
US08	En tant qu’utilisateur, je veux que l’ensemble du site utilise HTTPS pour sécuriser les échanges de données entre mon navigateur et le serveur.	Must

US09	En tant qu'administrateur, je veux que toutes les entrées utilisateur soient validées pour éviter les attaques par injection XSS.	Must
US10	En tant qu'administrateur, je veux imposer une politique de mots de passe forts pour les utilisateurs, comprenant des majuscules, des minuscules, des chiffres et des symboles.	Must
US11	En tant qu'entreprise, je veux utiliser un prestataire tiers certifié (comme PayPal) pour traiter les paiements, sans stocker les coordonnées bancaires localement.	Must
US12	En tant qu'administrateur, je veux limiter le nombre de tentatives de connexion afin de protéger le site contre les attaques par force brute.	Should
US013	En tant qu'administrateur, je veux restreindre l'accès aux données personnelles à des employés autorisés et mettre en place un contrôle d'accès basé sur les rôles.	Should