

Droit – Analyse d'impact

G1B-6 Esteban, Enzo, Marwan et Hai-Son



Sommaire :

1- Vue d'ensemble des traitements réalisés (Esteban) :	2
2- Données, processus & support (Esteban) :	3
3- Récapitulatif des risques (Enzo) :	6
4- Liste de mesures applicables et leurs modalités de mise en œuvre concernant la protection des données (Enzo) :	6
5- Liste de mesures applicables et leurs modalités de mise en œuvre concernant la sécurité des données (Marwan) :	7
6- Liste des issues à ajouter au dernier sprint pour tenir compte des points 4 et 5 les plus importants (Marwan) :	8

1- Vue d'ensemble des traitements réalisés (Esteban) :

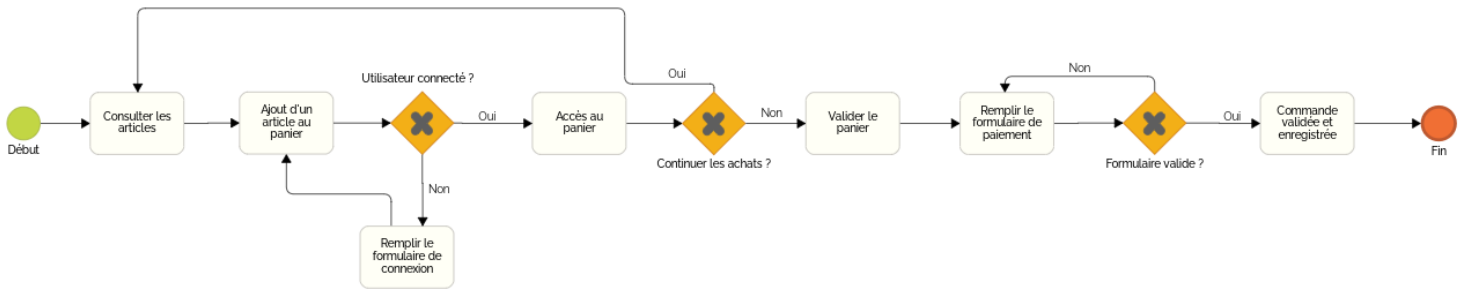
Numéro du traitement	Description	Finalités	Enjeux	Responsable(s)
1	Le site web de SubOne permet aux clients d'acheter des sous-marins.	Acheter des articles.	Créer un nouveau service de vente de sous-marins, créer une clientèle pour l'entreprise.	SubOne.
2	Le site web SubOne propose à l'utilisateur de se créer un compte.	Posséder un compte.	Permettre au client d'acheter des articles sur le site web de SubOne.	SubOne & le client.
3	Le site web SubOne propose aux clients de se connecter à leurs comptes.	Nécessaire pour acheter des articles, accéder à son espace client.	Permettre au client d'acheter des articles sur le site web de SubOne.	SubOne & le client.
4	Le site web SubOne propose aux clients de supprimer leurs comptes.	Supprimer son compte, retirer ses informations de la base de données de l'entreprise.	Permet au client d'avoir une marge de liberté sur ses données personnelles.	SubOne & le client.
5	Le site web SubOne propose aux clients de modifier leurs comptes.	Modifier son compte et donc ses informations dans la base de données de l'entreprise.	Permet au client d'avoir une marge de liberté sur ses données personnelles.	SubOne & le client.

6	Le site web SubOne propose aux clients de consulter leurs paniers.	Voir le détail du panier (prix total, articles et quantités), afin de le supprimer, de le modifier ou de le valider (passer à la commande).	Permet au client d'avoir une emprise totale sur son panier, de le supprimer si besoin etc.	SubOne.
7	Le site web SubOne propose aux clients de consulter leurs commandes et leurs détails.	Voir ses différentes commandes et leurs détails (numéro de la commande, prix, articles commandés et quantités de chaque articles).	Permet au client d'avoir une idée de ses commandes passées.	SubOne.

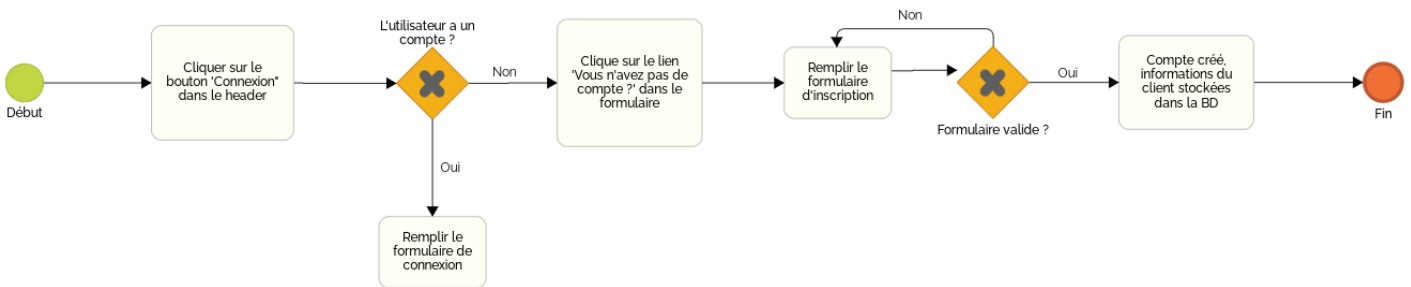
2- Données, processus & support (Esteban) :

Traitement	Données fournies par le client	Durée de conservation
Commander des articles	Nom, prénom, numéro de CB, date d'expiration et cryptogramme.	Aucune conservation.
Créer un compte	Nom, prénom, adresse e-mail, numéro de téléphone et mot de passe.	Jusqu'à la demande de suppression du client.
Connexion à son compte	Adresse e-mail et mot de passe.	Jusqu'à la déconnexion du client.
Modification de son compte	Nom, prénom, adresse e-mail, numéro de téléphone et mot de passe.	Jusqu'à la demande de suppression du client.

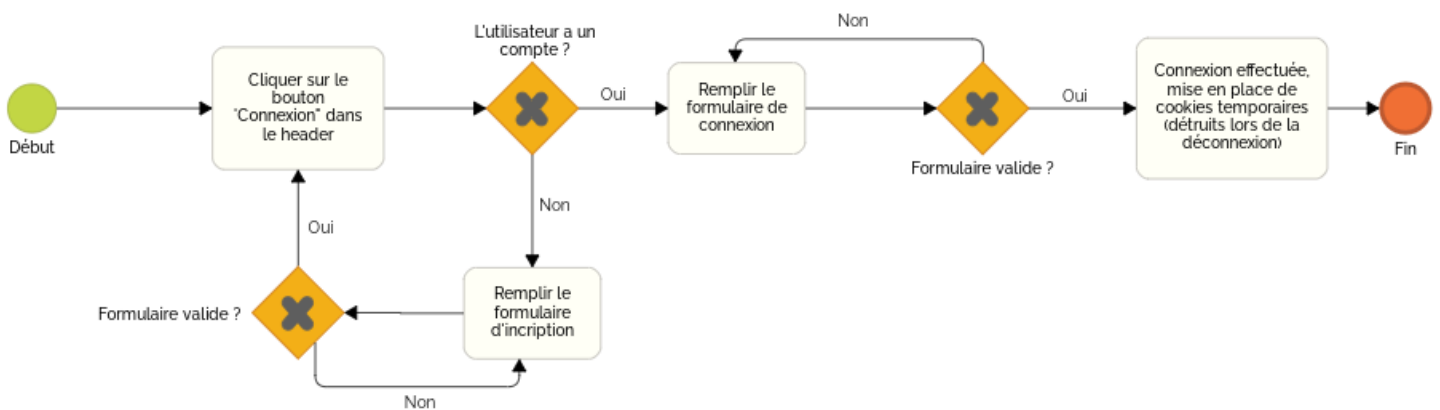
Processus de commande :



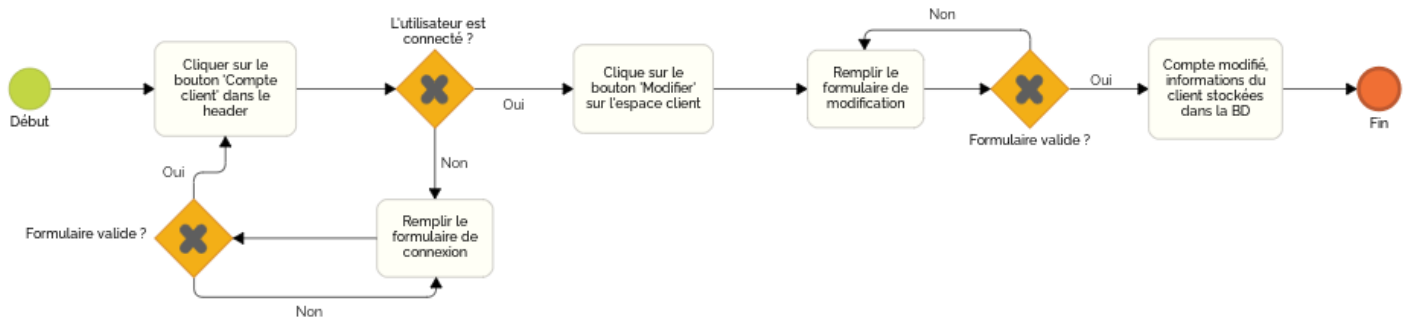
Processus de création de compte :



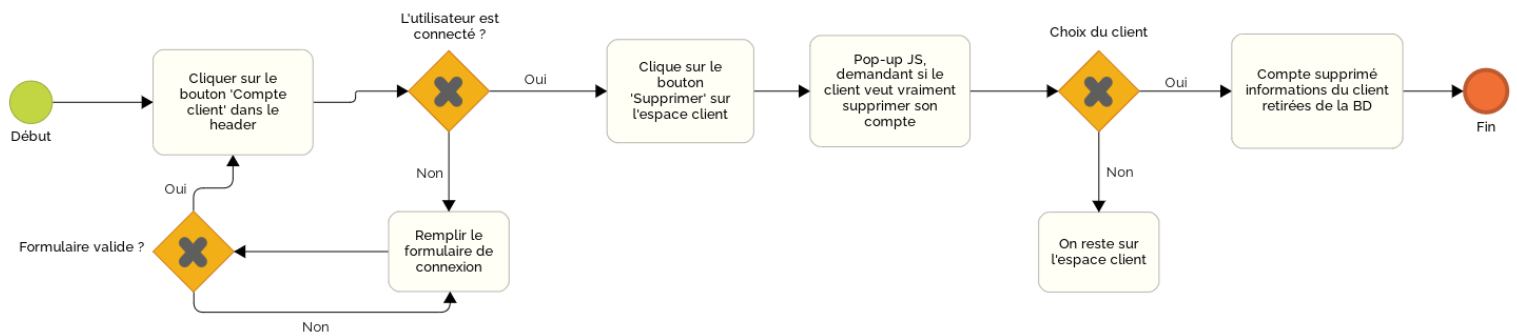
Processus de connexion à un compte :



Processus de modification de compte :



Processus de suppression de compte :



3- Récapitulatif des risques (Enzo) :

Risque	Menaces	Impacts	Mesures pour réduire le risque	Niveau de risque
Accès illégitime aux données	Vol de données confidentielles des clients	Utilisation des données bancaire et usurpation d'identité	Chiffrer les données sensibles et empêcher les accès non autorisé	Élevé
Modification frauduleuse des données	Les données des clients et les données du sites ne sont plus les bonnes	Peut bloquer la connexion d'un client et faire perdre de l'argent	Sécuriser les accès à la base de données	Élevé
Suppression frauduleuse des données	Suppression de données dans la base de données	Obligé de recréer un compte, de remettre toute les données	Sécuriser la base de données face aux tentatives de modifications de celle-ci	Limité
Ajout de donnée frauduleuse	Site/base de données qui ne fonctionne plus	Affichage des informations non fonctionnel	Sécuriser l'ajout de données	Limité

4- Liste de mesures applicables et leurs modalités de mise en œuvre concernant la protection des données (Enzo) :

Mesure	Modalités	Priorité
Chiffrement des données	Même si les données sont volées, celles-ci seront chiffrées donc inexploitable	Élevée
Backup des données	Si la base de données est corrompue ou supprimée, avoir une sauvegarde permet de rapidement remettre la base de données en l'état	Moyenne
Avertissement de faille de sécurité	En cas de vol de données sensibles des clients, les prévenir	Élevée

Surveillance des données	Les données sont surveillées pour mieux déceler les problèmes et y remédier rapidement	Moyenne
Surveillance des accès à la base de données	Les accès à la base de données sont vérifiés pour être sûr de leurs autorisation	Élevée

5- Liste de mesures applicables et leurs modalités de mise en œuvre concernant la sécurité des données (Marwan) :

Mesure	Modalités	Priorité
Contrôle de la confidentialité des accès (connexion)	Par identifiant et mot de passe. Il est de la responsabilité de l'utilisateur de maintenir la confidentialité de ses informations de connexion	Moyenne
Archivage des données	Les données concernant le nom, prénom, numéro de téléphone et adresse e-mail du client sont conservées	Élevée
Utilisation d'un mot de passe robuste	Mise en place de contraintes pour la création d'un mot de passe (8 caractères minimum, au moins 1 majuscule, 1 minuscule et 1 chiffre)	Élevée
Sécuriser le compte	Mise en place de l'authentification à double facteur, offre davantage de sécurité que le simple mot de passe	Élevée
Chiffrement des données sensibles	Les mot de passes sont chiffrés	Élevée

6- Liste des issues à ajouter au dernier sprint pour tenir compte des points 4 et 5 les plus importants (Marwan) :

- Mise en place de l'authentification à double facteur,
- Mise en place de sauvegarde des données,
- Mise en place d'avertissements en cas de faille de sécurité,
- Mise en place d'une surveillance des accès à la base de données.