Equipe G1A-3 :

Benachir Alexandre
Mabille Matthis
Massip Romain
Babel Teddy
Druelle Julien

Analyse d’impact “La Parure Française”

Table des matières

1. Vue d'ensemble des traitement réalisés 3
2. Description des processus, des données et supports. 3
3. Un récapitulatif des risques et leurs conséquences en matière de cyber sécurité. 5
4. Mesures applicables et modalités de mise en œuvre pour la protection des données 5
5. Mesures applicables et modalités de mise en œuvre pour la sécurité des données 6
6. Liste des issues à ajouter au sprint 8 pour tenir compte des points les plus importants 6

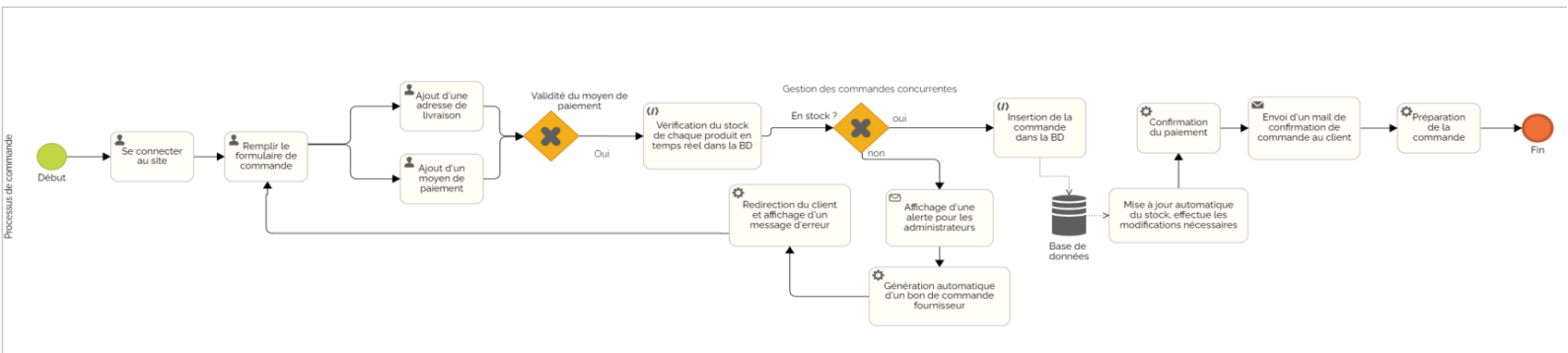
Analyse d'impact "La Parure Française"

1. Vue d'ensemble des traitement réalisés

Description du traitement	Finalités du traitement	Enjeux du traitement	Responsable du traitement	Sous-traitant(s)
Enregistrement d'un compte utilisateur.	Permettre aux utilisateurs de créer un compte sur le site de "La Parure Française" en saisissant des informations telles que leur nom, adresse email et mot de passe. Les utilisateurs pourront ensuite se connecter à leur compte pour accéder à des fonctionnalités exclusives du site, comme le suivi de leur historique d'achat.	Protection des données personnelles des utilisateurs Conformité avec les règles de protection des données Éviter les risques de fuites de données ou de piratage.	Responsable de la gestion des comptes utilisateurs de "La Parure Française"	Google (connexion par mail)
Traitement des paiements	Permettre aux utilisateurs de payer pour leurs achats en ligne en utilisant différentes méthodes de paiement telles que les cartes de crédit ou les portefeuilles électroniques.	Sécurité des transactions, conformité avec les normes de paiement en vigueur	Responsable de la gestion des paiements de "La Parure Française"	Prestataire de paiement tiers comme PayPal / Skrill / Venmo
Traitement des commandes	Gérer les commandes passées par les utilisateurs sur le site, incluant la vérification des informations de commande, la facturation et l'expédition.	Respect des obligations légales et contractuelles, gestion efficace des commandes	Responsable de la gestion des commandes de "La Parure française"	Prestataire de logistique tiers comme DHL / Colissimo / Chronopost
Stockage des données	Stocker les données des utilisateurs et des commandes pour une utilisation ultérieure telle que la personnalisation de l'expérience utilisateur. Cela inclut également la gestion des données de facturation et les historiques d'achat.	Respect de la confidentialité et de la sécurité des données, conformité avec les règles de stockage de données	Responsable de la gestion des données de "La Parure française"	Prestataire de stockage de données tiers comme Amazon Web Services / Microsoft Azure / Google Cloud

2. Description des processus, des données et supports.

Processus BPMN de commande : *(veuillez grossir l'image pour une meilleure visibilité)*



Description des données (Commandes / Comptes Clients) :

Données	Destinataires	Durées de conservation
Informations de compte (nom, prénom, date de naissance, pays, département, adresse email, adresse postale)	Service après-vente, Service marketing, différents prestataires possibles en cas de partenariats (toujours en respectant les lois et réglementations en matière de confidentialité)	Pour la durée de l'utilisation du compte, puis supprimées après 3 ans d'inactivité ou à la demande de suppression du compte
Historique des commandes et des paiements	Service logistique, Service informatique, Service après-vente	5 ans à compter de la dernière commande client (3 ans si inactif)
Informations de paiement / Adresse de facturation	Service logistique, Service informatique	Conformément aux politiques de confidentialités de la plateforme de paiement utilisée

Description des supports par processus :

Processus	Description détaillée du processus	Supports des données concernés
Création de compte	Lors de la création d'un compte sur le site web de vente de vêtements, les utilisateurs fournissent des informations personnelles telles que leur nom, prénom, date de naissance, département, adresse e-mail et leur adresse postale. Ils pourront ensuite enregistrer ultérieurement leurs informations de paiement (adresse de livraison, moyen de paiement). Ces informations sont utilisées pour donner accès aux fonctionnalités et avantages réservés aux utilisateurs enregistrés et simplifier les processus d'achat en enregistrant les informations de livraison et de paiement des utilisateurs.	Base de données (clients), système d'enregistrement de compte
Traitement des paiements	Pour permettre aux utilisateurs de payer leurs commandes sur le site web de ventes de vêtement, une plateforme de paiement en ligne est mise à disposition. Celle-ci permet de collecter les informations de paiement des utilisateurs, telles que les numéros de cartes de crédit ou les informations de compte PayPal, Skrill ou Venmo pour traiter les paiements. Pour assurer la sécurité des transactions, les informations de paiement sont cryptées lors de tout paiement.	Base de données (paiement), serveur de paiement sécurisé
Historique des commandes	A chaque commande passée sur le site web de vente de vêtements, des informations détaillées sont collectées auprès des utilisateurs. Ces informations incluent les articles sélectionnés, leur taille, leur coloris, les prix associés, les détails de livraison et de facturation ainsi que les informations de paiement. Ces données sont ensuite utilisées pour traiter efficacement les commandes, suivre leur progression et générer des factures pour les clients.	Base de données (commandes), système de gestion de commandes

3. Un récapitulatif des risques et leurs conséquences en matière de cyber sécurité.

Risque	Principales menaces	Principaux impacts	Mesures pour réduire ce risque	Niveau de gravité
Vol de données personnelles	Phishing, malware, attaques de force brute	Atteinte à la vie privée des utilisateurs, perte de confiance des clients, dommages à la réputation de l'entreprise, responsabilité juridique	Mise en place d'une politique de sécurité des données, formation des employés, utilisation de logiciels de sécurité	Élevé
Attaques DDoS	Flooding de trafic	Interruptions du service, perte de ventes, dommages à la réputation de l'entreprise	Mise en place de solutions de filtrage de trafic, utilisation de services de protection DDoS	Moyen-Élevé
Piratage de compte administrateur	Phishing, utilisation de mots de passe faibles	Modification de contenu du site, accès non autorisé à des données sensibles	Utilisation de mots de passe forts et de l'authentification à deux facteurs, surveillance régulière des comptes administrateur	Elevé
Failles de sécurité	Vulnérabilités non patchées, configurations de sécurité défectueuses	Accès non autorisé aux données sensibles, prise de contrôle du système	Mise en place d'une stratégie de gestion des vulnérabilités, utilisation de logiciels de sécurité, surveillance régulière des activités de réseau	Elevé

4. Mesures applicables et modalités de mise en œuvre pour la protection des données

Mesure	Modalités	Priorité
Cryptage de toutes les données	Utilisation de technologies de cryptage pour protéger les données sensibles	Haute
Sécurité des réseaux	Mise en place de firewalls et de protocoles de sécurité pour protéger les données transitant sur les réseaux	Haute
Sauvegarde et restauration	Mise en place de procédures de sauvegarde et de restauration des données pour éviter les pertes de données en cas d'incident	Moyenne-Haute
Contrôle d'accès	Mise en place de procédures de contrôle d'accès pour limiter l'accès aux données sensibles	Haute

5. Mesures applicables et modalités de mise en œuvre pour la sécurité des données

Mesure	Modalités	Priorité
Sécurité des applications	Mise en place de procédures pour sécuriser les applications utilisées pour stocker et traiter les données	Haute
Authentification forte	Mise en place de procédures d'authentification fortes pour protéger les comptes utilisateurs	Haute
Mise à jour de sécurité régulière	Mise en place de procédures pour mettre à jour régulièrement les logiciels et les systèmes pour corriger les failles de sécurité connues	Haute

6. Liste des issues à ajouter au sprint 8 pour tenir compte des points les plus importants

- Mettre en place des sauvegardes régulières des données pour limiter les pertes en cas d'incident de sécurité.

- Mettre en place un système de cryptage de bout en bout pour protéger les informations des utilisateurs.

- Mettre en place un mot de passe fort et unique pour chaque compte utilisateur.

- Mettre en place un système pour forcer les utilisateurs à changer régulièrement leur mot de passe et selon les périodes d'inactivités des comptes utilisateurs.

- Limiter les privilèges d'accès aux données en fonction du rôle de l'utilisateur (admin/client).