# Contexte

## Objectifs

La société WellCorp, leader dans la vente de compléments alimentaires et de produits de bien-être, souhaite améliorer son processus de gestion des données clients et l'expérience utilisateur sur son site web et son application mobile.

## Perimètre

WellCorp possède un site web et une application mobile qui permettent aux clients de passer des commandes et de consulter des informations sur les produits et les services proposés. Les clients peuvent également s'inscrire à des programmes de fidélité et de coaching personnalisés. WellCorp compte actuellement environ 500 employés répartis sur plusieurs sites, y compris un siège social, des centres de recherche et développement, des centres de distribution et des bureaux de vente régionaux.

## Organisation interne

L'organisation interne de WellCorp est structurée autour de plusieurs départements, dont la direction générale, le marketing et la communication, la recherche et développement, la production, la logistique, les ventes et le support client. Chaque département est dirigé par un responsable expérimenté et compte plusieurs équipes fonctionnelles.

## Culture d'entreprise

La culture d'entreprise de WellCorp est axée sur l'innovation, la collaboration et l'amélioration continue. L'entreprise encourage ses employés à partager leurs idées et leurs connaissances et à travailler ensemble pour développer des solutions novatrices. La direction s'engage à fournir un environnement de travail stimulant et gratifiant, où les employés peuvent se développer et réaliser leur potentiel.

## Marché cible

WellCorp cible principalement les consommateurs soucieux de leur santé et de leur bien-être, ainsi que les professionnels de la santé, tels que les médecins, les nutritionnistes et les entraîneurs sportifs. Les produits et services de l'entreprise sont conçus pour répondre aux besoins spécifiques de ces segments de marché en termes de qualité, d'efficacité et de facilité d'utilisation.

## Stratégie de croissance

La stratégie de croissance de WellCorp repose sur le développement de nouveaux produits et services, l'expansion géographique et les partenariats stratégiques. L'entreprise investit de manière significative dans la recherche et le développement pour identifier les tendances émergentes et les opportunités de marché. De plus, WellCorp cherche à établir des partenariats avec d'autres entreprises et organisations du secteur de la santé et du bien-être pour renforcer sa présence sur le marché et accroître sa part de marché.

## Défis et opportunités

Parmi les défis auxquels WellCorp est confrontée, on peut citer la concurrence croissante sur le marché de la santé et du bien-être, la régulation des produits et services de santé, et la protection des données personnelles des clients. Par ailleurs, l'entreprise doit également faire face à des attentes élevées en matière de responsabilité sociale et environnementale. Cependant, WellCorp a également de nombreuses opportunités de croissance grâce à l'adoption croissante de modes de vie sains, à l'innovation technologique et aux nouvelles tendances en matière de santé et de bien-être.

# Données à caractères personnels traitées

Les données à caractère personnel (DCP) collectées par WellCorp sont les suivantes :

**a. Pour les clients :**

- Nom et prénom
- Adresse postale
- Adresse e-mail
- Date de naissance
- Sexe
- Mot de passe
- Taille, poids
- Niveau d'activité physique
- Objectifs de santé et bien-être
- Préférences alimentaires (allergies, régimes spécifiques)
- Données synchronisées avec d'autres dispositifs (données de localisation, données de santé, fréquence cardiaque, nombre de pas, etc.)

**b. Pour les employés :**

- Noms, adresses
- Numéros de sécurité sociale
- Informations bancaires
- Antécédents professionnels

**c. Autres données collectées :**

- Données de localisation
- Historique de commandes
- Interactions avec le service client
- Données des représentants des fournisseurs et partenaires (nom, e-mail, téléphone)

Ces données sont traitées via plusieurs systèmes : le CRM pour la gestion client, les systèmes RH pour les employés, ainsi que des systèmes de reporting pour analyser les comportements.

## Mesures de sécurité implémentées

La société a implémenté les mesures de sécurité suivantes :

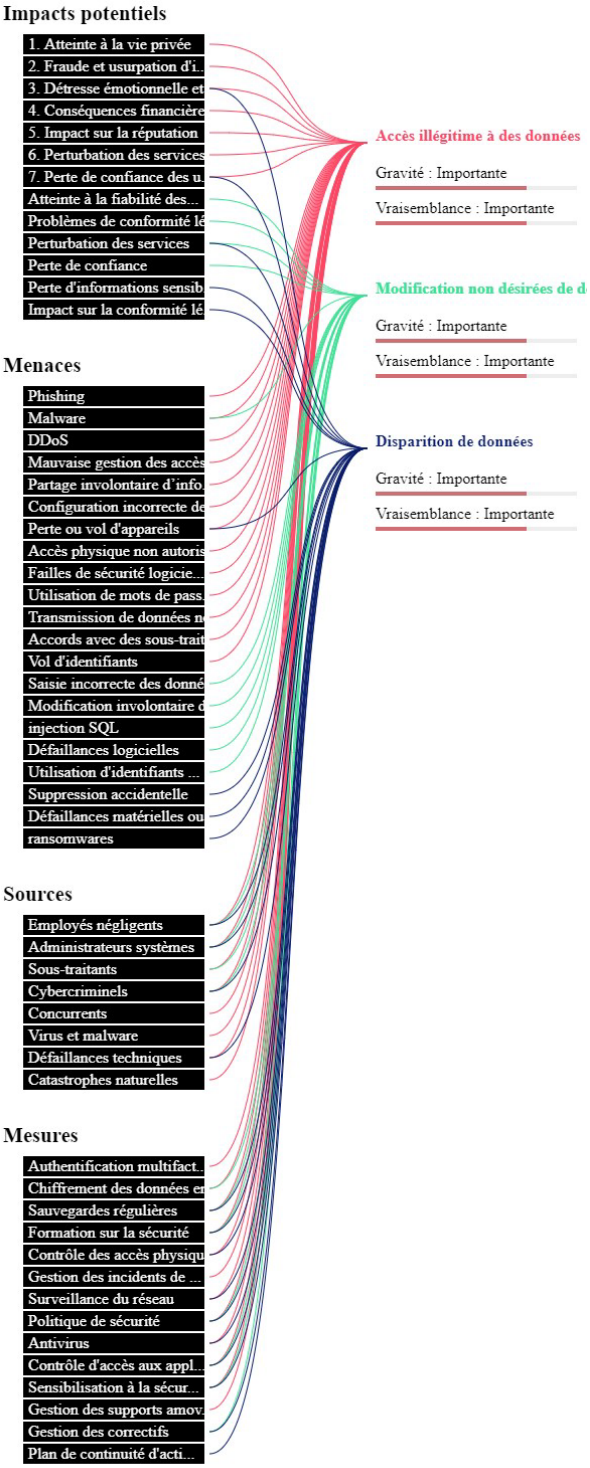
| **Mesure de sécurité** | **Description détaillée** |
|---|---|
| 1. Pare-feu | Installation de pare-feu matériels et logiciels pour filtrer le trafic entrant et sortant et bloquer les connexions non autorisées. |
| 2. Antivirus | Installation d'antivirus sur tous les postes de travail et serveurs, avec mises à jour automatiques des définitions de virus. |
| 3.Authentification multifacteurs | Utilisation d'un mot de passe et d'un code de vérification unique envoyé par SMS ou via une application d'authentification pour accéder au réseau. |
| 4. Chiffrement des données en transit | Utilisation de protocoles sécurisés (comme SSL/TLS) pour chiffrer les données personnelles lors de leur transfert entre les systèmes. |
| 5. Sauvegardes régulières | Sauvegarde quotidienne des données sur des disques durs externes stockés hors site pour permettre la récupération en cas de perte ou de corruption de données. |
| 6. Formation sur la sécurité | Organisation de sessions de formation annuelles pour les employés, abordant les politiques et protocoles de sécurité, |

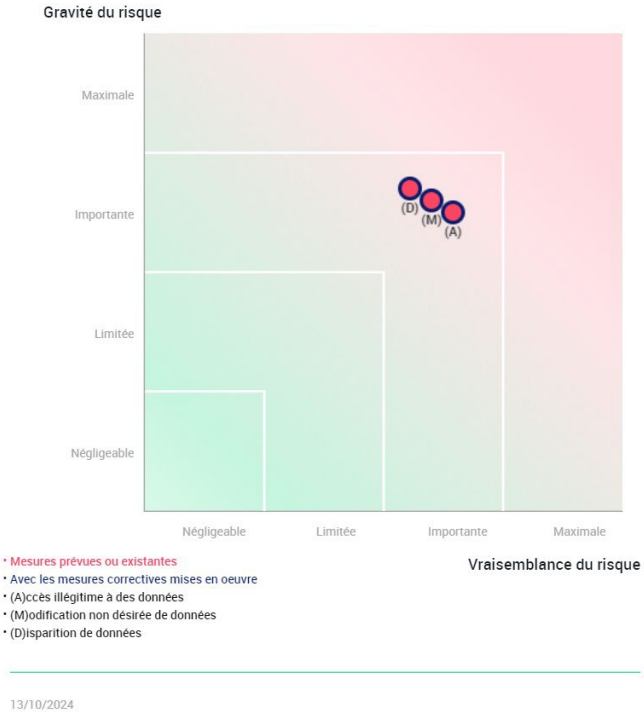
| | |
|---|---|
| | ainsi que les menaces et les bonnes pratiques en matière de cybersécurité. |
| 7. Gestion des incidents de sécurité | Mise en place d'un processus de signalement des incidents de sécurité, avec une équipe dédiée pour enquêter et résoudre les incidents. |
| 8. Contrôle des accès physiques | Utilisation de badges d'accès et de caméras de surveillance pour contrôler l'accès aux bureaux et aux zones sensibles, tel que les salles des serveurs. |
| 9. Mots de passe complexes | Exigence de mots de passe d'au moins 12 caractères comprenant des lettres majuscules et minuscules, des chiffres et des symboles, avec renouvellement tous les 6 mois. |
| 10. Mise à jour des logiciels | Mise à jour régulière des logiciels et des systèmes d'exploitation pour corriger les vulnérabilités, avec notifications automatiques et planification des mises à jour. |
| 11. Gestion des supports amovibles | Restrictions sur l'utilisation de supports amovibles (clés USB, disques durs externes), avec accès contrôlé et suivi des utilisations. |
| 12. Plan de continuité d'activité (PCA) | Établissement d'un PCA pour assurer le maintien ou la reprise rapide des activités en cas d'incident majeur, avec des exercices de simulation annuels. |

| | |
|---|---|
| 13. Gestion des équipements mobiles | Mise en place de politiques de sécurité spécifiques pour les équipements mobiles (smartphones, tablettes), incluant le chiffrement et la gestion à distance. |
| 14. Politique de sécurité | Rédaction et mise à jour d'une politique de sécurité détaillée, avec diffusion auprès de tous les employés et partenaires. |
| 15. Surveillance du réseau | Utilisation d'outils de surveillance pour détecter les anomalies et les intrusions sur le réseau, avec alertes en temps réel. |
| 16. Contrôle d'accès aux applications | Mise en place de contrôles d'accès granulaires aux applications, basés sur les rôles et les responsabilités des utilisateurs. |
| 17. Gestion des correctifs | Application régulière de correctifs de sécurité pour les logiciels et les systèmes d'exploitation, avec un suivi des correctifs appliqués. |
| 18. Segmentation du réseau | Division du réseau en segments distincts pour limiter l'accès aux ressources sensibles et réduire les risques de compromission de l'ensemble du réseau. |
| 19. Sensibilisation à la sécurité | Mise en place d'une campagne de sensibilisation à la sécurité, incluant des affiches, des bulletins d'information et des sessions de formation pour promouvoir les bonnes pratiques. |

# Analyse d’impact relative à la protection des données

## Cartographie des risques




Les mesures de sécurités en place ne suffisent pas à valider le traitement des données chez Wellcorp à l’heure actuelle.

Cependant la direction en est pleinement consciente et la mise en en œuvre des mesures prévues dans le plan de traitement suivant permettra de se mettre en conformité et assurer pleinement la protection des données.

## Plan de traitement

| Principe fondamental | Plan d'action / Mesures correctives | Date prévue de mise en œuvre | Responsable de la mise en œuvre |
|---|---|---|---|
| **Finalités** | Mettre en place une politique de rétention des données : Fixer des limites claires pour la conservation des données personnelles selon leur utilisation. | 12/09/2024 | Équipe de gestion des données clients |
| **Fondement** | 1. Mettre en place une politique de rétention des données.<br>2. Audit des pratiques des fournisseurs : Renégocier les contrats avec des clauses de protection des données et planifier des audits réguliers. | 12/09/2024 | Directeur commercial |
| **Données adéquates** | Recueillir le consentement explicite des utilisateurs pour les données marketing. | 12/09/2024 | Équipe de ventes et de marketing |
| **Données exactes** | 1. Mise à jour régulière des données : Faciliter l'accès et la correction des données par les utilisateurs.<br>2. Vérification des consentements : Processus régulier de vérification des | 12/09/2024 | Équipe de gestion des données clients |

| | | | |
|---|---|---|---|
| | consentements pour garantir leur pertinence.<br>3. Validation des données avant utilisation : Utilisation de contrôles automatisés pour garantir l'exactitude et la cohérence des données.<br>4. Formation spécifique sur la qualité des données pour les employés. | | |
| **Durée de conservation** | Mettre en place une politique de rétention des données : Fixer des limites claires pour la conservation des données personnelles selon leur utilisation. | 12/09/2024 | Équipe de gestion des données clients |
| **Information des personnes** | Mettre en place un processus continu pour maintenir les utilisateurs informés des changements dans le traitement de leurs données, y compris les mises à jour ou modifications de politiques. | 12/09/2024 | Service client |
| **Recueil du consentement** | 1. Mettre en place un processus pour obtenir le consentement explicite des utilisateurs pour les communications marketing.<br>2. Mettre en place un | 12/09/2024 | Équipe de ventes et de marketing |

| | | | |
|---|---|---|---|
| | processus de désinscription ou de modification des préférences pour les utilisateurs (option de retrait). | | |
| **Droit d'accès et à la portabilité** | Définir un processus. | 12/09/2024 | Équipe informatique et sécurité |
| **Droit de rectification et d'effacement** | Définir un processus. | 12/09/2024 | Équipe informatique et sécurité |
| **Droit de limitation et d'opposition** | Définir un processus. | 12/09/2024 | Équipe informatique et sécurité |
| **Sous-traitance** | Définir et contractualiser les obligations des sous-traitants. | | Directeur commercial |
| **Transferts** | S'assurer que les données soient protégées de manière équivalente si transfert en dehors de l'UE il y a. | | Équipe informatique et sécurité |