



PROTECTION DES DONNÉES PRIVÉES EN ENTREPRISE

Travail d'éthique

02 JUIN 2024
CORENTIN D'HAEYERE
Haute Ecole Léonard de Vinci

Table des matières

Introduction	1
Développement – Utilisation du paradigme libéral	1
Types de données collectées	1
Obligations et mesures appliquées	2
Mesures actuelles.....	2
Pistes d'amélioration.....	2
Conclusion	3
Bibliographie.....	4

Introduction

La protection des données privées est devenue super importante dans le monde numérique d'aujourd'hui. Chaque jour, des quantités massives de données personnelles sont collectées, utilisées et gérées par diverses organisations, soulevant des questions éthiques cruciales. Cette problématique est particulièrement pertinente dans le milieu professionnel, où les données des utilisateurs sont au cœur des processus décisionnels et opérationnels. Prenons l'exemple d'une étude de marché, on utilise les habitudes de consommation des clients afin de définir si on a une possibilité de se développer sur un certain marché.

Lors de mon stage de quatre mois chez Eachstapp, j'ai pu observer les défis et les responsabilités liés à la gestion des données. Eachstapp développe des solutions numériques qui aident les utilisateurs à intégrer plus efficacement le numérique dans leur quotidien. Ils collectent et traitent donc aussi des données, ce qui rend nécessaire la réflexion sur la protection de celle-ci.

À travers ce travail, j'utiliserai le paradigme libéral pour explorer les types de données collectées par Eachstapp, les obligations légales et morales auxquelles l'entreprise doit se conformer, ainsi que les mesures de protection en place. En mettant l'accent sur la liberté individuelle et le consentement éclairé, nous examinerons les meilleures pratiques et les pistes d'amélioration pour garantir une gestion éthique et sécurisée des données personnelles des utilisateurs. Mon analyse vise à offrir une compréhension nuancée des enjeux de la protection des données et à proposer des solutions concrètes pour renforcer la confiance des utilisateurs dans le respect de leur vie privée.

Développement – Utilisation du paradigme libéral

Types de données collectées

Chez Eachstapp, on collecte des infos sur nos utilisateurs, comme leurs noms, adresses e-mail, numéros de téléphone et même leur date de naissance ou des documents officiels pour s'assurer de leur identité. On a aussi des données sur ce qu'ils font sur l'appli, comme ce qu'ils regardent ou cliquent. Ça nous aide à rendre l'appli meilleure en comprenant ce que les gens préfèrent. Par exemple, si beaucoup de gens vont souvent sur une page, on va la rendre encore plus cool pour eux.

Obligations et mesures appliquées

Conformément au Règlement Général sur la Protection des Données (RGPD), Eachstapp est tenue à plusieurs obligations pour assurer la protection des données personnelles des utilisateurs. Nous obtenons le consentement explicite de nos utilisateurs avant de collecter leurs données. Par exemple, lors de la création d'un compte utilisateur, une case à cocher doit être présente pour que ce dernier accepte explicitement l'utilisation de ses informations. Il est également crucial de mettre en œuvre des mesures de sécurité adéquates pour protéger les données contre les accès non autorisés, telles que l'utilisation d'un chiffrement des données. Eachstapp a l'obligation d'informer les utilisateurs sur l'usage qui sera fait de leurs données, ce qui inclut la publication d'une politique de confidentialité claire et facilement accessible. Elle est généralement disponible lors de l'onboarding d'un utilisateur ou dans un menu « Paramètres » de l'application. Nous laissons la possibilité à nos utilisateurs de supprimer leurs données via un formulaire présent dans l'application. En fonction de la demande du client, les données sont supprimées tout de suite ou 30j après la demande afin de permettre une réactivation du compte.

Mesures actuelles

Actuellement, les données des utilisateurs sont conservées dans une base de données sécurisée, bien que l'accès à ces données ne soit pas toujours restreint aux seules personnes nécessaires. Par exemple, il est possible que certains employés aient accès à des informations non pertinentes pour leur rôle. Eachstapp utilise des mots de passe robustes et l'authentification à deux facteurs pour sécuriser l'accès à ces systèmes. Cependant, il n'existe pas de politique claire concernant la gestion des accès et leur révocation lors du départ d'un employé, ce qui peut laisser des failles potentielles pour des accès non autorisés.

Ces pratiques révèlent des lacunes en matière de protection des données, notamment sur la gestion des accès.

Pistes d'amélioration

Pour renforcer la protection des données, Eachstapp pourrait envisager l'utilisation d'une plateforme dédiée et sécurisée pour le stockage des données, permettant un contrôle strict des accès et la révocation automatique des droits en cas de départ d'un employé. Par exemple, un logiciel de gestion des identités et des accès (IAM) pourrait être utilisé pour automatiser et sécuriser la gestion des droits d'accès. Enfin, il est essentiel d'élaborer une politique claire de gestion des accès aux données, avec des procédures pour révoquer les accès lors de changements de rôle ou de départ. Actuellement tous les accès aux données sont gérés manuellement par les différents employés de l'entreprise. Il n'y a pas vraiment de personne référente en cas de besoin d'un accès à un certain service ou base de données.

Conclusion

En adoptant le paradigme libéral, ce travail m'a indiqué l'importance de la protection des données dans un contexte professionnel, en particulier dans l'entreprise où j'étais. La liberté individuelle, le consentement éclairé et la responsabilité sont des principes fondamentaux qui guident les pratiques de gestion des données personnelles. Eachstapp s'efforce de respecter la vie privée des utilisateurs en obtenant leur consentement explicite et en leur fournissant des informations claires sur l'utilisation de leurs données. De plus, l'entreprise met en place des mesures de sécurité robustes pour protéger les données contre les accès non autorisés.

Cependant, malgré les efforts déjà entrepris, des améliorations sont nécessaires pour renforcer davantage la protection des données. L'utilisation de plateformes sécurisées pour le stockage des données, l'élaboration de politiques de gestion des accès plus strictes et la mise en place de formations régulières et détaillées sont des mesures essentielles. En adoptant ces pratiques, Eachstapp peut non seulement se conformer aux exigences légales, mais aussi renforcer la confiance de ses utilisateurs, assurant ainsi un environnement numérique sûr et fiable.

En conclusion, la gestion éthique des données privées, guidée par les principes libéraux, est indispensable pour garantir le respect des droits individuels et la responsabilité des entreprises. Une recherche internet, la consultation de ses comptes, un achat en magasin avec une carte bancaire ou une simple photo publiée sur les réseaux sociaux : tel le Petit Poucet qui sème des cailloux, chacun s'expose à des risques car ce se sont autant de données que nous produisons et qui sont exposées, exploitées, voire détournées. Les risques de traçage abusifs, les virus, usurpation d'identité et tentatives d'escroquerie fleurissent à l'ère d'une société qualifiée de "numérique" .

En prenant des mesures concrètes pour améliorer la sécurité et la transparence, Eachstapp peut établir une relation de confiance avec ses utilisateurs et contribuer à un développement durable et éthique de l'entreprise. Pour approfondir ces aspects, le livre La protection des données personnelles par Laurane Raimondo offre des perspectives et des recommandations précieuses pour naviguer dans le paysage complexe de la gestion des données personnelles.

Bibliographie

- OpenAI (2024) ChatGPT, 30 mai. URL : <https://chat.openai.com/>
- CNIL. (2024). Le Règlement général sur la protection des données (RGPD). URL : <https://www.cnil.fr/fr/rgpd-par-ou-commencer>
- ENISA. (2022). Guidelines on Data Protection by Design and by Default. URL : <https://www.enisa.europa.eu/publications/guidelines-on-data-protection-by-design-and-by-default>
- European Commission. (2023). Data Protection Rules as a Trust Enabler in the EU and Beyond. URL : https://ec.europa.eu/info/law/law-topic/data-protection_en
- OWASP Foundation. (2024). OWASP Top Ten Web Application Security Risks. URL : <https://owasp.org/www-project-top-ten/>
- Raimondo L (2021) La protection des données personnelles, Paris, Ellipses