TP- PRA & RGPD

Contexte

Nous sommes le 10/03/2021 et vous venez d'être missionnés par Permabook pour :

- Gérer l'exploitation de leur site d'achat en ligne configuré sous Wordpress et hébergé chez OVH. Malheureusement, vous ne pourrez pas bénéficier de transfert de compétences puisque le développeur a fait un abandon de poste.

- Mettre en conformité RGPD le site d'achat en ligne.

M. Pouget souhaite que le site soit le plus transparent possible en ce qui concerne le traitement des données personnelles de ses utilisateurs. Il considère que la mise en conformité au RGPD peut être une chance dans sa communication vis-à-vis de ses clients et, plus globalement, pour la notoriété de sa librairie.

Afin de respecter le principe de minimisation des données du RGPD, il est nécessaire de traiter le moins de données possibles. La question des sous-traitants de la librairie pose problème : M. Pouget vous demande de travailler sur les données personnelles collectées par ces sous-traitants et de donner des éléments permettant de savoir s'il est nécessaire de faire appel à ces entreprises ou s'il est préférable de faire autrement.

Dans un premier temps, vous prévoyez de parcourir le site internet pour vous familiariser avec Permabook et faire un premier état des lieux de sa conformité RGPD.

Complications

Malheureusement, vous n'avez pas eu le temps de prendre en main le site internet et de vérifier l'ensemble des éléments d'exploitation en place car un incendie a ravagé un des datacenters d'OVH, dans lequel était hébergé le site de Permabook. Le site de Permabook n'est plus disponible en ligne.

Les priorités de votre mission viennent d'être revues : il faut impérativement relancer le site internet au plus vite en appliquant la procédure de reprise d'activité si elle existe (si elle n'existe pas, il faudra la créer et l'appliquer tout de suite)

Objectifs & Description des réalisations attendues

Partie 1 - PRA & Gestion de l'incident de sécurité :

- Ne pas oublier d'avertir la CNIL de l'incident de sécurité s'il y a lieu (argumenter, expliquer la démarche à suivre et les informations à transmettre si besoin).
- Rédiger une procédure de reprise d'activité
- Réinstaller le site Permabook : Dans un premier temps, vous installerez le site permabook sur une VM locale qui pourra ensuite être exportée ou transférée.
- Vérifier que le site est à nouveau opérationnel localement.
- Faites un CR état des lieux au dirigeant de Permabook avec un plan d'action si besoin. Ce plan d'action indiquera à minima la nécessité de tester le PRA régulièrement.

Partie 2 - RGPD

Une fois le site local à nouveau en conditions opérationnelles, le travail à faire est détaillé dans le document ci-dessous mais les grandes lignes sont :

- Faite un état des lieux des éléments manquants / à corriger / à produire pour un site internet respectant le RGPD
- Réaliser le registre des traitements de Permabook
- Réaliser une page de politique de confidentialité
- Recenser les formulaires et améliorations possible
- Solution en matière de cookies
- Définir s'il y a lieu de réaliser une PIA
- Réaliser une PIA

Ressources

- Fichier permabook.zip contenant la dernière sauvegarde du site internet de permabook
- Fichier permabook.sql contenant la dernière sauvegarde de la BDD du site de permabook
- Quelques bribes et mots-clés retrouvés sur le poste de travail du développeur après son départ. Ces éléments ont été retranscrits dans un fichier « install_permabook.txt »