BUT 2

Thème 1 Droit des Données et Protection de la Vie Privée

TD2 Mise en conformité Site WEB RGPD

TD2 MISE EN CONFORMITE NIVEAU 1 DU SITE WEB AU RGPD[1]

Contexte

Vous travaillez **pour le compte d'une entreprise de services du numérique (ESN)** qui apporte son expertise auprès de ses clients en matière de conformité au règlement européen relatif à la protection des données personnelles. Vous êtes jeune embauché(e) au sein du service informatique.

Vous participez, avec votre collègue **d**élégué à la **p**rotection des **d**onnées (DPD, ou DPO pour Data Protection Officer) à différentes **prestations de mise en conformité du règlement général pour la protection des données (RGPD) pour vos entreprises clientes**.

Votre travail consiste à accompagner la **librairie PermaBook** dans la mise en conformité au RGPD de son **site Internet**.

Permabook est un pure player : elle vend exclusivement sur internet. Elle a été créée par M. Loïc Pouget en 2010 pour répondre aux demandes toujours croissantes des lecteurs intéressés par la permaculture et les thèmes connexes.

> **La permaculture est une démarche de conception éthique visant à construire des habitats humains durables en imitant le fonctionnement de la nature.**

En 10 ans, Permabook s'est beaucoup développée. La librairie compte aujourd'hui plus de 15 salariés. Le chiffre d'affaires et le nombre de clients ont eux aussi beaucoup augmenté. Pour faire face à cette croissance inespérée, M. Pouget a décidé de revoir entièrement son site internet. Ses équipes informatiques ont réalisé une première maquette accessible à l'adresse suivante : http://permabook.si24.fr.

M. Pouget fait appel à vous car ses équipes ont besoin de soutien pour la mise en conformité du site au RGPD. Il considère pourtant que c'est un point crucial dans son activité : à la fois contrainte à respecter absolument et opportunité de mettre en avant l'éthique que son entreprise porte depuis le début.

Site internet

Le site de PermaBook est accessible à l'adresse http://permabook.si24.fr.

Il a été développé avec Wordpress, CMS le plus utilisé dans le monde aujourd'hui. Pour le moment, peu de fonctionnalités ont été ajoutées.

[1] Ce travail est tiré d'une ressource mise à disposition par le réseau Certa ; auteur Yann Barrot.

Voici les extensions (plug-ins) installées (mais pas forcément activées) :

- woocommerce : transforme le CMS en site de vente en ligne ;
- caldera forms : permet de créer des formulaires personnalisés ;
- slimstat Analytics : statistiques de trafic et d'utilisation du site ;
- mailchimp for woocommerce : fournisseur externe de solution de marketing par courriel (newsletter) ;
- Google Ads pour Woocommerce : permet de lier le système publicitaire de Google à un site de vente utilisant woocommerce.

Seules les quatre premières extensions sont réellement utilisées. La dernière est pour le moment en évaluation.

MISSION

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.

Organisation du travail

Vous travaillerez par groupe de 3/4 étudiants. Vous pourrez vous répartir les travaux -1 à 5) à réaliser mais vous constituerez un seul dossier documentaire.

❖ **Dossier documentaire à rendre**

1. Registre des traitements
2. Page de politique de confidentialité
3. Recensement des formulaires et des améliorations possibles
4. Solution en matière de gestion des cookies
5. Tutoriel sur la gestion des données utilisateurs dans Wordpress

Ressources

- Fiche méthode 1 : Démarche de conformité au RGPD

- Site web http://permabook.si24.fr
- > Ressources
  - > Kit RGPD
    - documents internes
      - **modèle de registre des traitements**
    - communication externe :
      - **modèle de page de confidentialité**
  - R_Mission 1 : liste des cookies du site

SOMMAIRE

I Registre interne de traitement des données

Travail à faire 1 Vous êtes chargés de compléter le registre des traitements correspondant aux activités de vente en ligne de Permabook.

1. Repérer l'ensemble des traitements de données personnelles. Compléter la feuille « liste des traitements » du registre.
2. Pour chaque traitement identifié, créer et compléter une fiche de registre en identifiant l'ensemble de données personnelles collectées.
3. Repérer pour chaque traitement les parties qui ne sont pas totalement en conformité avec le RGPD et proposer des améliorations.

Exemple : site:woocommerce.com GDPR.

Ressources : kit RGPD > modèle de registre de traitement simplifié

II Droits à l'information

Page politique de confidentialité

La page « Politique de confidentialité » est la page d'un site web qui rassemble les informations sur les traitements de données personnelles.

Elle doit apparaître en pied de page et à chaque fois que des données personnelles sont demandées aux utilisateurs. Le plus simple est de prévoir une case à cocher (non cochée par défaut) qui demande d'indiquer que la politique de confidentialité est acceptée.

Travail à faire 2 Rédiger la page politique de confidentialité du site.

Ressources :

- kit RGPD > Modèle de page « politique de confidentialité »

III Recueil du consentement sur les formulaires

Les formulaires sont un point de passage privilégié pour la collecte volontaire de données personnelles.

Ils doivent respecter les principes fondamentaux du RGPD et en particulier minimiser les données collectées.

La transparence devrait s'exercer de deux façons :

- dans le formulaire lui-même :
  - il s'agit de faire clairement apparaître les données indispensables et celles qui ne le sont pas ;
  - il faut aussi donner les raisons de la collectes des données non essentielles ;
- en informant dans une page dédiée à la politique de confidentialité.

Idéalement, un formulaire collectant des données personnelles devrait donc comporter 2 cases à cocher au moins (non cochées par défaut) :

- une validant la collecte des informations contenues dans le formulaire lui-même ;
- une autre pour valider le fait que l'utilisateur est d'accord avec la politique de confidentialité décrite sur une page dédiée.

Travail à faire 3 Recenser tous les formulaires présents sur le site et repérer les améliorations possibles.

Vous ferez en particulier attention aux formulaires qui concernent :

- la création de compte sur le site ;
- le processus de commande ;
- les commentaires ou les avis ;
- l'inscription à des newsletters.

IV Gestion des cookies

Les cookies sont des fichiers texte qui permettent de conserver des traces du comportement des visiteurs.

Certains cookies sont indispensables au bon fonctionnement des sites : c'est le cas par exemple des cookies permettant de se souvenir du contenu du panier du client. D'autres sont créés pour d'autres raisons par le site lui-même ou par des tiers : il s'agit le plus souvent de suivre le comportement du consommateur pour monétiser la publicité ou pour la rendre plus efficace.

Travail à faire 4 Proposer une solution pour informer correctement les visiteurs sur l'utilisation des cookies.

1. Sur la base du recensement des cookies (dossier ressources), identifier les différentes catégories de cookies déjà présents sur le site.
2. Trouver une extension permettant d'informer correctement les utilisateurs.

Ressources

- CNIL
  - https://www.cnil.fr/fr/cookies-et-autres-traceurs
  - https://www.cnil.fr/fr/cookies-et-traceurs-comment-mettre-mon-site-web-en-conformite
-
- > Ressources > R_Mission1
  - rapport d'analyse cookiebot : RapportCookies-permabooksi24fr-FR-2020-09-22

Remarque : cookiebot est un prestataire en ligne qui peut gérer la conformité d'un site en matière de cookie.

V Exercice des droits : effacement et modifications

Le RGPD prévoit qu'un utilisateur puisse facilement exercer un certain nombre de droits concernant les données qui le concerne : accès, rectification, suppression…

Pour rendre ce processus le plus simple possible, un site web peut prévoir une page dédiée expliquant comment exercer ces droits et renvoyant vers un mail spécifique.

Concernant Permabook, l'administrateur du site devra être capable de proposer aux utilisateurs :

- l'accès à leurs données ;
- la modification et la suppression de ces données ;
- la portabilité des données.

Travail à faire 5 Créer un tutoriel à destination du webmaster de Permabook expliquant comment réaliser ces opérations de façon simple dans Wordpress.