

Mise en conformité au RGPD d'un site de vente en ligne

Propriétés	Description
Intitulé long	Mise en conformité au RGPD du site internet d'une librairie en ligne fictive : Permabook.
Formation(s) concernée(s)	BTS Services Informatiques aux Organisations
Matière(s)	Bloc 3 SISR – Cybersécurité des services informatiques
Présentation	Ce TP demande aux étudiants de travailler en groupe sur la mise en conformité au RGPD du site internet d'une librairie en ligne fourni avec le TP. La mission 1 porte sur une mise en conformité minimale, qui pourrait concerner tout site web. La mission 2 suppose que ce site traite des données sensibles et amène à développer une gestion des risques plus approfondie à travers une AIPD (analyse d'impact relative à la protection des données personnelles) à l'aide du logiciel spécifique mis à disposition par la CNIL (PIA). Le TP vient avec un ensemble de ressources : fiches savoirs, fiche méthode, dont l'intérêt peut dépasser le TP lui-même et des ressources spécifiques au TP.
Savoirs	Les données à caractère personnel : définition, réglementation, rôle de la CNIL Typologie des risques et leurs impacts. Sécurité et sûreté : périmètre respectif. Principes de la sécurité : disponibilité, intégrité, confidentialité, preuve.
Compétences	<ul style="list-style-type: none">• Recenser les traitements sur les données à caractère personnel au sein de l'organisation• Identifier les risques liés à la collecte, au traitement, au stockage et à la diffusion des données à caractère personnel• Appliquer la réglementation en matière de collecte, de traitement et de conservation des données à caractère personnel• Sensibiliser les utilisateurs à la protection des données à caractère personnel
Prérequis	Notions de base sur le RGPD.
Mots-clés	RGPD, données personnelles, données sensibles, sécurité des données, AIPD, gestion des risques

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 **délégué à la protection des données (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.

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.

Voici la liste des comptes créés à des fins de tests [les mots de passe vous seront remis ultérieurement] :

- Admin ;
- gestioncom : gestionnaire de boutique ;
- deux clients : Jean Neymar et Agathe Zeblouz.

Missions

M. Pouget souhaite que vous travailliez sur la mission suivante :

- **Mission 1** : assurer la conformité « niveau 1 » du site web au RGPD ;

1 - Lister les éléments de correction du site web <http://permabook.si24.fr>

2 - Donner le Contenu de la page de confidentialité

3 - Vérifier la conformité du traitement des formulaires

Ressources

- Ressources du cours :
 - Fiche savoir 0 MOOC RGPD de la CNIL (copies d'écran)
 - Fiche savoir 1 Traitement des données à caractère personnel v1.1
 - Fiche savoir 2 Sécurité vs sûreté, c'est l'intention qui compte
 - Fiche savoir 3 Principes de sécurité des données
 - Fiche savoir 4 Gérer les risques portant sur les données personnelles
 - Fiche méthode 1 Démarche de conformité au RGPD
- Ressources du TP
 - kit RGPD
 - un dossier par mission
- Ressources liées au contexte :
 - site web <http://permabook.si24.fr> (DEMO)