Mise en conformité d'un site web avec les exigences du RGPD

Compte-rendu d'activité

Sommaire

1. Introduction

Ce compte-rendu fait la synthèse d'une séance de travaux pratiques réalisée en première année de BTS. Le contexte est le suivant : dans le cadre de l'audit du site internet d'une entreprise, développé à l'aide d'un CMS, certains manquements aux obligations légales du RGPD ont été remarqués. Notre mission est de participer au projet de mise en conformité du site, notamment par la refonte de ses formulaires.

2. Mission

L'application à traiter est un site web développé avec Joomla. La mission est composée de cinq tâches :

- supprimer les champs correspondant à des données facultatives,
- ajouter les éléments nécessaires au recueil de consentement de la personne au traitement (case à cocher et raison de la collecte des données),
- ajouter les éléments permettant aux utilisateurs de retirer leur consentement,
- donner la possibilité aux utilisateurs d'appliquer leurs droits d'accès, de modification ou de suppression de leurs données,
- recueillir le consentement des utilisateurs en matière de cookies.

3. Réalisation

Tâche 1 – Suppression des champs correspondant à des données facultatives

Le RGPD impose qu'une organisation ne collecte que le minimum de données nécessaires à la finalité, c'est-à-dire à l'objectif immédiatement poursuivi. Ce principe de minimisation des données recueillies implique une réflexion sur les champs réellement nécessaires.

Sur le formulaire du site du client, les champs suivants n'avaient pas de raison d'être et ont été supprimés :

- Le sexe, qui n'est pas pertinent pour l'inscription au site,
- L'âge, qui n'a pas besoin d'être précis et peut être remplacé par une case à cocher pour vérifier que la personne est majeure,
- La date de naissance, qui fait doublon avec le précédent, et encore une fois est une donnée trop précise pour l'utilisation qui sera faite des données.

Tâche 2 – Ajout des éléments nécessaires au recueil du consentement

L'un des principes du RGPD est le consentement éclairé. L'utilisateur d'un site web doit pouvoir consentir sans ambiguïté à l'utilisation prévue pour ses données. Les formulaires de contact, qui nécessitent la conservation d'une adresse mail à laquelle l'organisation pourra répondre, doivent donc comporter une case à cocher pour obtenir l'autorisation expresse de l'utilisateur.

Le formulaire de contact mis en place sur le site du client ne possédant pas cette case, elle a été ajoutée. Elle est décochée par défaut, puisque le consentement ne peut être obtenu que par une action positive de l'utilisateur : celui-ci doit accomplir un geste conscient pour que le recueil du consentement soit valable.

Le consentement doit ensuite être conservé. L'information de la case cochée, ainsi que les données permettant d'identifier l'utilisateur, sont stockés par Joomla. Un onglet permet de consulter la liste des consentements recueillis.

Tâche 3 – Ajout des éléments permettant de retirer son consentement

À tout moment, un utilisateur doit avoir la possibilité de retirer son consentement, si le motif de sa demande n'est pas contraire aux intérêts légitimes de l'organisation (par exemple l'exécution d'un contrat à la demande de l'utilisateur).

Dans la tâche précédente, l'utilisateur a pu donner son consentement lui-même, lors de l'utilisation du formulaire de contact. Cependant, il ne possède pas de compte, et ne peut donc pas s'identifier et s'authentifier sur le site. Pour cette raison, il est impossible de mettre en place un formulaire lui permettant de retirer son consentement, car son identité ne peut être prouvée. À la place, on a créé un nouveau formulaire permettant à l'utilisateur de demander explicitement la suppression de son consentement.

Tâche 4 – Ajout de la possibilité pour les utilisateurs d'appliquer leurs droits d'accès, de modification ou de suppression de leurs données

Avant la mise en place du RGPD, la législation française prévoyait déjà des droits spécifiques pour les utilisateurs quant au traitement de leurs données personnelles (toute donnée permettant d'identifier une personne directement ou indirectement). Le RGPD renforce ces droits, dans un contexte où ces données augmentent en volume et représentent une richesse considérable pour les entreprises. L'utilisateur doit ainsi être informé clairement des données qui seront recueillies, du traitement qui en sera fait et par qui, de la durée de leur conservation, et s'il est prévu de les transférer vers un pays tiers, le cas échéant.

L'utilisateur a également des droits, dont il doit être informé : droit, à tout moment, de consulter les données recueillies à son sujet, de les rectifier si elles sont incorrectes ou incomplètes, d'en obtenir une copie dans un format exploitable, voire de les supprimer dans certains cas.

Sur le site du client, de nouveaux formulaires ont donc été mis en place pour que les utilisateurs puissent exercer ces droits.

Tâche 5 – Consentement des utilisateurs en matière de cookies

Pris isolément, les cookies ne contiennent que des informations anonymes de connexion et de navigation sur des sites. Cependant, par recoupement avec d'autres données, ils peuvent mener à l'identification d'une personne. À ce titre, on doit donc les considérer comme des données personnelles, et les mêmes règles s'appliquent : les cookies ne doivent être conservés que dans un objectif spécifique, pour un temps limité, et en toute transparence.

Pour utiliser les cookies dans le respect du RGPD, il faut :

- Indiquer quels cookies sont utilisés et à quelle catégorie ils appartiennent,
- Décrire l'utilisation qui en est faite,
- Permettre aux utilisateurs de donner leur consentement indépendamment pour chaque cookie,
- Déployer les cookies non essentiels au fonctionnement du site seulement une fois que l'utilisateur a donné son consentement,
- Permettre aux utilisateurs de modifier à tout moment leurs préférences en matière de cookies,
- Respecter les préférences et consentements des utilisateurs en les conservant le temps nécessaire.

Concrètement, trois éléments ont été mis en place sur le site du client :

- La bannière de recueil de consentement, affichée lors du premier accès au site,
- La page « Politique en matière de cookies », accessible depuis le *footer* du site, qui liste notamment les cookies, l'utilisation qui en est faite et les droits des utilisateurs,
- La gestion de la conservation des préférences et consentements des utilisateurs.

Pour la bannière de recueil de consentements, il existe des extensions Joomla comme EU e-Privacy Directive, qui permettent de mettre en place facilement un système de choix de cookies granulaire.

La page « Politique en matière de cookies » doit mentionner tous les cookies utilisés sur le site, par catégorie : cookies essentiels, cookies liés aux performances et fonctionnalités, cookies d'analyse, cookies publicitaires et cookies de réseaux sociaux.

Quant à la conservation des préférences et consentements des utilisateurs, elle peut aussi être réalisée directement par Joomla et l'extension EU e-Privacy Directive ou autre extension similaire.