RAPPORT DE SUIVI D'IMPLEMENTATION DES REGLES RGPD

Maxime Gaultier, Aurian Baudet

I. Tables des matières

II. Introduction

Dans ce Rapport nous allons vous présenter tout le parcours de gestion de projet qui se doit de respecter les règles du RGPD et les règles de la CNIL.

Nous allons en premier temps vous présentez le contexte, puis les différentes étapes du projet.

Nous vous présenterons aussi notre diagramme de GANTT en le décrivant et nous ferons aussi un point sur l'implémentation et la réflexion des règles RGPD et de la CNIL au niveau de notre application.

A. Contexte :

Dans le cadre de la formation DEUST IOSI nous avons été chargés de créer une application web complexe pour le projet multidisciplinaire.

B. L'application :

Pour ce projet, nous devons respecter le cahier des charges qui nous a été fourni. Il s'agit d'une application web de réservation en ligne de séances de cinéma, qui contient un back-office pour les gérants du cinéma et un front-office pour les clients. Il y a des fonctionnalités importantes à implémenter sur l'application, et nous sommes guidés tout au long du projet :

- **Interface de gestion (back-office)** : cette partie du site web sera à destination du responsable du cinéma.
- **Interface pour clients (front-office)** : cette partie du site web sera à destination des clients du cinéma.

Les principales fonctionnalités requises pour les clients (front-office) sont les suivantes :

- **Accès à la programmation des séances** : Pour chaque séance seront indiqués les horaires, le numéro de salle, le descriptif succinct du film, éventuellement accompagné d'une image ou d'une bande annonce.
- **Visualisation des places disponibles** : Pour une séance programmée, un client pourra visualiser le nombre de places disponibles. Il peut être envisagé d'afficher la localisation des places disponibles sur le plan de la salle associée à la séance programmée choisie.
- **Réservation de places** : Pour une séance programmée avec des places réservables, un client pourra indiquer le nombre de places qu'il désire réserver. Il peut être envisagé de proposer le choix des places à partir d'un plan de la salle montrant les places encore disponibles. Un tarif normal et un tarif réduit seront prévus, constants quel que soit le film projeté. En réponse, un numéro de réservation accompagné du nombre de places réservées et du numéro des places seront affichées au client. Le caissier présent à l'entrée pourra ainsi présenter la note à payer.

- **Espace client** : Tout client doit avoir la possibilité de se créer un compte, une fois connecté au site web il doit pouvoir accéder à ses informations personnelles, ses précédentes commandes et un récapitulatif des réservations déjà effectuées pour les séances à venir.

Les principales fonctionnalités requises pour l'interface de gestion (back-office) sont :

- **Compte gestionnaire** : Un compte spécifique sera créé uniquement pour le gestionnaire du cinéma, une fois connecté il doit pouvoir accéder à ses informations personnelles, aux options de configuration du site web et au paramétrage des informations sur le contenu du site web (détaillé ci-après).
- **Programmation des films** : Pour chaque film, il faudra permettre l'ajout de films à l'affiche avec descriptif des films et des séances dans une salle.
- **Liste des réservations** : Pour chaque séance, il faudra pouvoir accéder aux réservations associées.
- **Affichage d'un tableau de bord** : Il faudra proposer une interface présentant de façon synthétique et agréable la recette prévue (en cours) pour chaque film.

Afin de garantir le bon déroulement du projet, nous avons ajouté une large gamme de fonctionnalités à notre application et nous nous sommes organisés en conséquence.

C. Étapes du projet :

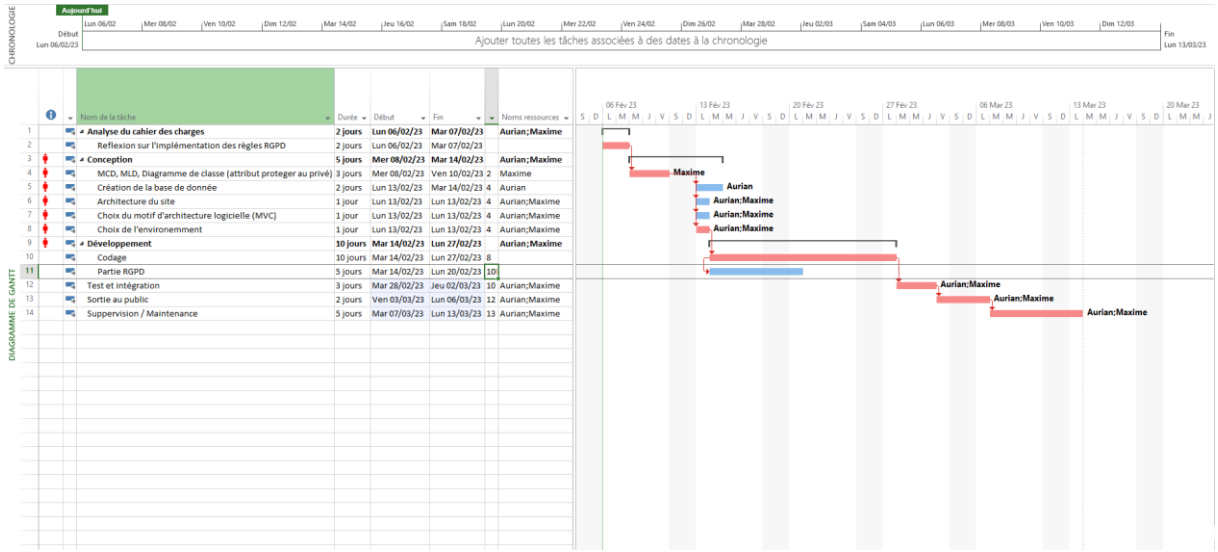
Nous avons donc découpé le projet en une multitude d'étapes :

- Analyse du cahier des charges :
    - Réflexion sur l'implémentation des règles RGPD et de la CNIL
- Conception :
    - MCD, MLD, Diagramme de classe (inclus la réflexion sur les attributs de classe privé ou protéger)
    - Création de la base de données
    - Architecture du site
    - Choix du motif d'architecture logicielle (MVC)
    - Choix de l'environnement (PHP Storm)
- Développement :
    - Codage
    - Partie d'implémentation RGPD et CNIL
- Tests et intégrations
- Mise en production du site
- Supervision et maintenance

Nous avons donc décider de transmettre cette planification en diagramme de GANTT.

D. Planification GANTT :

Nous pouvons voir ci-dessous notre diagramme de GANTT qui a été créé en respectant les étapes du projet énoncé ci-dessus.



Tout d'abord qu'est-ce qu'un diagramme de GANTT ?

Un diagramme de Gantt est un outil pratique pour planifier des projets. Grâce à une vue d'ensemble des tâches planifiées, chaque personne concernée sait quelle activité doit être effectuée et à quelle date précise. Un diagramme de Gantt montre : La date de début et de fin d'un projet

En rouge sur le diagramme vous pouvez voir la route critique qui est le chemin ou les timings doivent être respecter pour ne pas mettre en péril le projet. Nous avons aussi mis 2 ressources qui sont nous-même : Maxime Gaultier et Aurian Baudet, pour se répartir équitablement le travail.

Le diagramme de GANTT est aussi très utile pour garder une trace de qui a fait quoi dans le projet, il nous aide aussi beaucoup pour l'avancement dans la conception du rapport de projet car nous aurons juste à suivre la chronologie pour présenter dans l'ordre l'avancement sur notre projet.

III. Implémentation des règles RGPD et de la CNIL

A. Sécurité des données : migration vers TLS

Le principe lié à la sécurité des données stipule que les responsables du traitement et les sous-traitants doivent mettre en place des mesures afin de garantir un niveau de sécurité adapté au risque.

Ces mesures doivent prendre en compte les risques d'accès non autorisé, de modification, de perte et de divulgation des données à caractère personnel.

Dans le cas de l'utilisation du protocole TLS, cela signifie que les responsables et sous-traitants doivent utiliser un protocole sécurisé (tel que TLS 1.2 ou 1.3) pour s'assurer que leurs données sont sécurisées et chiffrées.

Pour se faire, lors de la configuration du serveur web, il faut générer des certificats via des autorités de certifications (CA) tel que DigiCert, GlobalSign, Let's Encrypt.

Les principes clés du protocole TLS sont les suivants : authentification et cryptage des données, confidentialité des données, intégrité des données, contrôle d'accès et confidentialité des communications. TLS utilise un système de chiffrement asymétrique qui permet de s'authentifier et de sécuriser les communications. Une fois la connexion établie, les données sont cryptées et l'intégrité des informations est assurée grâce à des mécanismes tels que le hachage et l'empreinte digitale. Enfin, TLS permet d'accorder un contrôle d'accès et une confidentialité des communications en imposant des politiques de sécurité sur l'envoi et la réception des données.

En ce sens la mise en place d'une telle technologie permettra d'établir des échanges chiffrés entre le client qui utilise notre site web et le serveur qui l'héberge. De plus cela est un élément essentiel car la majorité des sites chiffrent leurs échanges.

B. Transparence : gestion des cookies

Selon le RGPD, le consentement doit être libre, spécifique, informé et univoque. Cela signifie que l'utilisateur doit être informé des finalités du traitement des données, et donner son consentement en toute connaissance de cause. Les cookies doivent donc être gérés de manière à assurer un consentement réel de l'utilisateur.

La gestion des cookies qui nécessite un consentement réel de l'utilisateur doit respecter les principes suivants :

- Les utilisateurs doivent être clairement informés sur le type de cookies qu'ils acceptent, ainsi que sur les fins pour lesquelles ils sont utilisés.
- Les utilisateurs doivent donner leur consentement de manière active et spécifique.
- Les utilisateurs doivent pouvoir refuser ou retirer leur consentement à tout moment.
- Lorsque les utilisateurs donnent leur consentement, ils doivent être en mesure de le faire selon des paramètres simples et intuitifs.
- Le consentement des utilisateurs doit être recueilli spécifiquement pour chaque type de cookie et chaque fin pour lesquelles ils sont utilisés.
- Les cookies doivent être stockés de manière sûre et ne pas être accessibles à des tiers non autorisés.

Au vue des éléments apportés ci-avant, nous permettons à l'utilisateur, lorsqu'il accèdera au site web, de choisir s'il veut donner son consentement vis-à-vis de ces cookies. Il peut donc choisir quelles informations accepter avec une mention visible et clair des cookies pour rendre l'expérience intuitive et claire.

C. Respect des droits des personnes concernées : mentions légales

Les mentions légales sont des informations obligatoires à mentionner sur un site internet ou une communication. Elles sont définies par des lois, des règlements et des normes qui dépendent du pays ou de la région.

Les mentions légales peuvent inclure des informations sur la propriété intellectuelle, le droit d'auteur, l'information sur le responsable du site, les conditions générales d'utilisation et les politiques de confidentialité.

D'autres informations telles que les conditions de paiement, les informations sur la livraison et les garanties peuvent également être incluses. Les mentions légales sont nécessaires pour protéger l'entreprise et ses clients, et pour s'assurer que les règles et les règlements sont respectés.

Les mentions légales peuvent être placées dans le cadre du principe du respect des droits des personnes concernées. Selon ce principe, les responsables de traitement doivent prendre des mesures pour veiller à ce que la collecte, le traitement et l'utilisation des données personnelles soient effectués conformément aux droits des personnes concernées. Ces droits incluent le droit à l'information, le droit d'accès, le droit de rectification et le droit à l'oubli. En ce sens, les mentions légales doivent être claires et accessibles, et fournir des informations sur le responsable du traitement des données, les données qu'il collecte et comment celles-ci sont utilisées.

Afin de rendre en total adéquation la valorisation d'une telle implémentation, nous avons choisi de positionné dans le site web une rubrique contenant les mentions légales, permettant ainsi de fournir toutes les informations nécessaires concernant les conditions générales et autres politiques de confidentialité.

D. Intégrité et confidentialité : chiffrement des données

La CNIL recommande de chiffrer les données avant leur envoi et de mettre en place des procédures pour s'assurer que seules les personnes autorisées y ont accès. La CNIL recommande également d'utiliser des algorithmes de chiffrement forts et robustes qui sont mis à jour régulièrement pour éviter les failles de sécurité. De plus, elle recommande de limiter les accès aux seules données dont un utilisateur a besoin pour accomplir sa tâche et de s'assurer que les clés de chiffrement sont bien stockées et accessibles uniquement par les personnes autorisées.

Les principes du hachage et du salage des mots de passe consistent à crypter les mots de passe afin de les protéger contre les attaques. Le hachage consiste à appliquer une fonction de hachage à un mot de passe pour créer un résultat qui est alors stocké dans la base de données. Cela signifie qu'au lieu de stocker le mot de passe en clair, un résultat crypté est stocké dans la base de données. Le salage de mot de passe consiste à ajouter une chaîne aléatoire à un mot de passe avant de le hacher. Cela rend le hachage plus difficile à casser, car il nécessite une analyse plus approfondie pour trouver le mot de passe original.

Cette étape est d'une importance cruciale car cela garantie l'intégrité et la confidentialité des données et nous avons procéder à cette réflexion dès la conception du projet. De ce fait nous avons appliqué un algorithme de hachage et de décryptage dans la partie développement du projet notamment au sein des contrôleurs de connexion.

E. Droits des personnes : droit d'accès à l'information

Les principes liés à la possibilité pour un utilisateur d'obtenir une copie de toutes ces informations sont les suivants : l'utilisateur doit avoir la possibilité de consulter ou copier toutes les informations qu'il fournit à un tiers, et il doit également avoir la possibilité de demander que ces informations soient corrigées ou supprimées.

De plus, l'utilisateur doit être en mesure de recevoir une confirmation de la manière dont ses données sont utilisées et une explication de leur utilisation. Enfin, l'utilisateur doit être en mesure de s'opposer à la collecte et à la diffusion de ses données.

Le Règlement Général sur la Protection des Données (RGPD) prévoit des droits spécifiques aux personnes concernées notamment le droit d'accès et de rectification. Ces droits s'appliquent à toute personne concernée par un traitement de données personnelles, notamment par la collecte, le stockage, la conservation ou l'utilisation de telles données.

Le droit d'accès donne à la personne concernée le droit de savoir quelles données personnelles sont collectées, stockées, conservées et/ou utilisées à son sujet.

Le droit de rectification donne à la personne concernée le droit de demander la modification ou la correction des données personnelles à son sujet, afin que celles-ci soient exactes ou à jour.

Dans cette dernière partie, nous proposons à l'utilisateur d'obtenir une copie de l'ensemble de ces informations, il possède également un droit de rectification et de suppression qui est rendu possible dans notre site en procédant à l'envoi d'un formulaire auprès du service client.

IV. Conclusion

Ce projet propose une mise en œuvre intégrée des règles RGPD et de la CNIL dans le contexte d'une application web. Il comprend les étapes suivantes : planification GANTT, implémentation de la sécurité des données, transparence, respect des droits des personnes concernées, intégrité et confidentialité, et droits des personnes. Grâce à cette mise en œuvre, l'application web est en conformité avec les règles RGPD et de la CNIL et garantit la sécurité des données et des personnes concernées.

De plus, des technologies telles que le TLS et le chiffrement des données sont utilisées pour garantir la sécurité et la confidentialité des données. Les mentions légales et les cookies sont gérés pour assurer la transparence et le respect des droits des personnes concernées. Les personnes concernées disposent aussi des droits d'accès à l'information.

En conclusion, les avantages de la mise en œuvre des règles RGPD dans le cadre de notre formation universitaire sont multiples et variés. Il s'agit d'une excellente occasion de développer et d'améliorer nos compétences en matière de protection des données et de sécurité informatique, et d'améliorer nos aptitudes à mieux comprendre et gérer nos informations personnelles. En mettant en pratique ces compétences et connaissances acquises dans le cadre de nos études universitaires, nous bénéficions d'un enrichissement personnel et d'un avantage significatif sur le plan professionnel.