Mise en place d'une application de gestion de processus conformité RGPD

Antoine Lonné (antoine@antoinelonne.dev)

Avril - Juillet 2021

Rapport de stage CPI A2

DL PLace
Maître de stage : Jean Christophe Lairie (gestion@dlplace.eu)

CESI École d'ingénieur
Responsable école : Marc-Alexandre Arnaud (maarnaud@cesi.fr)

Confidentialité : ***DIFFUSION LIBRE***

ÉCOLE D'INGÉNIEURS

FICHE DE CONFIDENTIALITE DES RAPPORTS ET MEMOIRES
NON-DISCLOSURE AGREEMENT

CE DOCUMENT DOIT ETRE COMPLETE POUR TOUT RAPPORT OU MEMOIRE DIFFUSE A CESI ECOLE D'INGENIEURS ET CONTENANT DES INFORMATIONS SUR L'ENTREPRISE D'ACCUEIL

CE DOCUMENT EST ETABLI EN TROIS EXEMPLAIRES : UN SERA CONSERVE PAR CESI ECOLE D'INGENIEURS, UN AUTRE PAR L'ENTREPRISE, LE TROISIEME DEVRA IMPERATIVEMENT ETRE INTEGRE AU RAPPORT PAR L'ELEVE.

THIS PAGE MUST FEATURE IN ANY DOCUMENT PRODUCED FOR EVALUATION PURPOSES AT CESI GRADUATE SCHOOL OF ENGINEERING AND CONTAINING INFORMATION ABOUT A HOST COMPANY.

IT IS ESTABLISHED IN THREE COPIES: ONE FOR THE SCHOOL'S RECORDS, ONE FOR THE COMPANY, AND ONE IMPERATIVELY INCLUDED IN THE STUDENT'S REPORT.

Titre du rapport ou du mémoire/ *Title of the document* **:**
Mise en place d'une application de gestion de processus conformité RGPD

Nom et prénom de l'étudiant/ *Intern's Name* **:** Antoine Lonné

Formation suivie/ *Course at CESI* : CPI A2

Nom du maître de stage/ *Intern's Supervisor* **:** Jean-Christophe Lairie

Structure d'accueil/ *Host Company* **:** DL Place

Confidentialité du rapport ou du mémoire (soutenance)
Confidentiality of the document produced for evaluation purposes

◉ **Diffusion libre / *Full disclosure***
Les rapports / mémoires sont conservés en archives et ils peuvent être librement consultés. Ils peuvent être utilisés par les destinataires, les études peuvent faire l'objet de publication …
The documents are kept in the school's archives and can be consulted freely. They can be used by whomever receives them and the studies they contain can be published…

○ **Diffusion restreinte / *Limited disclosure***
Les rapports / mémoires **sont restitués à l'entreprise à l'issue** de la soutenance. Aucune reproduction n'est autorisée. La responsabilité de cette opération est confiée au stagiaire.
*The documents **are given back to the company** at the end of the viva voce. No copy is allowed. The retrieval of the document is the full responsibility of the intern.*

Dans le cadre de la politique de lutte contre le plagiat, les rapports / mémoires seront susceptibles d'être analysés pour en vérifier les sources et ceci quel que soit le mode de diffusion prévu ci-dessus.

As part of our policy against plagiarism, reports are likely to be analyzed to verify the sources regardless of the level of confidentiality specified above.

Date : 03/06/2021	Date : 05/06/2021	Date : 07/06/2021
L'entreprise/ the company	**Le stagiaire** / the intern	**L'école / the school**
DL Place Signature numérique de DL Place Date : 2021.06.03 16:32:28 +02'00'		

Table des matières

Table des figures

1 Remerciements

En tout premier lieu, je tiens à remercier Jean-Christophe Lairie, mon maître de stage, sans qui cette première expérience n'aurait pas été possible. Je tiens aussi à saluer son courage d'entreprendre et de parier sur deux stagiaires pour lancer son entreprise. Il a une motivation et un intérêt pour plusieurs domaines variés et ne manque jamais d'idée pour son entreprise !

Je tiens aussi à remercier ma collègue, stagiaire comme moi, Maureen Joseph-François, avec qui j'ai bien rigolé, qui a apporté une très bonne ambiance à ce stage.

J'aimerais remercier toutes les personnes qui ont relu ce rapport, Rudy, Mathilde, Maureen, ma mère.

Je souhaite aussi adresser un remerciement à l'école pour me permettre de réaliser cette expérience et plus particulièrement à Cynthia Péboscq d'avoir relayé cette offre de stage.

2 Introduction

Ce stage à été effectué dans le cadre de ma deuxième année en classe préparatoire intégrée spécialité informatique au CESI École d'ingénieurs. Il a eu pour but de m'offrir une première expérience professionnelle dans le milieu de l'informatique.

Ce stage dans une entreprise avec un effectif réduit m'a permis de toucher à des technologies et aspects diversifiés de l'informatique. Cela m'a fait découvrir un cadre de travail et m'as permis approfondir et développer des connaissances sur des technologies utilisées durant ce stage.

Mes attentes personnelles sur ce stage étaient de me former sur une technologie, d'apprendre à comprendre seul un code source à l'aide de sa documentation. Les objectifs étaient d'implémenter dans l'application toutes les fonctionnalités requises par mon maître de stage. L'application est un plugin [1] se rajoutant à GLPI [2] qui est basé sur un plugin déjà existant permettant de gérer le processus de conformité RGPD. Le code source est écrit en PHP.

Ma problématique est donc la suivante : **Comment mettre en place une application web de gestion de processus de conformité RGPD de manière autonome ?**

Dans un premier temps, nous décrirons l'entreprise, son histoire, ses produits proposés et son but. Ensuite, nous étudierons mes différentes missions au sein de cette entreprise et quelles ont été les actions mennées pour les compléter.

3 Présentation de l'entreprise

3.1 Historique et secteur d'activité

DL Place est une startup très récente, composée à l'origine de trois personnes, Jean-Christophe Lairie mon maître de stage, et deux stagiaires, Maureen Joseph François, chargée du marketing et de la communication et moi-même, chargé du développement. Dès qu'il le pourra, et probablement dès septembre 2021, le créateur prévoir d'investir de manière plus pérenne en transformant ces emplois temporaires en postes permanents.

DL Place veut développer et commercialiser une plateforme SaaS [3] dédiée au pilotage de la protection.

1. Greffon se rajoutant à un logiciel
2. Gestionnaire Libre de Parcs Informatiques : logiciel web permettant de faciliter la gestion d'un parc informatique (voire même de la gestion d'actifs)
3. *Software as a Service* en anglais, logiciel en tant que service en français, qui décrit une solution logicielle clé en main sous forme d'abonnement plutôt que de licence d'utilisation (seul l'accès au logiciel est proposé, les autres couches techniques sont prises en charge)

Ce type de logiciel s'appelle GRC : "Gouvernance, gestion des Risques et pilotage de la Conformité". La catégorie de ce type de logiciel est relativement peu connue des petites structures. Jusqu'à présent il est plutôt utilisé par les grandes entreprises, notamment les banques depuis la loi Sapin 2. Ces outils permettent d'établir une matrice des risques, de proposer proposer des actions visant à diminuer la fréquence et l'impact des risques, de suivre la mise en œuvre de ces actions en impliquant les directions, acteurs et auditeurs, en mode projet, puis d'indiquer le risque résiduel à l'issue des actions, outils, procédures, systèmes de surveillances et audit en continu si ont pu être mis en œuvre

Or la multiplication de ces normes et l'application à des organisations de moindre taille, la volonté également plus fréquente par ces organismes d'obtenir des labels basées sur des normes, la volonté de faciliter et de partager le travail des auditeurs avec l'ensemble des acteurs et des tiers impliqués, conduit DLPlace à estimer une démocratisation prochaine de l'utilisation de ce type d'outil. Le RGPD en est un exemple flagrant : une norme relativement complexe s'appliquant à tous les organismes quel que soit leur taille. Un exemple précédent, qui date de 2004 mais qui n'avait pas fait l'objet d'efforts de digitalisation est le DUER, c'est à dire la protection des salariés (postes de travail).

DL place estime que la multiplication des contraintes dans les prochaines années, notamment dans les domaines RSE, va amener plus d'organisation à utiliser ce type de logiciel. Les organisations étant plus petites, avec moins de moyens humains et une connaissance technique moindre de ces sujets, elles doivent trouver des outils qui les guident, leur fournissent une bases de connaissance sur ces sujets nouveaux et souvent complexes. Un objectif est de couvrir avec une plateforme unique l'ensemble des besoins nécessaires à la réalisation de ce type de projet complexe, délicat et impactant pour l'organisme.

DLRegister se veut être cette plateforme. Actuellement, le premier module proposé est celui concernant la réglementation RGPD. En effet, DLPlace est née du besoin de formalisation de ses audits et démarches de conformité, mises en œuvre par Jean-Christophe Lairie, DPO après des clients d'ActuelBuro depuis juin 2018.

Par ailleurs, il est actionnaire de cette entreprise à structure familiale pour laquelle il travaille depuis 18 ans. Bien qu'ActuelBuro avait la structure pour se lancer dans ce projet, les associés ne se sont pas entendus autour de cette initiative. En conséquence JC Lairie a décidé de se lancer seul en créant l'entreprise DL Place, avec l'objectif de développer et commercialiser ce logiciel, tout en conservant dans un premier ses fonctions de DPO.

3.2 Produits et services proposés

DL Place propose des solutions logicielles en tant que service, aussi nommées SaaS. Ces solutions permettent actuellement de gérer le processus de conformité aux RGPD d'entreprises et d'associations : de telles organisations traitent des quantités d'informations importantes ou des informations sensibles (données clients, dossiers médicaux, données des salariés...). Elles doivent s'assurer qu'elles s'inscrivent dans une démarche de conformité vis-à-vis du **Règlement Général sur la Protection des Données** européen. [4]

3.2.1 À destination des TPE, commerces, professions libérales

Le premier produit de DL Place est "DPORegister Express" : il permet à n'importe qui de répondre à l'obligation légale du RGPD en élaborant rapidement un registre des traitements. En effet, le RGPD exige de tous les organismes qu'ils élaborent le registre de leurs traitements [3].

Ce produit contient une bibliothèque pré-remplie de bases légales, catégories de personnes et donnés, indication et ressources diverses qui permettent d'éditer un traitement personnalisé rapidement. Le tout sans posséder de connaissances particulières dans le domaine du traitement des données et de la conformité à celui-ci.

3.2.2 À destination des DPO [5]

Un autre produit de DL Place est DPORegister (non-express, complet), un outil similaire à sa version Express, mais plus complet et plutôt à destination des DPO.

Il permet d'élaborer le même type de registre de traitement, mais contient plus de fonctionnalités[4] : comme le suivit d'audits, des ressources de formation telles que des QCM, une intégration avec des documents et contrats...

3.2.3 DPO à la demande

M. Lairie ayant une expérience en tant que DPO, il propose ses services en tant que personne à la disposition d'entreprises ne bénéficiant pas de DPO. Certaines entités doivent obligatoirement posséder un DPO, c'est le cas des organismes publics, des organismes qui effectuent du suivi régulier de personnes à grande échelle ou qui traitent des données sensibles (ex: secteur médical)[5].

4. Abrégé RGPD en français et GDPR en anglais
5. *Data Protection Officer* en anglais ou Délégué à la protection des données en français, personne en charge de la protection des données et de la conformité de leur traitement dans une organisation

3.3 Liens avec les autres acteurs

Les principaux clients actuels de DL Place sont des clients de Jean-Christophe Lairie de ActuelBuro pour lesquels il suivait déjà le processus de conformité RPGD et aujourd'hui nous prestataires de services pour ActuelBuro. Nous leur sous-traitons la gestion du processus de conformité RGPD de ces clients.

Le produit principal de DL Place est un plugin venant se greffer sur GLPI, un outils web libre (comprendre un logiciel libre [7 : 12, section 4.]) de gestion de parcs informatiques créé et maintenu par la société Teclib'[11]. Cette société propose soit une version gratuite à héberger soit même, soit GLPI sous forme de SaaS et offre un support.

Nous hébergeons donc GLPI et son plugin nous-même, DL Place sous-traite la partie matérielle de l'hébergement de machines : nous louons un VPS [6] à OVHcloud, le numéro 1 français de solutions d'hébergement. Cela permet d'avoir un contrôle total sur l'application sans avoir à se soucier de l'hébergement d'une machine, de plus l'application consommant peu de ressources, il revient plus économique de sous-traiter cette partie.

3.4 Philosophie

DL Place proposant des offres en rapport avec la protection des données, il en va de soit qu'elle vise à être un modèle dans ce domaine-là. Cela en adoptant des bons réflexes en terme de RGPD, c'est-à-dire ne collecter que les données nécessaires, être transparent, faciliter exercice des droits des personnes, mettre en place des durées de conservation des données, sécuriser ces données et prendre au veiller régulièrement au bon respect des procédures [6].

4 Mes missions

DL Place, au départ de ma période de stage, n'a aucun produit SaaS à présenter à proposer à ses clients, ma mission maîtresse est donc de créer ce produit, de le déployer sur une infrastructure et de le rendre fonctionnel et utilisable de manière autonome, c'est-à-dire sans nécessité des compétences informatiques poussées, par les clients et mon maître de stage. Une fois ce travail réalisé, je dois rendre compte sous forme d'une documenation mes connaissances acquises à destination des prochianes personnes qui vont développer cette plateforme.

6. *Virtual Private Server* en anglais ou Serveur Privé Virtuel, aussi machine virtuelle

4.1 Création du produit

4.1.1 Contexte

Ma mission première et principale dans ce stage est la réalisation du produit "DPO Register" (et dans un premier temps sa version "Express"), ce produit se comporte sous la forme d'un plugin s'ajoutant à GLPI. Il a pour but de permettre une saisie qui permet de suivre le processus de conformité aux RGPD, il est basé sur un plugin déjà existant sous plusieurs noms selon les version "dporegister" "gdprropa" (signifiant *GDPR Register of processing activities* ou en français Registre RGPD de traitement des activités). Ces plugins sont disponibles librement sur le dépôt github des auteurs [8,9], ils fournissent un cadre au développement de l'outil de DL Place, le permettant ainsi d'être relativement rapide.

GLPI étant écrit en PHP, ses plugins aussi, il semble important de préciser quelques-unes des caractérises de ce langage. PHP est un langage de programmation dédié au domaine du web, il n'est pas visible des utilisateurs, il fait partie du *back-end*[7]. Il permet entre autres l'affichage de pages, le traitement de requêtes HTTP. Il est exécuté part un serveur web[8] tel que Apache2, NGINX, IIS pour ne citer que les plus connus. On peut le décrire comme un langage appartenant à plusieurs paradigmes de programmation[9] :

- *Impératif* car un script PHP comporte un liste d'instructions qui vont être exécutées (le contraire de déclaratif qui sert à décrire un état/contenu)
- *Orienté objet*, car on peut créer des briques logicielles qui peuvent représenter des abstractions entités réelles (par exemple, un utilisateur est un objet, un contrat est un objet...)
- *Fonctionnel*, car on peut écrire un script PHP en appels de fonctions similaires sur le principes à des fonctions mathématiques (elles exécutent une transformation d'état.)
- *Procédural*, car comme pour l'aspect fonctionnel, on peut décomposer un script en appels de procédures qui réalisent des actions
- *Réflexif*, car le PHP peut s'auto-examiner et déterminer son propre état
- Et finalement l'aspect qui le caractérise le plus, il est *interprété* c'est-à-dire que le code PHP est compris par le serveur web à chaque exécution, contrairement aux langages compilés qui eux sont transformés en langage machine, c'est-à-dire une liste d'instruction dites de *bas niveau*[10] directement exécutés par le processeur.

Pour plus d'informations quant à son histoire son utilisation ou son fonctionnement, je ne peux

7. Partie immergée de l'iceberg d'un site web : c'est la partie invisible des utilsateurs
8. Aussi appelé serveur HTTP, c'est une application qui permet de servir du contenu (ex: des pages) web à un utilisateur émettant des requêtes HTTP(S) (accéder à un site web)
9. Un paradigme de programmation est une manière d'aborder l'exécution d'un programme
10. Bas niveau signifie proche du matériel, peu de couches d'abstraction

que vous référer au rapport de veille technologique de mon ami et camarade de classe Nicolas sur *"L'évolution du Langage PHP ainsi que son environnement d'exploitation"* [2].

4.1.2 Attentes

La première étape de cette mission à été de recevoir les attentes déjà établies à l'avance dans le but de les comprendre, et de déterminer leur importance. Le produit est un formulaire de saisie sophistiqué qui permet de saisir des informations à propos d'un traitement de données, une fois les données saisies l'application génère un rapport sous format pdf. Il est intégré à GLPI, c'est-à-dire qu'il interagit avec les objets déjà renseignés dans GPLI (contrats, utilisateurs, entreprises...).

Toutes les attentes de ce formulaire ont d'abord été listées dans un tableau : il regroupe les fonctionnalités et le contenu des éléments souhaités pour l'enregistrement d'un rapport, de manière exhaustive (cf. Figure 1).

Ensuite, un "mockup" du formulaire a été dressé, il permet d'avoir une vision plus lisible pour faciliter la réalisation. Cela a été ma référence principale pour durant la phase de réalisation. Avec ces informations je connais donc l'objectif à atteindre et un plan d'action a pu être dressé : dans un premier temps mettre en place un environnement de développement pour me familiariser avec la plateforme en mode "bac à sable" ; ensuite, il y a une partie assez importante de compréhension de la documentation, afin de prendre connaissance de ce qu'il est possible de réaliser et comment le réaliser ; et enfin la réalisation du plugin, il faut donc analyser le code source de l'existant afin d'y apporte toutes les modifications nécessaires.

4.1.3 Réalisation

Durant quelques semaines au début de la réalisation, j'ai eu à me familiariser avec l'environnement de GLPI : il m'a fallu comprendre le fonctionnement et les rôles des différentes briques applicatives. J'ai pu dresser ces diagrammes qui permettent d'appréhender le processus de fonctionnement de GLPI et de ses plugins, architecture logicielle qui ne m'est pas familière (il semble différent d'un MVC [11]). Lorsque l'on accède à une page de GLPI, on émet une requête HTTP(S) vers un URL se terminant en `.form.php`. Ce fichier PHP se trouve dans le répertoire `front/` de GLPI, ces fichiers gèrent les requêtes, ils peuvent être assimilés à des contrôleurs de route [12]. Leur rôle est de vérifier les autorisations de l'utilisateur qui émet la requête puis, appellent des méthodes qui vont effectuer les actions demandées :

11. Modèle Vue Contrôleur : architecture logicielle qui découpe le code source en 3 parties : le modèle gère l'interaction avec la base de données, la vue contient des parties du visuel qui sera affiché et le contrôleur reçoit une demande de l'utilisateur et va composer un résultat en utilisant des modèles et des vues

12. Élément d'un logiciel web permettant de savoir quelle ressource doit être fournie en fonction de l'URL donnée

afficher des informations, des formulaires, ajouter ou supprimer un élément de la base de données... Ces méthodes sont présentes dans les fichiers `.class.php` se trouvant dans le répertoire `inc/` de GLPI, ces méthodes contiennent de la logique et permettent l'affichage . On peut faire l'analogie avec un contrôleur dans une architecture MVC même si dans ce cas-là les fonctions de la vue (affichage) et du modèle (interaction avec la base de données) sont aussi remplies (pour un visuel du traitement d'une requête, cf. Figure 2).

D'un autre coté, pour les plugins le fonctionnement entre les `.form.php` et les `.class.php` est similaire à GLPI, la différence est qu'ils contiennent des "crochets" (`hook`). Ils sont déclarés dans le plugin et qui permettent de s'implanter à GLPI et réaliser des ajouts divers (dans des menus, formulaires ou pages) ou juste le fonctionnement du plugin comme le crocher d'installation qui peut gérer les tables de base de données nécessaires.[11] (pour un détail visuel sur les plugins, cf. Figure 3).

En parallèle de cette tâche, il faut comprendre la logique du plugin GDPRRoPA (qui sert de base à l'application réalisée), pour cela, j'ai dressé un MPD [13] des tables de bases de données du plugin afin d'avoir une base de compréhension grâce aux relations des données. Le SGBD [14] utilisé par GLPI et donc par extension aux plugins est MySQL (ou son implémentation équivalente MariaDB). Par la suite, un nouveau modèle à été créé permettant de s'accorder au mieux aux spécifications du cahier des charges. Il permet de stocker toutes les données utilisées de l'application(cf. Figure 4), ce modèle, avec le tableau correspondant aux fonctionnalités (cf. Figure 1) a servi de base à la réalisation.

Ensuite, la seconde étape après l'analyse de l'environnement technique est "simplement" la réalisation. Pour cela, un grosse partie d'analyse de la documentation fournie par GLPI à destination de ses développeurs[12] est très utile et intéressante, elle m'a personnellement semblé barbare à la première approche et n'encourage pas à la création, il est nécessaire d'avoir une motivation importante. Cette documentation sert plutôt de référence aux débutants qui connaissent et comprenant déjà le fonctionnement de GLPI. Aussi les sources de plugins existants m'ont permit de trouver des information non-présentes dans la documentation développeur, ainsi que des exemple d'utilisation complets des fonctionnalités offertes par GLPI pour les développeurs.

Une fois l'analyse préliminaire de l'environnement technique réalisée, le modèle dressé, les fonctionnalités peuvent être implémentées : le résultat est un formulaire multi-pages qui permetent la saisie d'un traitement. Si le traitement a déjà été complété (ou des parties le sont) les résultats y sont intégrés soit directement dans les champs de saisie, soit dans des tableaux selon leur cardinalité [15]. Par exemple,

13. Modèle Physique des Données : diagramme qui décrit l'agencement des données dans les tables, qui tiens compte de la réalisation des relations les éléments entre eux (les clé étrangères sont précisées, elles indiquent qu'un champ provient d'une autre table, cela permet de démontrer les relations)

14. Système de Gestion de Bases de Données : logiciel gérant des bases de données, dans ce cas là des bases de données relationnelles, c'est-à-dire que les éléments des tables ont des relations entre eux, on utilise donc l'algèbre relationnelle

15. Multiplicité, dans un schéma relationnel en modélisation de données, ce indique le nombre maximum et minimum

un traitement de données peut se baser sur plusieurs bases légales qui seront affichées dans un tableau (cardinalité 1-n), mais le responsable du traitement est global est unique dans le traitement (cardinalité 1-1) (Cf. Figure 4).

L'interface du plugin utilise des composants stylistiques présents dans GLPI, le plugin doit paraître comme partie itégrante de GLPI (cf. Figure 7).

4.1.4 Organisation de travail

J'ai été autonome sur mon processus d'organisation, j'ai cherché la méthode qui me permettrai de fournir des fonctionnalités le plus rapidement possible ainsi qu'avoir un retour rapide afin d'implémenter l'entièreté des fonctionnalités pendant la durée de mon stage.

La réalisation est effectuée par petits cycles itératifs apportant des fonctionnalités, il est en quelques points ressemblant à une organisation agile scrum. J'ai découpé le projet en groupes de tâches que l'ont peut assimiler à des *sprints*, leur *backlog* comporte le détail d'une fonctionnalité avec les tâches à effectuer. Le *product backlog* est le cahier des charges, mon maître de stage le *product owner*. En suivant ce cycle d'évolution, Jean-Christophe Laire peut tester et utiliser une version du plugins même en cours de développement et donner un retour, modifier le backlog en accord et induire un modification pendant le processus de développement.

Pour m'organiser, même seul, j'ai eu recours à l'utilisation d'outils de gestions de projet tels que ceux inclus dans GitHub ou dans GLPI. Même si le travail se concentre autour de GLPI et qu'il peut sembler intéressant de l'utiliser pour la gestion de projet, en réalité les outils de GitHub sont mieux intégrés à la gestion du code source et permettent d'être plus efficace. Git étant utilisé pour le versionnage, l'intégration de gestion de projet GitHub est facile et évite de perdre du temps. GihHub offre une vue de type Kanban (cf. Figure 5).

4.2 Déploiement, intégration, système

4.2.1 Besoins

Pour poursuivre sur l'organisation, il faut penser à une stratégie de gestion de version et de sources, qui permette idéalement la réalisation du déploiement et de l'intégration du plugin à GLPI. C'est-à-dire passer du code source créé et testé sur un ordinateur de développement au produit livré et fonctionnel. Pour un souci de séparation des phases de tests de d'utilisation du produit, il faut prévoir

de chaque objet que contient une relation. Elle se compose de deux chiffres indiquant le maximum et le minimum pouvant être 0 (aucune), 1 (une seule), ni (aucune ou plusieurs).

différents environnements. C'est-à-dire un environnement de développement qui permet de réaliser des tests avec des données non importantes. Il permet de tester des fonctionnalités et de s'assurer de leur bon fonctionnement avant de les déployer sur un autre environnement, celui de production. Cet environnement a pour but d'être opérationnel tout le temps. Il contient toutes les données "live", il sert les utilisateurs finaux.

Un autre point important, après mon départ, mon maître de stage devra être en capacité d'utiliser le système dans le but de le mettre à jour. Il faut donc une solution rapide à prendre en main, et avec une complexité faible.

4.2.2 Situation de départ

Il convient dans un premier temps de dresser les points positifs et négatifs de l'état de départ de l'architecture système, cela dans le but de connaître les axes sur lesquels il faut apporter des modifications et ce qu'il faut conserver.

À mon arrivée en stage, GLPI était hébergé sur une machine (virtuelle) d'ActuelBuro fonctionnant sous Windows Server. XAMPP, un ensemble d'outils de développement PHP, servait de serveur web. Les avantages pour un débutant sont importants : l'environnement graphique Windows est facilement utilisable par une grande majorité de personnes et XAMPP est facile à mettre en place. Cela permet donc à un débutant de rendre opérationnel rapidement un site web.

Néanmoins ce système présente des lacunes plus ou moins importantes sur plusieurs niveaux qui sont notamment accentuées par le fait que l'application est développée en continu. Des nouvelles fonctionnalités sont ajoutées en continu dans l'application, il y a un besoin de déployer des changements facilement : il est donc inimaginable de se connecter en contrôle à distance avec le logiciel Anydesk pour mettre à jour le plugin. De plus, avec une mauvaise connexion, des *lags*[16] peuvent apparaître en utilisant cette méthode.

XAMPP permettant une mise en place rapide, par défaut, ne prend pas en charge l'instauration de directives de sécurité, en effet l'accès à PhpMyAdmin, était ouvert publiquement sur le web sans mot de passe. En d'autres termes, cela signifie que toute la base de données de l'application est accessible par n'importe qui pour effectuer n'importe quelle action (modifications, suppressions...). Cela car PhpMyAmin est un client web pour les bases de données MySQL, c'est-à-dire un logiciel qui se connecte à un SGBD, il permet de réaliser toute tâche d'administration sur celles ci.

16. Échec de maintien d'une connexion stable à un serveur qui peut entraîner une dégradation de l'interaction, des retours en arrière, un écran figé par intermittence...

4.2.3 Solutions mises en place

4.2.3.1 Moyens organisationnels

L'outil le plus évident pour s'occuper de la plupart de ces besoins est Git, un outil de gestion de versions de code source[7 : 13 Section 4.2. §2]. Git permet un versionnage en stockant les modifications de manière incrémentielle, chaque modification est contenue dans un "*commit*", les commits sont signée par un utilisateur (plus précisément par son adresse mail) et possèdent la signature du précédent cela génère une signature unique, cette suite de commits est consultable et compose l'historique (on peut avoir une représentation visuelle avec des logiciels : Figure 6). Les commits permettant d'avoir une atomicité [17], ce qui simplifie l'échange de versions : seuls les commits les plus récents sont envoyés (et non pas l'entièreté du code source).

Cet outil permet aussi d'utiliser plusieurs branches qui permettent de collaborer en parallèle et de répondre aux besoins de séparation d'environnement, permet une intégration à l'application présente sur un serveur. L'intégration et le déploiement sont grâce aux crochets ("*hooks*" de post-réception de git) qui exécutent des scripts qui vont intégrer le plugin à GLPI. Comme énoncé précédemment (Cf. 4.1.4), nous utilisons un dépôt Github dans un but de sauvegarde d'une copie du logiciel (en plus du dépôt présent sur le serveur) ainsi qu'en tant qu'outil collaboratif de suivi de l'avancement.

4.2.3.2 Système choisi

Comme énoncé précédemment (Cf. 3.3 §3), nous avons choisis de sous-traiter l'hébergement de machine chez OVHcloud en louant un VPS, cela présente plusieurs avantages. Nous pouvons notamment mettre en lumière le coût réduit proposé par cette solution, car nous n'avons pas l'utilité d'une machine dédiée [18]. La location d'une seule machine virtuelle semble aussi être la solution pour une application qui n'a pas besoin d'une immense flexibilité de charge (le nombre trafic est faible et ne prévoit pas d'exploser), cela ne justifie pas la mise en place d'une infrastructure plus complexe. On obéit dans ce cas là au principe KISS [19]. Aussi, un autre aspect à noter à propos de ce choix est la sécurité, que ce soit sur la sauvegarde des données ou sur l'aspect matériel (vol, destruction...), OVH s'en occupe (Même s'il reste tout de même bon à noter qu'en théorie les datacenters sont des lieux sûr, on peut noter le récent incendie d'un des datacenters d'OVH à Strasbourg[10], qui au passage m'a fait perdre quelques données personnelles).

17. se dit d'un élément élémentaire, non subdivisible
18. Terme utilisé pour décrire un serveur physique alloué entièrement à un client, en opposition à une machine virtuelle qui ne représente qu'une partie d'une machine physique
19. *Keep It Simple Stupid* ou en français, on peut traduire en Garde le simple et con, on peut aussi assimiler ces principes à la "Philosophie Unix" [7 : 3, section 2.1.2.]

Le système d'exploitation choisi est Linux, une distribution [20] prévue pour les serveurs (Ubuntu server), il répond au critère de simplicité, tourne très facilement sur un petit serveur. Cela grâce au fait linux n'est pas livré avec des tas de programmes tournant en arrière-plan, aussi les versions serveurs ne possèdent pas d'interface graphique ce qui les rends d'autant plus léger. Aussi, il me semble important de noter que plus un système est simple, plus la sécurité l'est. En effet, Linux étant simple, meilleure est sa compréhension globale, donc meilleur est sa sécurité, l'administrateur du système peut comprendre ce qu'il se passe sur la machine pour la sécuriser au mieux. Moins il y a d'éléments différents, moins il y a de sources potentielles de problèmes.

4.2.3.3 Stack technique

À propos du soucis de XAMPP, ici un réel stack LAMP [21] a été mis en place, il a été installé et configuré de manière sécurisée (convenable pour un environnement de production) sur la machine.

Apache2 est le serveur web, il est configuré pour gérer plusieurs sites virtuels (ex : un site de développement et un de production sur une même instance d'Apache) et sa configuration permet de mettre en place des directives de sécurité. Par exemple, on doit restreindre l'accès à un répertoire du site pour l'utilisateur afin d'éviter que l'utilisateur ne puisse consulter l'entièreté des fichiers stockés par GLPI. Ou bien limiter le nombre d'information données par le serveur lors de sa réponse à une requête : en effet, si la version d'Apache est connue, cela facilitera l'exploitation de failles connues sur une version spécifique [22].

Le langage PHP est installé sur le système dans sa version 7.4, il permet d'exécuter le code du logiciel. Il existe néanmoins une version de PHP plus récente, PHP 8, sorti en fin d'année 2020. Cette version propose des correctifs permettant d'accroître les performances et la lisibilité du code au détriment de certaines fonctionnalités des versions antérieures.

GLPI est désormais compatible avec PHP 8, de même que le plugin que nous développons (mon environnement personnel de développent utilise aussi cette dernière version) mais notre infrastructure tourne grâce à la version précédente : PHP 7.4. Néanmoins, nous utilisons d'autres plugins tiers sur notre installation de GLPI et j'ignore actuellement s'ils sont compatibles eux aussi avec cette dernière version. Une idée très peu réfléchie serait de mettre à jour PHP vers sa version 8 directement sur la machine pour profiter des avantages offerts par cette version, mais en cas d'échec de compatibilité avec un

20. Distribution d'un logiciel, dans le cas de Linux, c'est une version qui contient Linux (le noyau), des programmes et utilitaires (compilateur, shell, gestionnaire de packets)[7, . page 9, section 3.2]

21. Acronyme désignant le *technology stack* (pile technologique, ensemble de logiciels en harmonie pour faire fonctionner une application) composé de Linux, Apache, MySQL (ou MariaDB) et PHP (ou Perl ou Python)

22. À noter tout de même que cela s'apparente à de la sécurité par l'obscurité, on cache les détails pour ralentir les découvertes de failles, cette pratique n'est pas forcément efficace. Certes, cela peut aider, mais il ne faut pas penser tout un dispositif de sécurité sur cette méthode

plugin, cela mettrait au pire inutilisable l'application, au mieux une partie du plugin non-fonctionnelle. Il faut donc prendre le temps de préparer un environnement similaire à celui présent en production pour vérifier cette compatibilité. Les solutions peuvent être soit de tester sur une autre machine (locale) mais cela ne reproduirais pas totalement les conditions de l'environnement de production, soit une autre piste envisageable serait la containerisation [23] mais, ne connaissant que peu cette technologie, le temps investi à comprendre et utiliser cette technologie ne semble pas bénéfique au cadre de cette entreprise. En effet, la période de stage se terminant bientôt et le nombre de tâche restant important, cela semble tendu d'un point de vue délais de réalisation.

Du côté de SBGD, le choix est porté sur MariaDB, un fork [24] totalement open-source de MySQL. MariaDB étant communautaire, son développement est plus actif et réactif face à MySQL (qui lui est actuellement développé par Oracle), aussi MariaDB possède des correctifs qui le rendent plus rapide et performant.

4.2.3.4 Sécurité

Cette infrastructure fait tourner un logiciel qui est notre produit, ce produit est accessible de manière publique (il y a bien une authentification pour accéder à l'application, mais celle-ci est accessible depuis n'importe quel possédant une connexion internet et un navigateur web). Le fait que cet accès soit public induit qu'il faut mettre en place des moyens de sécurités.

Comme abordé précédemment (section 4.2.3.3 §2), une configuration d'Apache sur notre serveur web permet de limiter les exploitations de failles de sécurité. Aussi, il a fallu le plus rapidement possible adresser l'erreur de configuration de XAMPP permettant à n'importe qui d'accéder à la base de données par PhpMyAdmin (section 4.2.2 §4). La solution est simplement implémentée en configurant MariaDB en ajoutant un mot de passe ainsi qu'en activant l'authentification dans PhpMyAdmin.

L'accès au serveur, pour réaliser les tâches d'administration, est effectué en utilisant le protocole SSH (Secure SHell). Ce protocole utilise la cryptographie asymétrique pour garantir une liaison sécurisée entre deux hôtes, plus précisément cela établit un shell [25]. Pour établir cette connexion, il a été choisi de ne pas utiliser de mot de passe, mais plutôt une paire de clés de chiffrement. Une clé publique est présente sur le serveur, cette clé ne peut valider une connexion seulement si elle a été émise avec la clé privée correspondante (clée privé appartenant à l'utilisateur souhaitant se connecter), ce système de

23. Sur un système de soit type Linux, c'est l'isolation d'un logiciel dans son propre environnement, il n'interagit pas avec l'extérieur du container et n'a conscience seulement de ce qu'il contient. Une solution de container populaire et largement utilisée est Docker.

24. Scission, dans ce cas-là d'un logiciel qui en est devenu deux.

25. Interprète de commande, il peut être bash (le plus souvent sur les systèmes de type Unix actuels), sh, zsh, PowerShell... et permet de contrôler un ordinateur avec seulement un échange texte, rendant cette communication rapide et facile

clés possède trois avantages par rapport à un mot de passe : les clés sont plus grandes que des mots de passes (entre 1024 et 4096 bits [26]), possèdent une entropie [27] plus grande qu'un mot de passe généré par un humain, et enfin chaque utilisateur peut posséder sa clé et il est donc possible de les révoquer individuellement (en retirant la clé publique correspondant du serveur), là où un mot de passe du compte administrateur est unique.

Ce shell (offert par la connexion SSH) permet donc de contrôler le système à distance. Cette solution peut, certes, paraître moins évidente pour un utilisateur moins expérimenté par son aspect austère (ce n'est qu'une console avec du texte) mais est bien plus performante et stable qu'un contrôle de bureau réalisé avec Anydesk. De plus, la liaison SSH peut servir de passerelles pour d'autres protocoles : on peut utiliser le protocole SFTP [28] qui permet de transférer facilement des fichiers depuis ou vers une machine distance, ou utiliser un tunnel SSH pour une connexion à une base de données afin d'éviter d'exposer la base de données au public.

Pour poursuivre sur le sujet suivant, il reste important de noter qu'à la suite de ce stage, Jean-Christophe Lairie sera seul durant un certain temps, il ne faut pas que les mesures de sécurité soient un frein à l'utilisation : le système se doit d'être simple à comprendre.

4.3 Futur du produit

4.3.1 Nécessitées

Étant le seul stagiaire chargé du développement et de l'administration système dans cette organisation, il faut qu'à la fin de ma période de stage, l'entièreté du système mis en place soit utilisable de manière simple, autonome et complète par mon maître de stage. Il faut aussi rendre l'application accessible et fonctionnelle par les clients.

Aussi, la base de code doit être plus facile à prendre en main pour le ou les prochains développeurs qu'elle l'a été pour moi. Le code est très peu commenté, peu sembler ressembler à du "*code spaghetti*", c'est une métaphore en informatique désignant un système désordonné tel un plat de spaghetti, en tirant sur un fil d'un côté de l'assiette cela provoque des mouvements de l'autre côté[1]. Le but est donc d'avoir un code clair avec peu d'enchevêtrements, et un documentation technique permettant une maintenance et une compréhension la plus facile et rapide. Cela dans l'espoir que la prochaine personne en charge du développement ne perde moins de temps sur la compréhension du système et soit opérationnelle rapidement. En effet, j'ai avancé à tâtons sur cette base de code.

26. Rappel : 8 bits = 1 octet (ou *byte* en anglais) = 1 caractère alphanumérique
27. Désigne le taux de désordre, plus il est élevé, plus le résultat est imprévisible
28. FTP (File Transfert Protocole, protocole de transfert de fichiers) par un tunnel SSH

En parallèle de cette documentation technique, un document moins technique est produit, cela dans le but d'aider mon tuteur à comprendre comment accéder à la machine, comme utiliser le système de versionnage et comment adresser certains problèmes qui pourraient survenir.

4.3.2 Réalisation

À propos de l'expérience utilisateur, il a été fait usage au maximum des mécanismes existants dans GLPI : l'interface homme-machine comporte une logique identique à celle de GLPI avec des composants similaires (boutons, champs de texte et sélection...). Cela permet à un utilisateur connaissant déjà des rudiments de GLPI de s'y retrouver facilement. De plus, cette similitude avec les autres parties de GLPI donne un access plus "fini" au produit, il semble faire partie de l'emsemble.

Vis-à-vis de mon tuteur, l'application correspond à ses attentes sur le plan de l'expérience utilisateur. En tant que qu'utilisateur aguérit de GLPI, l'intégration sur ce plan là lui semble réussie et lui permet de réaliser des rapport de traitement efficacement.

Sur un plan plus proche du développement, une documentation orientée technique est réalisée qui permetra au développeur suivant de mieux comprendre l'environement GLPI, la structure du code de ce dernier ainsi que l'architecture du code du plugin réalisé. Il peut être important de retenir que le code existant du plugin a été écrit par quelques bénévoles au fil du temps[8,9], certaines parties sont claires à lire et comprendre alors que d'autres parties semblent avoir été réalisées par d'autres personnes qui ont fourni un résultat moins soigné. Aussi, le code est très peu commenté, cela, avec les points énoncés précedement peuvent réelement ralentir la compréhenssion du code, il est donc nécéssaire d'avoir une documentation adaptée pour éviter la perte de temps et augmenter l'efficacité des développeurs.

5 Conclusion

L'ensembles des missions réalisées dans cette entreprise ont de mettre en place dans GLPI un module de gestions de processus de conformité RGPD, l'application est fonctionelle dans son emsemble et est hébergée.

Ce premier stage a été très enrichissant pour moi, il m'as permit de me forger une première expérience professionelle dans le milieu du développement et de l'administration système. Ceci sur un milieu teinté par la conformité, par le RGPD, qui sont des thèmatiques plutôt nouvelles qui n'existaient pas il y quelques années. L'entreprise DL Place qui m'as accueilli est en plein création et je suis fier d'avoir pu contribuer à ce lancement et participer à ce début d'aventure.

Sur un plan plus personnel, ce stage a renforcé mes capacités en autonomie, mes capacités techniques sur les technologies web. Je pense que les missions variées m'ont permit de savoir quelles sont les technologies avec le plus d'affinités, par exemple je ne souhaite pas continuer ma carrière dans le développement PHP. Et je préfère me diriger vers d'autres technologies plus récentes tout de même couplées à l'administration système. Ce mix peut éventuellement s'apparenter à un métier de devops.

6 Annexes

6.1 Figures

ONGLET				
GENERAL	TITRE	Description générale		zone de texte court
on indique pour quelles raisons & j	Finalités	Finalité 1, Finalité 2, Finalité 3, Finalité 4		zones de texte longue
	Statut	Actif / inactif		choix simple
	Diffusion	Publique / interne		choix simple
	Rédacteurs	+ AJOUTER rédacteur	rôle (DPO / responsable de traitement /	choix depuis la base Utilisateurs
	(si besoin)	+ AJOUTER rédacteur	rôle (DPO / responsable de traitement /	
	(si besoin)	+ AJOUTER rédacteur	rôle (DPO / responsable de traitement /	
	Dernière date de modification			date
BASES LEGALES	Bases légales	+ AJOUTER base légale (nom / type/ contenu)	commentaire	choix depuis la base Bases légales
indiquer les bases légales 1/ selon	*(si besoin)*	+ AJOUTER base légale (nom / type/ contenu)	commentaire	
	(si besoin)	+ AJOUTER base légale (nom / type/ contenu)	commentaire	
	Référentiel(s) suivi(s)	+ AJOUTER base légale (nom / type/ contenu)	commentaire	choix depuis la base Bases légales
	(si besoin)	+ AJOUTER base légale (nom / type/ contenu)	commentaire	
	(si besoin)	+ AJOUTER base légale (nom / type/ contenu)	commentaire	
PERSONNES, DONNEES	Catégories de personnes	+ AJOUTER catégories de personnes		choix depuis la base Catégories de personnes
RETENTION		+ AJOUTER catégories de personnes		
quelles sont les personnes concern		+ AJOUTER catégories de personnes		
	Catégories de données	+ AJOUTER catégories de données	sensible / vue comme sensible / générale	choix depuis la base Catégories de données
		+ AJOUTER catégories de données	choix simple : obligatoire / facultatif	
		+ AJOUTER catégories de données	choix simple : obligatoire / facultatif	
	obligatoire / facultatif	obligatoire / facultatiif	explication	zone de texte court
	Rétention des données	Définie par		choix parmi une base légale / le contrat / autres / non requis
		+ AJOUTER bases légales		choix depuis les bases légales ajoutées
		+ AJOUTER contrat		choix depuis les contrats ajoutés
	Commentaire	Commentaire libre		zone de texte court
	(si besoin)	+ AJOUTER catégories de personnes		
		+ AJOUTER catégories de personnes		
		+ AJOUTER catégories de personnes		
		+ AJOUTER catégories de données	choix simple : obligatoire / facultatif	
		+ AJOUTER catégories de données	choix simple : obligatoire / facultatif	
		+ AJOUTER catégories de données	choix simple : obligatoire / facultatif	
		obligatoire / facultatiif	explication	
		non requis / selon bases légales / selon contrat / autres		
		+ AJOUTER bases légales		
		+ AJOUTER contrat		
	Commentaire	Commentaire libre		

FIGURE 1 – Cahier des charges (partiel, seulement le début, le reste étant similaire)

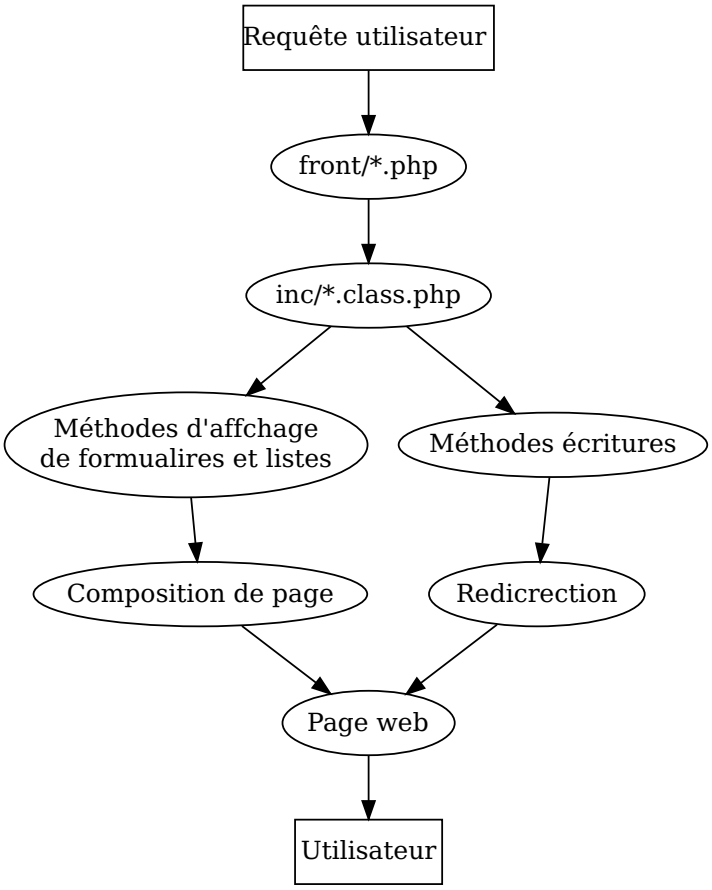

FIGURE 2 – Processus de traitement d'une requête par GLPI pour procéder à l'affichage d'une page web

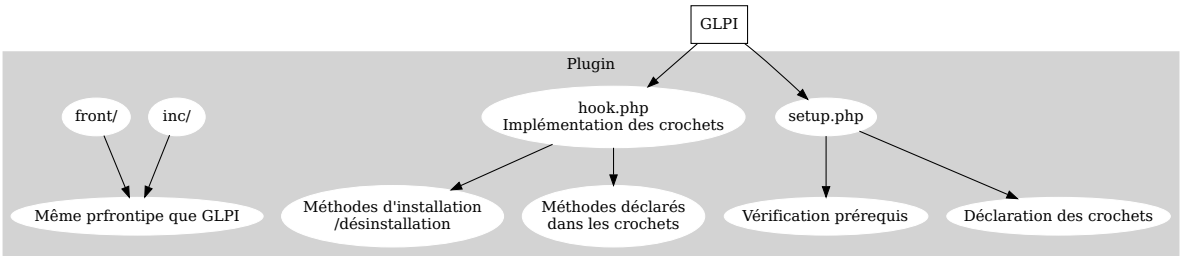

FIGURE 3 – Fonctionement d'un plugin GLPI (les plugins ont une structure similaire à GLPI avec inc/ et front/)

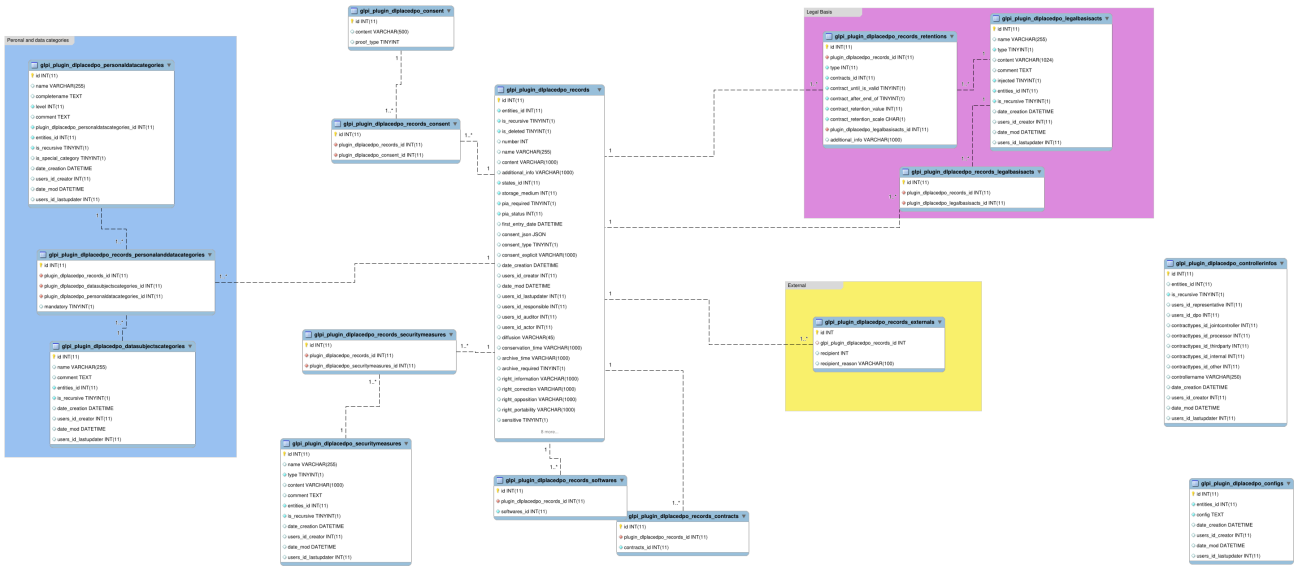

FIGURE 4 – MPD : Les tables du plugin et leurs relations sont indiquées

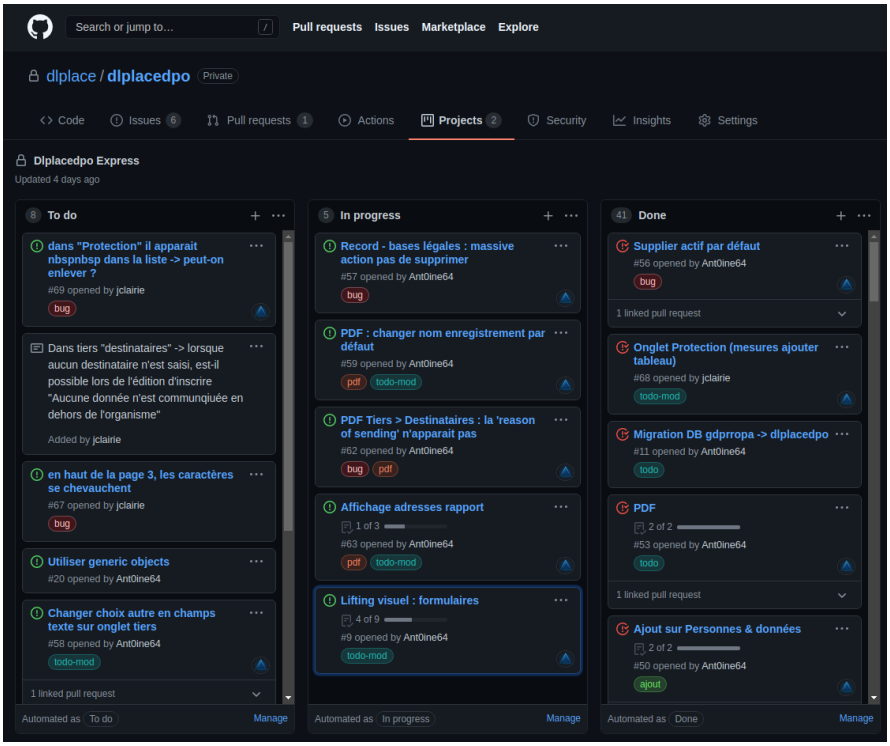

FIGURE 5 – Affichage Kanban sur l'outil de gestion de projet GitHub

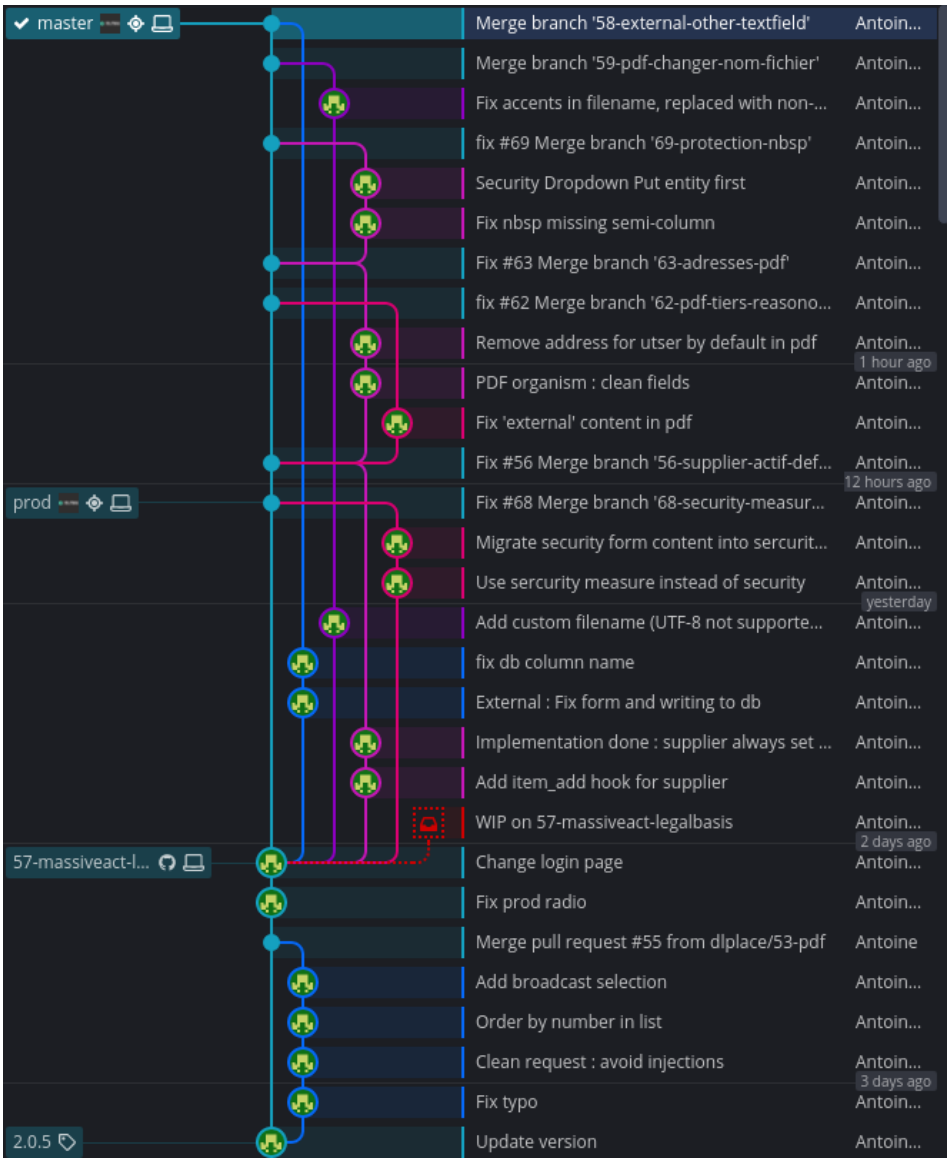

FIGURE 6 – Affichages d'une partie de l'historique des commits Git (visualisé sur le logiciel GitKraken)

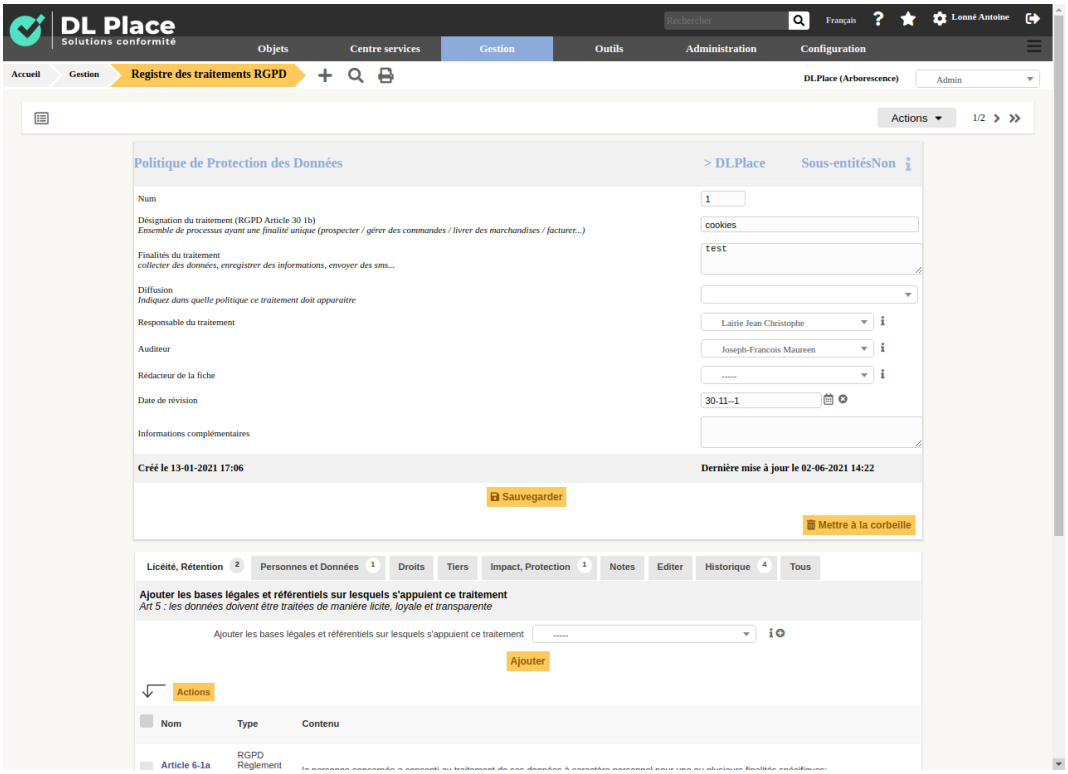

FIGURE 7 – Visuel du plugin dans GLPI lors de la modification d'un traitement

6.2 Bibliographie

1. Penny Grubb et Armstrong Takang. 2003. *Software maintenance - concepts and practice (2. ed.).*

2. Nicolas Dusserre. 2021. *L'évolution du Langage PHP ainsi que son environnement d'exploitation.* CESI Pau.Consulté à l'adresse https://cdn.discordapp.com/attachments/632219726076051456/846814541609566288/Veille_Nicolas_Dusserre_rapport.pdf.

3. Jean-Christophe Lairie et Maureen Joseph-François. 2021. DPO Register Express. DLPlace | Conformité. Consulté 6 juin 2021 à l'adresse https://www.dlplace.eu/dporegister-express.

4. Jean-Christophe Lairie et Maureen Joseph-François. 2021. DPO Register. DLPlace | Conformité. Consulté 6 juin 2021 à l'adresse https://www.dlplace.eu/dlregister.

5. Jean-Christophe Lairie et Maureen Joseph-François. 2021. DPO. DLPlace | Conformité. Consulté 10 juin 2021 à l'adresse https://www.dlplace.eu/dpo-mutualisé.

6. Jean-Christophe Lairie et Maureen Joseph-François. 2021. DL Place RGPD. DLPlace | Conformité. Consulté 14 juin 2021 à l'adresse https://www.dlplace.eu/rgpd-les-droits.

7. Antoine Lonné. 2021. *L'évolution des systèmes Linux et de l'open source dans le milieu des systèmes d'exploitations*. CESI Pau.Consulté à l'adresse https://antoinelonne.dev/Antoine_Lonné_Veille_Technologique_Linux.pdf.

8. yild. 2021. *yild/gdprropa*. Consulté 6 juin 2021 à l'adresse https://github.com/yild/gdprropa.

9. Karhel. 2021. *karhel/glpi-dporegister*. Consulté 6 juin 2021 à l'adresse https://github.com/karhel/glpi-dporegister.

10. OVH. Dernières informations sur notre site de Strasbourg. OVHcloud News. Consulté 15 juin 2021 à l'adresse https://www.ovh.com/fr/news/presse/cpl1785.dernieres-informations-notre-site-strasbourg.

11. Teclib'. GLPI ITSM Gestion de Services Informatiques. GLPI Project. Consulté 10 juin 2021 à l'adresse https://glpi-project.org/fr/.

12. Teclib'. GLPI Developer Documentation. Consulté 10 juin 2021 à l'adresse https://glpi-developer-documentation.readthedocs.io/en/latest/index.html.