Stage 3A

Anthony Barbier

Entreprise : Beijaflore
Maitre de stage : Thibaut Sylvestre

•••

Tuteur ENSIIE : Dimitri Watel

“ RGDP - Outillage d’offres de sécurité de pointe dans un modèle de fonctionnement international. ”

Plan

I - L'entreprise Beijaflore

II - Objectifs du stage et encadrement

III - Mission RGPD chez un client

I - L’entreprise Beijaflore

I - L’entreprise Beijaflore

→ Cabinet de conseil, fondé en 2000

→ Situé à Paris XVIè, d’autres locaux à Bruxelles, Rio de Janeiro, Sao Paulo, New York

→ 1200 collaborateurs

→ 3 grandes expertises : Digital, Graphène Advisory et Cyber Risk & Security

II - Objectifs du stage et encadrement

II - Objectifs du stage et encadrement

→ Stage en deux temps : au cabinet puis chez un client

→ En interne : production d'un document sur la protection des données, participation à une réunion pour préparer le "post-RGPD"

→ Mission chez un client grand compte

→ Stagiaires formés à devenir consultants

III - Mission RGPD chez un client

III - Mission RGPD chez un client

→ Client : Établissement public à caractère industriel et commercial (EPIC). Gère les infrastructures ferroviaires en France.

→ Patrimoine informationnel à protéger :

- Données
- Référentiels de maintenance et de conception
- Codes sources

→ Protéger ce patrimoine informationnel pour :

- Le valoriser
- Respecter les lois : RGPD, loi informatique et libertés, loi Lemaire, LPM...
- Encadrer sa responsabilité dans l'utilisation de ses données ou référentiels

III - Mission RGPD chez un client

→ Intégration du pôle protection du patrimoine informationnel (pôle PPI)

→ 3 principaux sujets RGPD :

- Cartographie des traitements
- Mise en place d'un registre des traitements applicatif
- Rédaction de procédures

→ Travail en autonomie

III - Mission RGPD chez un client

Cartographie des traitements

→ Obligation de tenir un registre des traitements de DCP (article 30 RGPD)

→ Chaque traitement : plusieurs informations (finalité, personnes concernées, données personnelles traitées, acteurs qui manipulent les données...)

→ Processus continu :

- Noter les nouveaux traitements conformes
- Mettre à jour les anciens (MÀJ des informations et/ou mise en conformité)

III - Mission RGPD chez un client

Cartographie des traitements

→ **Conformité des nouveaux traitements** : sollicitations de l'équipe ISP (intégration de la sécurité dans les projets) ou des chefs de projet eux-mêmes via une liste de diffusion

→ **Mise à jour des anciens traitements** : deux équipes différentes qui travaillent dessus, distribuer la dernière version à chaque modification

→ Suivi de la mise à jour globale dans un deuxième fichier

III - Mission RGPD chez un client

Cartographie des traitements

→ Étape 1 : identifier les traitements non conformes et/ou “assez vieux” qu’il faut mettre à jour

→ Étape 2 : prendre contact avec la bonne personne, préparer un atelier de mise à jour du traitement

→ Étape 3 : faire la mise à jour avec le contact

III - Mission RGPD chez un client

Cartographie des traitements

→ Concrètement : plus d'une dizaine d'ateliers de mise à jour de traitements, vérification de la suppression des données pour plusieurs dizaines de jeux concours...

→ À la fin de ma mission : mise à jour du registre presque complète (entre 90 et 95% de traitements conformes)

→ Objectif : atteindre la conformité de 100% d'ici fin 2019, et le rester !

III - Mission RGPD chez un client

Mise en place d'un registre des traitements applicatif

→ Registre "tableur" : pas adapté aux très grandes entreprises

→ Choix d'utiliser une application web d'un éditeur externe

→ Application déjà en place à mon arrivée : environnement de test & environnement de production

→ Transition progressive d'un registre "tableur" à un registre "applicatif"

III - Mission RGPD chez un client

Mise en place d'un registre des traitements applicatif

→ Travail avec les deux autres établissements du groupe : réunions, décisions communes...

→ Utilisateurs et rôles : tester puis fixer les rôles nécessaires à l'utilisation du groupe

→ Automatisation de la mise à jour des traitements : nombreux tests, rédaction d'un document récapitulatif

→ Génération d'un registre "lisible" sous forme de tableur

III - Mission RGPD chez un client

Mise en place d'un registre des traitements applicatif

→ Transition vers ce registre applicatif toujours en cours.

→ Beaucoup de tests réalisés, conclusions notées sur des documents

III - Mission RGPD chez un client

Rédaction de procédures

→ Rédaction et relecture de deux procédures : inspiration de documents mis à disposition par Beijaflore, adaptation au contexte du client, vérification avec les conseils de la CNIL sur son site internet

→ Procédure PIA (analyse d'impact relative à la protection des données) en lien avec l'article 35 du RGPD.

→ Procédure de gestion des droits des personnes en lien avec les articles 15 à 21 du RGPD

III - Mission RGPD chez un client

Rédaction de procédures

→ Procédures rédigées, en attente de validation par le pôle PPI, puis par le DPO du client

→ D'autres procédures à rédiger, par exemple procédure de contrôle par la CNIL

Conclusion

→ Stage de fin d'études d'ingénieur dans deux contextes différents : besoin d'être flexible pour s'adapter rapidement

→ Cabinet de conseil : montée en compétences sur un sujet précis, puis mise en situation chez un client

→ Apport d'une nouvelle vision sur le RGPD, d'une nouvelle manière de faire les choses

→ Grande autonomie sur ma mission, mais validation toujours nécessaire : délais supplémentaires

Merci pour votre attention