

Lettre des "Lundi de la cybersécurité" n° 95

Les "Lundi de la Cybersécurité"

Lundi 19 octobre
18h00 - 20h00

**DPO et RSSI :
enfin le grand amour ?**

Organisateurs

Pr Ahmed Mehaoua
Université Paris Cité

Béatrice Laurent

Bruno RASLE
Expert RGPD –
Formateur de DPO

Philippe Salaün
Président de l'AFCDP

Gérard Peliks

Image générée par ChatGPT

DPO et RSSI : Se complètent-ils quand ce n'est pas la même personne qui cumule les deux fonctions ?

Les **RSSI** – Responsables de la Sécurité des Systèmes d'Information - sont des employés d'origine plutôt technique, qui doivent aussi comprendre le côté juridique de la protection des données numériques. Les **DPO** - Data Protection Officers ou Délégué à la Protection des Données à caractère personnel - ont une activité plutôt juridique, avec le PDCA, mais parfois aussi technique. Les uns comme les autres ont en charge la cybersécurité de l'organisation qui les emploie : la protection des systèmes d'informations numériques pour le RSSI, la protection des données à caractère personnel pour le DPO, avec pour les deux la maîtrise des aspects techniques, humains et sociétaux pour apprécier les risques.

Parfois, comme c'est le cas par exemple pour l'intervenant du Lundi de la Cybersécurité de septembre, Cédric Cartau, RSSI et DPO du CHU de Nantes et du GHT 44, les fonctions du RSSI et du DPO sont occupées par le même expert. Mais quand ce n'est pas le cas, doivent-ils s'ignorer ou se compléter ? Et, d'un point de vue hiérarchique, à qui doivent-ils être rattachés ? A la DSI (Direction de la Sécurité de l'Information) ? Sûrement pas ! Sur ce point, RSSI et DPO ont besoin pour travailler normalement d'une grande indépendance. A la Direction Qualité ? Ça me semble être une bonne solution, C'est dans l'esprit des deux fonctions. car le RSSI et le DPO concourent tous deux à établir la sécurité de l'information en accord avec les règlements comme le RGPD, et les directives comme la NIS2.

Dans ce « Lundi de la Cybersécurité » du mois d'octobre, laissons un expert qui cumule depuis beaucoup d'années ces deux métiers et qui les enseigne, nous dire ce qu'il pense du rapprochement des deux fonctions.

Je donne la plume à Bruno Rasle

DPO et RSSI doivent travailler la main dans la main. C'est une évidence. Et pourtant, on n'observe pas systématiquement sur le terrain cette synergie qui devrait profiter à ces deux fonctions et aux organismes qui les emploient.

L'intervenant s'est intéressé très tôt à ce sujet (notamment avec une intervention lors de l'Université AFCDP 2012 intitulée « Synergie entre RSSI et CIL » et en initiant dès 2013 une conférence commune à l'AFCDP et au CLUSIF sur ce même thème).

Or deux nouveautés marquantes sont introduites par le RGPD

1. Les analyses d'impact
2. les notifications de violation de données –

Ceci pousse à une meilleure interaction entre les deux fonctions.

Au travers de l'interview de plusieurs représentants des deux métiers concernés, Bruno Rasle cherche à identifier et décrire des bonnes pratiques (si cela peut donner des idées à certains) mais aussi des situations « perfectibles », anormales ou franchement ubuesques - voire choquantes-, en tentant pour cette dernière catégorie d'identifier ce qui aurait dû être fait pour les éviter ou pour en sortir « par le haut », au bénéfice de toutes les parties.

Qui est Bruno RASLE ?



Bruno Rasle se définit comme un « monomane » de la conformité au RGPD et pratique cet art martial sous trois formes : à titre professionnel, il a été DPO mutualisé pour l'une des branches de la Sécurité sociale ; à titre bénévole, il a été délégué général de l'AFCDP pendant une douzaine d'années ; en tant qu'enseignant enfin (il forme les professionnels de la Privacy depuis 2007).

Il a également pris une part active dans la création du métier de Correspondant Informatique et Libertés (puis de Délégué à la Protection des Données). Coauteur de plusieurs ouvrages (dont "Halte au Spam", Eyrolles, 2003 et "Se préparer au RGPD", Éditions législatives, 2017), il a créé l'Université AFCDP des DPO, l'Index AFCDP du droit d'accès et le Job bord des DPO.

Bruno Rasle est également le co-auteur du code de déontologie du DPO. Ses publications sont nombreuses, dont :

- « Analyse d'impact RGPD : faut-il l'illustrer d'une matrice des risques, et si oui, laquelle ? »,
- « Communication aux victimes d'une violation de données : aller plus loin que le RGPD ? »,

- « Il faut sauver le soldat DPO ! »,
- « La sécurité des données personnelles enfin prise au sérieux ? »,
- « Faut-il être parano pour faire un bon PIA ? »,
- « La purge des données – Un effort qui en vaut la peine »,
- « PSSI : contrainte ou opportunité ? »).

Quelques minutes avec une association : l'AFCDP

Suivant la tradition de nos « Lundi de la cybersécurité », entre l'exposé des intervenants et la session questions / réponses, qui commence autour de 19 h 30, nous donnons pour une quinzaine de minutes la parole à une organisation qui opère dans l'écosystème du numérique et dans la sécurité de l'information.

La séquence des **quelques minutes avec une association**, sera animée par **le président de l'AFCDP** (Association Française des Correspondants à la Protection des Données à caractère Personnel).



Philippe Salaün, nous présentera cette association professionnelle, L'AFCDP qui rassemble plus de 6 000 professionnels impliqués dans la conformité au RGPD et à la loi Informatique et Libertés. Elle organise notamment l'Université AFCDP des DPO, des groupes de travail, conférences et webinaires. C'est un lieu d'échange de pratiques et de retours d'expérience.

L'AFCDP mène des actions de sensibilisation auprès des directions d'entreprises, des collectivités et des universités pour promouvoir le rôle stratégique de la gouvernance des données.

Demande d'inscription au lundi 19 octobre, par visio-conférence à partir de 18 h 00.



Nos « Lundi de la cybersécurité » sont gratuits et veulent vous offrir une fête technologique. Demandez votre inscription, par courriel, nous vous enverrons, un peu avant le jour de l'événement, un hyperlien pour entrer dans la visioconférence Zoom.

Les demandes d'inscriptions sont à adresser à **Béatrice Laurent** co-organisatrice de nos événements :

beatricelaurent.CDE@gmail.com

Les prénoms, noms et adresses mails des inscrits seront connus des organisateurs et communiqués aux intervenants. Si vous voulez être ajoutés à ma liste de distribution des lettres des « *Lundi de la cybersécurité* » mensuels, demandez-le-moi par mail (gerard.peliks@noos.fr).

Si vous vous inscrivez pour assister à notre évènement, soyez connectés le **lundi 19 octobre dès 18 h 00 ou mieux, un peu avant**. La salle d'attente Zoom sera ouverte aux alentours de **17 h 00** pour des conversations informelles entre intervenants et participants. Ce sont toujours d'agréables échanges qui se font avant 18 h 00.

Nos « Lundi de la cybersécurité » sont gratuits et veulent vous offrir une fête technologique. Demandez votre inscription, par courriel, nous vous enverrons, un peu avant le jour de l'évènement, un hyperlien pour entrer dans la visioconférence Zoom.



Lorsque l'organisateur des « *Lundi de la Cybersécurité* » montre du doigt le mail qu'il a envoyé pour le prochain Lundi, l'imbécile regarde le doigt.

Les autres lisent attentivement le contenu du mail, en comprennent l'intérêt, et demandent leur inscription 😊

Les demandes d'inscriptions sont à adresser à **Béatrice Laurent** co-organisatrice de nos évènements :

Gérard