Compte rendu du Lundi de la Cybersécurité du 19 octobre 2026

DPO et RSSI : enfin le grand amour ?

Présenté par Bruno Rasle

Organisé par Pr. Gérard Peliks, Béatrice Laurent et Pr. Ahmed Mehaoua
Rédigé par Rayan Al Mohaize, consultant en Cybersécurité

Table des matières

I Introduction **2**
1 Les intervenants 2
2 Le thème de la synergie entre RSSI et DPO 2

II DPO et RSSI : enfin le grand amour ? (Par Bruno RASLE) **2**
1 Point d'étape 2
2 Perceptions réciproques 2
3 Synergie et importance du facteur humain 3
4 Un manque d'effort de clarification 3
5 Quand tout va mal... 3
6 Quand tout va bien ! 4
7 Des sujets de réflexion communs 4
8 Enseignements et recommandations 5

III Présentation de l'AFCDP (Par Philippe Salaün) **5**

IV Questions / Réponses **6**

I Introduction

L'événement « Lundi de la Cybersécurité » est une série mensuelle de conférences en ligne organisée de manière indépendante par Gérard Peliks, Béatrice Laurent et Pr. Ahmed Mehaoua. Elle a pour vocation d'explorer chaque mois une thématique différente liée aux enjeux contemporains de la sécurité numérique et de la société.

1 Les intervenants

Pour animer ce Lundi de la Cybersécurité, nous avons la chance d'accueillir **Bruno Rasle**, ex DPO pour l'une des branches de la Sécurité sociale, délégué général de l'AFCDP et également une des figures ayant pris une part active dans la création du métier de Correspondant Informatique et Libertés, puis de Délégué à la Protection des Données. Il nous a fait l'honneur de partager avec nous son expérience pour mieux comprendre la coopération entre DPO et RSSI.

Par la suite, **Philippe Salaün**, nous a présenté l'AFCDP (Association Française des Correspondants à la Protection des Données à caractère Personnel), dont il est président, pour le quart d'heure des associations.

2 Le thème de la synergie entre RSSI et DPO

Le Lundi de la cybersécurité du 19 octobre 2026 portait sur la relation en interne entre le Responsable de la Sécurité des Systèmes d'Information (RSSI) et le Délégué à la Protection des Données (DPO). Bruno Rasle a présenté l'état d'avancement de ses travaux visant à démontrer l'importance de cette synergie pour la protection et la conformité des entreprises.

II DPO et RSSI : enfin le grand amour ? (Par Bruno RASLE)

1 Point d'étape

Bruno Rasle mène actuellement une étude qualitative reposant sur une quarantaine d'interviews de praticiens, qui donnera lieu à une publication début 2027. Il a choisi de restreindre son périmètre aux situations impliquant un DPO interne et un RSSI interne, et recherche encore des témoignages de RSSI qui auraient à se plaindre de leur DPO afin d'équilibrer son étude.

2 Perceptions réciproques

La relation part très souvent de stéréotypes profondément ancrés.

— **Côté RSSI :** Le DPO est fréquemment perçu comme un "gratte-papier" administratif, psychorigide, qui n'a que le RGPD à la bouche et pense que "documenter la conformité, c'est l'obtenir". Un RSSI a même avoué de façon amusante : "Moi ça

m'arrange : il dit plus souvent 'non !' que moi", sous-entendant que c'est désormais le DPO qui prend les coups et "mange tout seul à la cantine".
- **Côté DPO :** La profession est fréquemment exercée par des profils juridiques, tandis que le RSSI est vu comme un pur technicien. Les DPO estiment qu'il ne s'intéresse jamais aux personnes concernées ni aux cas d'usage, se limitant à sécuriser le contenant, et qu'il est trop souvent obligé de se plier à la volonté de sa hiérarchie (la DSI) plutôt que de défendre l'entreprise.

3 Synergie et importance du facteur humain

La synergie se définit comme la mise en commun de moyens qui se renforcent entre eux pour aboutir à un même but : c'est l'idée que 1+1=3. Aujourd'hui, cette synergie reste perfectible car elle se construit au jour le jour, de façon totalement empirique et informelle. Surtout, elle tient presque exclusivement au facteur humain. Pour que cela fonctionne, il faut une évidence, une véritable volonté de travailler ensemble et une ouverture d'esprit. Chacun doit faire un pas vers l'autre : le DPO doit se former à la technique pour ne pas s'autocensurer face aux développeurs, et le RSSI doit se former aux aspects juridiques. Le rapprochement physique (être installés dans le même bureau) est également un formidable accélérateur d'échanges.

Quant à la direction, elle bénéficie de cette synergie mais s'en désintéresse souvent : "Tant qu'on ne la dérange pas, elle nous laisse faire", confient les acteurs, même s'ils préféreraient bénéficier de son soutien et de son impulsion. Bruno Rasle suggère d'ailleurs une idée novatrice : pourquoi ne pas tenir compte de l'avis du RSSI en poste lors du recrutement du futur DPO (et inversement) pour s'assurer que le courant passera bien ?.

4 Un manque d'effort de clarification

Même quand la relation est bonne, les périmètres, les méthodes et les priorités respectifs sont rarement objectivés et définis. Les deux acteurs naviguent à vue, soit ils se marchent sur les pieds, soit ils pensent à tort que l'autre s'occupe d'un sujet, créant ainsi un dangereux trou dans la raquette.

5 Quand tout va mal...

Bruno Rasle illustre l'absence de synergie par des cas très concrets :

- **Sexisme et Analyses d'impact (AIPD) :** Une jeune DPO n'arrive pas à obtenir la participation d'un RSSI plus âgé à l'AIPD. Ce dernier fait le mort, attend tranquillement que la DPO fasse signer le document par le directeur général, pour ensuite aller voir le patron et dénigrer le travail réalisé.
- **Violations de données :** Un RSSI gère un incident de sécurité mais "oublie" totalement de prévenir le DPO. Le DPO l'apprend incidemment 15 jours plus tard à la machine à café, alors qu'une notification à la CNIL était légalement exigée sous 72h. Pire, dans un autre cas, la DSI interdit carrément à son RSSI de participer au Retex (retour d'expérience) piloté par le DPO, et refuse de lui communiquer ses propres écrits.
- **Exploitation des traces (logs) :** Le RSSI refuse de donner les durées de conservation des logs au DPO, en disant que ce ne sont pas des données personnelles.

En réalité il craint que le DPO ne l'oblige à diminuer ces durées. (Bruno Rasle rappelle d'ailleurs qu'une grande assurance risque 7 millions d'euros d'amende de la CNIL pour avoir conservé des logs 5 ans au lieu de l'année déclarée).
— **Guerre d'ego :** Un DPO, ayant réalisé une cartographie très riche des sous-traitants, propose gentiment de la partager au RSSI. On lui claque la porte au nez ; il faudra deux ans d'insistance pour que son apport soit enfin accepté.

6 Quand tout va bien !

Lorsque le RSSI et le DPO décident de s'épauler, les résultats sont remarquables :

— **Soutien mutuel face aux métiers :** L'appui du DPO a permis à un RSSI d'obtenir le budget pour un outil de test de sécurité du code. Inversement, face au syndrome "Saint Google" des développeurs (qui pensent que tout ce que fait Google est parfait), c'est la voix du RSSI jointe à celle du DPO qui a permis d'empêcher l'intégration du module reCAPTCHA, jugé totalement non conforme.
— **Solidarité budgétaire :** Chose rare, certains binômes étudient en fin d'année la possibilité de faire bénéficier l'autre de leur reliquat de budget. On a vu un RSSI financer une action de sensibilisation pour un DPO à court de budget, ou encore un DPO faire profiter le RSSI de son cabinet de conseil juridique lors d'une crise.
— **Réalisations d'envergure :** À deux, ils ont un poids immense. Ils ont notamment réussi à imposer le MFA, obtenu par contrat des correctifs de sécurité rapides de la part d'un éditeur (anticipant le CRA), ou encore convaincu la direction de fermer un site e-commerce vulnérable pendant 15 jours. Ils formalisent des doctrines communes (sur la souveraineté, ou l'évaluation des sous-traitants), obligent les métiers à étudier des alternatives "on premise" aux GAFAM, et définissent ensemble un plan d'action commun dès le lancement d'un nouveau projet pour ne pas harceler les opérationnels en posant deux fois les mêmes questions.
— **Création de valeur externe :** Ensemble, ils vont jusqu'à s'impliquer en avant-vente pour rassurer les clients et aider l'entreprise à gagner des appels d'offres.

7 Des sujets de réflexion communs

Plusieurs thématiques exigent que le RSSI et le DPO travaillent de concert :

— **Analyse de risques vs Analyse d'impact :** Le RSSI utilise la méthode EBIOS pour traiter les risques pesant sur l'entreprise, tandis que le DPO doit traiter les risques pesant sur les personnes. Ces deux approches sont complémentaires et doivent être harmonisées.
— **La Veille :** Le RSSI suit souvent les référentiels de sécurité (OWASP, NIST) mais ignore les recommandations techniques publiées par la CNIL (ex : sur la sécurisation des API en 2023). Le cas du hachage des mots de passe est frappant : le RSSI pense être à l'état de l'art avec du SHA256, alors que le DPO sait pertinemment que la CNIL a lourdement sanctionné Intersport pour ce choix précis (exigeant des algorithmes avec facteur de charge comme BCrypt).
— **La purge des données :** C'est l'intérêt commun ultime. Comme le résume Bruno Rasle : "La donnée la plus simple à sécuriser est celle qu'on a purgée". Le DPO et le RSSI doivent s'épauler pour imposer ces "nettoyages de printemps", qui sont

souvent ignorés par les métiers jusqu'à ce que les factures de stockage des éditeurs explosent.

8 Enseignements et recommandations

La synergie est extrêmement bénéfique mais terriblement fragile puisqu'elle ne tient qu'aux individus. Bruno Rasle conclut sur trois grands enseignements :

1. Les directions générales doivent cesser d'être passives et s'impliquer pour l'impulser et l'encourager (notamment via le recrutement et l'installation dans le même bureau).
2. Il est vital de clarifier le plus tôt possible les rôles, les périmètres, les priorités et de les documenter pour éviter les "trous dans la raquette".
3. La collaboration ne doit plus se faire au coup par coup. Il faut gérer cette synergie comme un véritable projet : lister les thématiques, établir un constat et formaliser un plan d'action.

III Présentation de l'AFCDP (Par Philippe Salaün)

L'AFCDP (Association Française des Correspondants à la Protection des données à caractère Personnel) soutient et défend le métier de DPO depuis 2004.

L'association regroupe aujourd'hui plus de 6 300 professionnels passionnés qui s'entraident via "Agora AFCDP", une plateforme privée qui facilite la vie de ses membres. L'AFCDP s'organise autour de 15 groupes régionaux en métropole, 3 groupes dans les DOM-TOM, et 2 groupes internationaux francophones (Belgique, Monaco).

Elle compte 6 groupes thématiques :
- Données de santé
- DPO Groupe
- IA
- Marketing Digital
- Médico-social
- Flux Transfrontières

Et 8 groupes sectoriels :
- Associations/Fondations
- Banque et finances
- Collectivités
- Formation / Enseignement
- Hôtellerie / Restauration
- Logement social
- Transports
- Retail

L'AFCDP produit de nombreux livrables gratuits mis à disposition sur son site : newsletter, RGPD annoté, fiche de poste, ou encore charte de déontologie. Elle dispose d'un

espace emploi gratuit et d'une "Place de marché RGPD" permettant de faire se rencontrer les besoins des responsables de traitement et les prestataires. L'association propose aussi des outils ludiques de sensibilisation comme le jeu de plateau "RGPD Challenge".

Son événement phare, l'Université des DPO, rassemblera 900 participants le jeudi 4 février 2027 (suivi de sessions numériques).

IV Questions / Réponses

1. **Pourquoi cette synergie n'est-elle pas davantage encouragée par les directions générales (les responsables de traitement) ?**

   Réponse de Bruno Rasle : La synergie se fait souvent à l'insu de la direction, même si c'est elle qui en bénéficie au final en termes de création de valeur (1+1=3). Il conseille aux DPO d'inclure dans leur bilan annuel un chapitre illustrant spécifiquement leurs réussites conjointes avec le RSSI, pour démontrer concrètement aux dirigeants l'intérêt de soutenir activement cette collaboration. Les règles du RGPD sont d'abord des règles de "bon sens" que les directions devraient naturellement embrasser pour protéger leurs actifs immatériels.

2. **Est-ce que l'utilisation de modules comme Google reCAPTCHA peut être rendue conforme en recueillant simplement le consentement des utilisateurs ?**

   Réponse de Bruno Rasle : Non. Un consentement, pour être valable au titre du RGPD, doit être libre et parfaitement informé. Or, avec Google reCAPTCHA, l'entreprise propriétaire du site ignore quelles données Google récupère, pour quelle finalité exacte, combien de temps elles sont conservées, ni avec qui elles sont partagées. L'information n'étant pas transparente, le consentement recueilli est invalide.

3. **Un organisme public peut-il légitimement refuser une demande de suppression de données d'un usager ?**

   Réponse de Bruno Rasle : Oui, si ces données sont nécessaires pour répondre à une obligation légale ou à un litige. L'exemple typique est celui d'un allocataire fraudeur qui demande son "droit à l'oubli" pour éviter de rembourser des prestations indues : l'organisme refusera la demande tant que la dette ne sera pas réglée, et la CNIL validera cette décision.

4. **Les recommandations de la CNIL et de l'ANSSI sont-elles cohérentes et applicables pour les directions ?**

   Réponse de Bruno Rasle : La CNIL et l'ANSSI travaillent main dans la main, il n'y a donc pas de dissonance. Avant de publier une recommandation (ex : sur la taille des mots de passe), la CNIL consulte régulièrement les associations professionnelles pour s'assurer que ses exigences techniques restent proches de l'état de

l'art et proportionnées.

5. **Comment les DPO externes s'en sortent-ils pour créer une synergie avec le RSSI interne ?**

   Réponse de Bruno Rasle : C'est une position très difficile. S'ils bénéficient parfois d'une oreille plus attentive de la direction (l'effet "consultant externe"), le DPO externe manque cruellement du contact informel du quotidien (les discussions "machine à café"). Il doit impérativement se trouver des alliés en interne pour réussir sa mission.

6. **Dans les domaines judiciaires ou régaliens (ex : contrôle des fréquences), comment gérer la conservation à long terme et la purge des données ?**

   Réponse de Philippe Salaün : On peut conserver les données personnelles tant que cela reste justifié par le métier. Au-delà, pour garder un historique statistique à long terme, les données doivent être anonymisées de façon stricte et irréversible. Dans le cas contraire, elles doivent sortir de la base "active" et être isolées dans des "archives intermédiaires" ultra-sécurisées, uniquement accessibles aux personnels en charge des contentieux.