



DPO et RSSI : enfin le grand amour ?

BRUNO RASLE – BRUNO_RASLE@HALTE-AU-SPAM.COM

LUNDI DE LA CYBER – 19 OCTOBRE 2026

Point d'étape

- ▶ Mes travaux donneront lieu à une publication **début 2027**
- ▶ **Je me focalise sur les situations « DPO interne + RSSI interne »**
- ▶ Je ne traite pas de la question **« Est-il possible d'être simultanément DPO et RSSI ? »**
- ▶ Je procède **par interviews de praticiens** (qualitatif), qui serait doublé **d'un sondage** (quantitatif) au sein de l'AFCDP
- ▶ Je suis toujours à la recherche **de témoignages de RSSI qui auraient à se plaindre de leur DPO**

Perception réciproque ?

Le DPO ? C'est un gratte papier. Il n'a que le RGPD à la bouche. Il est éloigné des réalités

RSSI



Le RSSI ? Il ne jure que par la technique... Il ne pense jamais aux personnes concernées

DPO



Verbatim RSSI

- ▶ « Notre DPO pense que documenter la conformité, c'est l'obtenir ! »
- ▶ « Il est psychorigide »
- ▶ « Moi ça m'arrange : il dit plus souvent « non ! » que moi ... »

Verbatim DPO

- ▶ « Notre RSSI ne cherche pas à comprendre les métiers de leur organisme, c'est-à-dire d'avoir connaissance de l'utilisation des données. Il se limite trop souvent à sécuriser le contenant et l'infrastructure, sans s'intéresser aux cas d'usage »
- ▶ « Comme notre RSSI est rattaché à la DSI, il est souvent obligé de se plier à la volonté de sa hiérarchie »
- ▶ « Quelques fois, on a l'impression que sa priorité est de défendre la DSI plus que notre entreprise ! »

Synergie ?

« Mise en commun de moyens qui se renforcent entre eux pour aboutir à un même but »



Synergie entre
DPO et RSSI ?

Quand elle
existe...

- ▶ Elle tient principalement **aux personnes**
- ▶ Elle se construit au jour le jour, **de façon informelle**
- ▶ Elle est souvent incomplète, **« perfectible »**

Importance du facteur humain

Verbatim

- ▶ « La synergie suppose une démarche volontaire des deux côtés, **une envie de travailler ensemble**, de partager des objectifs communs. C'est indispensable pour espérer un fonctionnement idéal de ce couple »
- ▶ « Ce qui compte, c'est la volonté de chacun de travailler avec l'autre, **de chercher à comprendre son interlocuteur**. Nous avons tous les deux l'ouverture d'esprit qui nous pousse à privilégier le travail en commun »
- ▶ « Dès son arrivée, on s'est tout de suite bien entendu. **Pour nous deux, travailler ensemble était une évidence** »

Suggestion...

- Lors du cycle de recrutement de l'un des deux acteurs...

Pourquoi ne pas tenir compte (entre autres) de l'avis de l'autre acteur ?

- **Le courant passera-t-il bien entre eux ?**

Posture de la direction ?

Tant qu'on ne la
dérange pas, elle
nous laisse faire

RSSI



Nous aurions tout de
même préféré bénéficier
de son soutien...

DPO



Chacun doit faire un pas vers l'autre

J'ai fait un effort de formation sur les aspects juridiques

RSSI



J'ai fait un effort de formation sur les aspects techniques

DPO



Les mettre dans le même bureau ?

- ▶ « Par le fait du hasard, nous avons été placés dans le même bureau, dans une zone distincte de la DSI, ce qui permet à tout salarié de venir librement échanger avec nous »
- ▶ « Nous sommes physiquement proches, ce qui facilite les échanges »
- ▶ « Nous sommes rattachés à la même direction »

Un effort de clarification ?

- ▶ **Les périmètres respectifs sont rarement objectivés et définis** (« Il nous arrive de nous marcher sur les pieds ou de penser – à tort – que l'autre s'en occupe »)
- ▶ **Même constats concernant les objectifs, les priorités, les méthodes, etc.** (« On avance de façon empirique, au cas par cas »)
- ▶ **La synergie n'est pas recherchée systématiquement, elle n'est pas exploitée à son maximum** (« On travaille main dans la main lors des violations de données mais pas pour les analyses d'impact »)



Quand tout va mal...

Vous avez dit sexisme ?

- ▶ La DPO n'arrive pas à obtenir la participation du RSSI lors des analyses d'impact
- ▶ **Celui-ci attend que la DPO fasse endosser l'AIPD au directeur général**
- ▶ **Puis il dénigre le travail réalisé ...**

Vous avez dit violation de données ?

- ▶ La RSSI traite un incident de sécurité mais oublie totalement le DPO
- ▶ **Celui-ci en prend connaissance incidemment quinze jours plus tard, alors qu'une notification à la CNIL était nécessaire**

Vous avez dit violation de données ?

- ▶ Après une violation de données, le DPO pilote un Retex et invite le RSSI (rattaché à la DSI)
- ▶ **La DSI formalise son propre Retex, interdit à son RSSI de participer à celui piloté par le DPO et refuse de communiquer ses écrits au DPO**

Vous avez dit exploitation des traces ?

- ▶ Le DPO n'arrive pas à obtenir de la part du RSSI les informations qui lui permettrait de mettre au registre le traitement des logs
- ▶ **Selon le RSSI, les logs ne sont pas des données personnelles...**
- ▶ **En fait, il craint qu'on l'oblige à diminuer leur durée de conservation**

Accepter l'aide du DPO ?

- ▶ Le DPO propose de mettre à disposition du RSSI sa liste de tiers (destinataires, sous-traitants) qu'il a identifiés et qui est bien plus riche que celle établie par le service informatique
- ▶ **Ce n'est qu'au bout de deux ans que son apport a été accepté**



Quand tout va bien !

Soutien mutuel

- ▶ La DPO a aidé le RSSI à obtenir, concernant les développements internes, **l'acquisition d'un outil permettant de valider le code sur les aspects sécurité**
- ▶ Le conseil du DPO **visant à éviter la présence d'un module reCAPTCHA de Google** n'ayant pas été entendu et devant la posture du sous-traitant en charge du développement du site (« *C'est forcément conforme, puisque fourni par Google* »), le soutien du RSSI pour obtenir gain de cause a été précieux

Budget

- ▶ À l'approche de la fin de l'exercice, **RSSI et DPO étudient la possibilité de faire bénéficier l'autre d'un reliquat sur son budget**

Budget

- ▶ Le RSSI **a pris sur son budget** une action de sensibilisation initiée par le DPO (dont le budget était épuisé)

Budget

- ▶ À l'occasion d'une violation de données, **le DPO a fait bénéficier son RSSI du support juridique de son cabinet conseil** (sur son propre budget)

Ensemble, ils
ont...

- ▶ réussi à imposer **la mise en œuvre de MFA**
- ▶ obtenu d'un éditeur externe de logiciel, par contrat, **qu'il s'engage à fournir rapidement des correctifs de sécurité**, prenant ainsi de l'avance sur l'entrée en application du CRA
- ▶ conçu **un document commun qui vise à évaluer les sous-traitants** (auparavant, chacun avait son propre document)
- ▶ obtenu de la direction **la décision de fermer durant une quinzaine de jours un site de e-commerce**. Un *white hat* leur avait signalé une vulnérabilité sur ce site, faille qui ne pouvait être corrigée à court terme

Ensemble, ils ...

- ▶ Ont réussi **à obtenir que soit étudié le traitement des données on premise** (en alternative à une offre de l'un des GAFAM)
- ▶ rédigé **une note commune pour clarifier la doctrine en matière de souveraineté** (quand il est nécessaire de la respecter strictement)
- ▶ sont impliqués dans les actions destinées à conserver les clients. Ils le sont également en avant-vente, **pour gagner de nouveaux clients**
- ▶ formalisent de concert **leur propre plan d'action en cas de lancement d'un projet** (« Comment allons-nous accompagner ce projet ? »)



Des sujets sur lesquels il
serait nécessaire de se
pencher

Analyse de risques vs. Analyse d'impact

29

J'utilise la méthode
Ebios et je traite les
risques qui pèsent sur
l'entreprise

RSSI



J'utilise ma propre méthode
et je traite les risques qui
pèsent sur les personnes

DPO



Veille : sécurisation des API



J'écoute l'OWASP API Security Top 10 et le NIST 800-204 Security Strategies for Microservices-based Application Systems

RSSI



Et la recommandation technique de la CNIL sur les API, publiée en 2023 ?

DPO

Veille : hash des mots de passe



Nous les hashons en
SHA256 avec du sel

RSSI



C'est ce que faisait
Intersport, sanctionné par la
CNIL à cause de cela

DPO

Un sujet qui devrait faire consensus, la purge des données !

- ▶ **La donnée la plus simple à sécuriser est celle qu'on a purgée**
- ▶ Purger les données dont on n'a plus besoin, c'est réduire l'exposition au risque
- ▶ Le DPO a obtenu à grande peine que des millions de vieux tickets de demande de support soient éliminés
- ▶ Succès ponctuel resté sans suite 
- ▶ Ce n'est que quand l'éditeur du service a annoncé qu'il était sur le point d'émettre une facture de plusieurs centaines de milliers d'euros compte tenu du volume de données stockées que le DPO a été entendu
- ▶ **Voici un sujet sur lequel DPO et RSSI devraient s'épauler, se soutenir**
- ▶ Opération « nettoyage de printemps » ?



Quelques enseignements à ce stade

La synergie est bénéfique

- ▶ Le plus souvent, la synergie tient aux personnes. Elle est donc fragile : **les directions devraient l'impulser, l'encourager**
- ▶ **Avis pris lors du recrutement ?**
- ▶ **DPO et RSSI rattachés à la même direction ?**
- ▶ **Installés dans le même bureau ?**

Clarifier tout ce qui peut l'être

- ▶ Pour éviter les doublons, les conflits potentiels et pire, les trous dans la raquette (effet tennis en double)...
- ▶ **Le plus tôt possible, clarifier les rôles, les périmètres, les responsabilités, les priorités, les méthodes**
- ▶ **Qui est sensé faire quoi, quand, comment et avec qui ?**
- ▶ **Documenter**

Gérer la synergie comme un projet

- ▶ Pour en tirer le maximum, plutôt que de laisser la collaboration se faire au coup par coup, la prendre à bras le corps, de façon volontariste et maîtrisée
- ▶ **Lister les thématiques qui devraient donner lieu à synergie et établir un constat**
- ▶ **Formaliser un plan d'action et définir des priorités**
- ▶ **S'inspirer de ce qui a porté ses fruits ailleurs**

Merci de votre
attention

- ▶ Publication **début 2027 de mes travaux définitifs**
- ▶ Je suis toujours à la recherche **de témoignages de RSSI qui auraient à se plaindre de leur DPO**
- ▶ **bruno_rasle@halte-au-spam.com**
- ▶ **www.linkedin.com/in/brunorasle**