SF Holding Consulting Services

Keynote d'ouverture

DPO FORUM

Jeudi 25 Septembre 2025, Lille

Qui suis-je ?

SF Holding Consulting Services

Joseph Graceffa, 51 ans

- Anciennement : Responsable sécurité de l'information chez Decathlon International (1997-1999), consultant sécurité chez Bull (1999-2000), Fondateur associé et Directeur Technique et Innovation chez Advens (2000-2013), accompagnateur de startups (accompagnement Réseau Entreprendre Nord et LMI/HODEFI), Membre d'un comité d'engagement REN, Animateur de clubs et de réseaux d'influence (CLUSIR Nord de France, R&D-SSI, Cluster CyberSécurité et Confiance Numérique)
- Actuellement :
  - Business Angel / investisseur sur la Région Hauts-de-France, accompagnateur HODEFI et REN, accompagnateur en stratégie produits numériques / marketing / services informatique
  - Président du CLUSIR Nord de France, relaie de relations entre RSSI / CIL DPO, administrations (ANSSI, Forces de l'ordre…) et autres clubs (CLUSIF, CESIN, AFCDP…)
  - RSSI délégué au sein de différentes startups, petites ESN, TPE, …
  - Directeur Technique chez Bina CyberSec qui déploie des innovations de sécurité sur le marché Français

Passionné de technologies et d'entreprenariat, d'automobiles sportives, de voyages et surtout des bonnes choses et des relations saines sur la durée !

Passionné d'IA : j'avoue ici que toutes les images de ce support ont été générées par une IA avec des prompts génériques n'entraînant aucune fuite de données et aucun risque en particulier pour l'auteur et son auditoire.

et déjà …

Au contact des CIL (vous vous en souvenez ?) depuis … pfiou …

Auprès de DPO depuis … au moins…

et là devant vous ce jour pour relater ces formidables relations DPO/RSSI maintenant saupoudrées de LCEN, RGPD, DORA, NIS2, IA Act …

on va se marrer non?

Vivement le Whisky-Act à la sauce Amora

1ère anecdote

Nous, les RSSI, quand on entendait parler des CIL …

Nous, les RSSI, quand on a compris et rencontré les DPO …

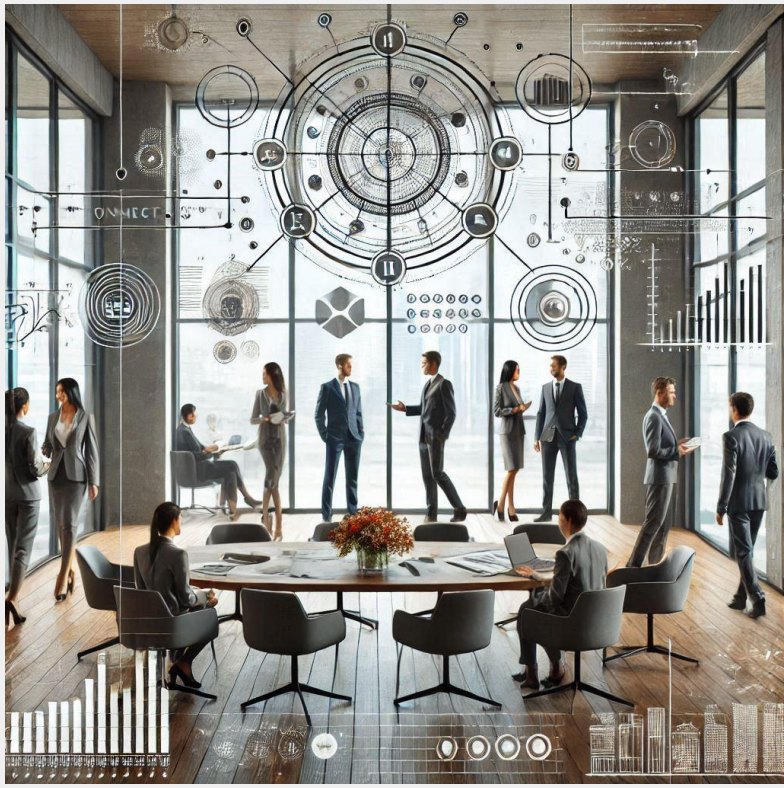
Qu’est ce qu’un RSSI ?

SF Holding Consulting Services

Responsable de la sécurité des Systèmes d’Information ou même CISO des fois!

Un positionnement varié : tantôt à la DSI, à la DAF, au CODIR ou pas …

Pour moi c’est un **faiseur de miracles !** et oui je m’appelle Joseph



Le bonheur d’être RSSI en 2025…

SF Holding Consulting Services

- **Gardien invisible** de l’entreprise : tout le monde sait que j’existe, mais personne ne veut me voir, sauf en cas de crise.
- C’est **anticiper l’imprévisible** : les ransomwares du lundi, les Dev et leur nouvelle IA du mardi, les failles 0-day du mercredi, et les fausses alertes du vendredi… le tout avec une **zen attitude** de moine Shaolin dopé au café.
- Je **jongle avec les normes** : ISO, PCI, NIS2, DORA, IA Act… Ces acronymes testent notre endurance mentale !
- Ma mission : prouver à la direction que la cyber, c’est plus fun qu’un audit, et qu’il s’agit autant de **confiance humaine** que de pare-feu et budgets.
- **Pédagogie, diplomatie** : rendre la cyber sexy pour les métiers, traduire le hacker en bullet points pour le COMEX, survivre aux mails “URGENT” à 2h du matin.
- Privilège : faire partie d’une **communauté** où tout s’invente, on **casse les codes**… ou les réinstalle en mode patch du vendredi.

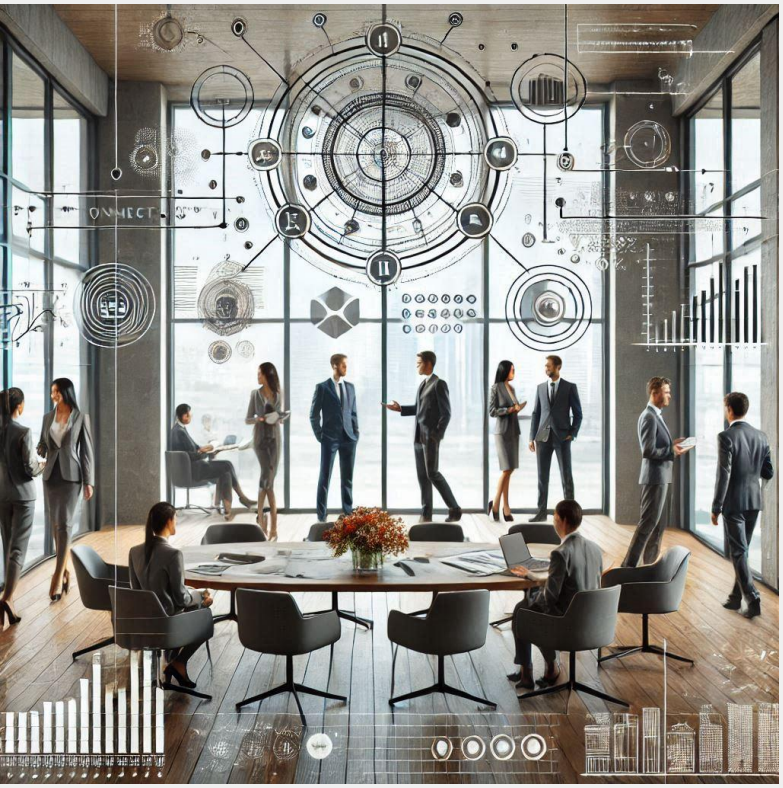
Qu’est ce qu’un RSSI ?

SF Holding Consulting Services

Bref, être RSSI/CISO en 2025, c’est partager chaque jour la formidable aventure de protéger l’essentiel :

La confiance dans le numérique !

Qu’est ce qu’un DPO ?



Data Protection Officer ou Délégué à la protection des données (DPD)

Un positionnement varié : tantôt à la DSI, à la DAF ou la Direction juridique, au CODIR ou pas …

C’est incarner le **garant de la confiance**, le **rempart de la vie privée,** l’intermédiaire éclairé entre les métiers et le juridique, parfois le **médiateur entre l’utilisateur, le hacker et le juriste…**

Le bonheur d'être DPO en 2025…

SF Holding Consulting Services

- C'est être le **grand chef d'orchestre de la conformité RGPD**, celui qu'on appelle pour arbitrer entre le business pressé, la DSI anxieuse, le juridique tatillon et l'utilisateur inquiet… mais qu'on oublie aussitôt la crise passée !
- C'est **jongler au quotidien avec le RGPD**, le DORA, la NIS2, l'IA Act, la LCEN… et les **acronymes** en mode Scrabble qui changent tous les six mois au gré des publications, jurisprudences et autres amendes record !
- C'est **expliquer à tout le monde** que « non, la donnée ce n'est pas juste un fichier Excel sur le drive », et que « oui, il faut demander l'avis du DPO AVANT d'envoyer la base tout court, pas APRÈS la fuite… »
- C'est médiatiser la **privacy** dans une entreprise où tout le monde veut **« plus d'agilité »,** mais **moins de contraintes…**
- Tempérer les marketeurs, canaliser les juristes, rassurer les boss — et éviter d'être vu comme "flicaillon" **ou traître à la cause !**
- C'est (essayer de) rendre sexy la **sécurité des données personnelles** à coup de formations, d'affiches dans les ascenseurs et de cafés/découverte RGPD… le tout en gardant le sourire, malgré les « oh ça va, on n'a rien à cacher ».
- C'est **se demander tous les jours pour qui tu travailles :** la CNIL, ta boîte, les clients, les salariés, ou cette fameuse « confiance numérique ».

Qu’est ce qu’un DPO ?

SF Holding Consulting Services

Bref, être DPO en 2025, c’est partager chaque jour la formidable aventure de protéger l’essentiel :

la confiance humaine dans le numérique !

et d’avoir donc un petit truc en plus

finalement les mêmes C-ombats …

SF Holding Consulting Services

Le RSSI, c'est les 4 C :

- Cartographier ses risques, et concevoir sa politique de sécurité
- Contrôler la bonne application de ses politiques
- Communiquer pour convaincre
- S'assurer de la conformité de l'Entreprise

Le DPO a d'autres C :

- Cartographier les traitements sur les données personnelles
- Concevoir une politique de conformité à la protection des données
- Contrôler l'application des principes de protection adaptés
- Communiquer pour convaincre

finalement les mêmes C-ombats …

SF Holding Consulting Services

Le RSSI, c'est les 4 C :

- Cartographier ses risques, et [illegible] politique
- Contrôler [illegible] applicatio politiques
- Commun convainc
- S'assurer de la conformité de l'Entreprise

Le DPO a d'autres C :

- Cartographier les [illegible] sur les [illegible]sonnelles [illegible]e politique [illegible]é à la [illegible]s données [illegible]plication [illegible]s de protection adaptés
- Communiquer pour convaincre

et un grand C en commun :

COLLABORER

En fait tout est lié …

SF Holding Consulting Services

Ici notre RSSI heureux …

Sécurité de l'information

- Formation / Sensibilisation à la cyber sécurité
- Gestion des risques
- Gestion des actifs
- Politiques de sécurité
- Gestion des incidents de sécurité
- Gère une conformité (ISO, DORA, NIS2…)

RSSI : "DoctorNO" / tech / geek / firewalls / hackers (ou lui-même un ancien hacker)

Ici notre DPO heureux …

Protection des données personnelles

- Cartographie des traitements et PIA
- Respect des droits des personnes (accès, effacement, consentement…)
- Gestion du RGPD, IA Act, CNIL, privacy by design
- Dialogue avec les autorités, gestion des requêtes internes
- Sensibilisation privacy

DPO : "juriste" / médiateur / RGPD / "agent de la CNIL" / utilisateurs & usagers

Culture de la sécurité et de la confidentialité

Valorisation de la confiance

Sensibilisation et formation

Collaboration : incidents/violations, audits, projets transverses

Ils travaillent donc ensemble…

SF Holding Consulting Services

Face à toutes les évolutions des risques, des menaces et des réglementations / obligations … ils ont dû se mettre à :

1/ Se parler … sont tous les 2 dans le même bateau

2/ Partager / échanger … pour arriver à sortir des silos

3/ S'épauler / s'aider … pour convaincre

Parfois, le RSSI porte aussi la casquette DPO…

face aux nouveautés …

SF Holding Consulting Services

Coup de chance : les RGPD, NIS2, DORA, IA-Act convergent sur pleins de points :

- besoin de cartographier, adapter les mesures à la menace, respecter des cadres et des règles ou même des bonnes pratiques…
- des textes obscures au début :-)

Coup de bol : ces obligations convergent sur la maîtrise des risques (atteintes aux données personnelles, résilience, éthiques, confiance, gestion des tiers, souveraineté …)

et le **DPO “juriste” est le meilleur ami du RSSI “geek” qui ne veut pas être vu comme le DoctorNo… car il n’a plus le choix !**
LE RSSI EN A MARRE DE MANGER SEUL A LA CANTINE !

et le **RSSI “super héro / toujours pas DoctorNo” qui vole à la rescousse du DPO à la première violation de données, au premier audit CNIL ou NON conformité; car il le vaut bien… ET IL VEUT UN AMI AVEC QUI MANGER A LA CANTINE !!**

RSSI, DPO…
UNISSONS-NOUS !

SF Holding
Consulting
Services

SF Holding
Consulting
Services

SCAN ME

Gardons contact !