

4 Saisons de la Data

DPO & RSSI : une vision binoculaire pour une homologation de sécurité renforcée.

Découvrez notre approche complémentaire dans le secteur hospitalier : une méthodologie éprouvée et adaptable à votre contexte.

- En tant que DPO, j'identifie les risques juridiques et réglementaires.
- En tant que RSSI, j'identifie les risques techniques

***« Ensemble, nous créons une sécurité à 360 °
En mettant ces différents constats en relation »***



Vos intervenants

Le Groupement Hospitalier de Territoire (GHT) Savoie-Belley regroupe 7 établissements publics de santé :

CH Métropole Savoie (établissement support) / CHS de la Savoie / CH Bugey Sud / CH d'Albertville-Moutiers / CH Michel Dubettier / CH Vallée de la Maurienne / CH Bourg St Maurice.

Objectifs principaux du GHT :

- **Coordonner** la prise en charge continue et le parcours médical des patients
- **Mutualiser** les équipes médicales et répartir les activités entre établissements
- **Optimiser** l'orientation des patients et l'accès aux soins sur tout le territoire
- **Partager** les fonctions administratives et logistiques



André PILLON : RSSI du GHT Savoie-Belley et membre du Club RSSI Santé



Thomas LADANT : DPO du GHT Savoie-Belley et membre du réseau des DPO hospitaliers



Le GHT regroupe
8000 agents



Contexte & postulat de départ



Exigences réglementaires

RGPD, PGSSI-S, SecNumCloud, IA Act... Les normes se multiplient rapidement.



Perception cloisonnée

L'homologation de sécurité reste perçue comme une démarche technique isolée ou subie.



Notre proposition

Transformer l'homologation de sécurité en levier commun DPO/RSSI.

« Concevoir de façon unifié évite le dédoublement d'actions correctrices »

Notre méthode : une vision binoculaire

L'approche mutualisée

- Combine la focale sécurité (RSSI) et conformité (DPO)
- Lecture croisée des exigences
- Réduction des angles morts
- Meilleur pilotage des projets.

Un DPO, un RSSI : deux acteurs, un même bureau



« L'homologation en monocle, c'est dépassé. Mettez vos jumelles. »

Les deux champs de vision : DPO & RSSI

Champ de vision du RSSI	Champ de vision du DPO
l'analyse de risques	l'analyse d'impact sur la vie privée
les référentiels techniques du numérique	le cadre juridique du numérique
le contrôle d'accès	le droit d'en connaître
les objectifs fonctionnels du SI [DICT]	les exigences du droit
les biens supports de l'établissement (serveurs, PC, réseaux)	les sources de données (stockage, hébergement)
les utilisateurs	les destinataires
les applications et services informatiques	les traitements d'information
les vulnérabilités techniques et organisationnelles	les éléments (données) sensibles
Droit des utilisateurs sur le SI	Responsabilités individuelle des utilisateurs

« Le RSSI sécurise ce que personne ne lit. Le DPO encadre ce que tout le monde contourne. »

Quand les visions se rejoignent



Sécurisation dès la conception

Intégration des exigences de sécurité et conformité dès l'amont des projets.



Voix unifiée

Position renforcée et cohérente auprès des directions et éditeurs, grâce à une approche commune.



Homologation stratégique

Transformation de l'homologation en un levier proactif d'amélioration continue et de valeur.

« La direction voulait une solution rapide. On leur a construit un cadre pérenne. »

Convergence dans les documents cadres



Chartes informatiques

Règles d'usage claires et cohérentes.



Politiques administrateurs

Droits et responsabilités alignés.



Gouvernance IA

Cadre éthique, juridique et sécurisé.

« Quand la technique et le droit s'accordent, les chartes deviennent des leviers pour avancer. »

Sensibilisation : 1 message, 2 angles

Fiches pratiques et supports de formations co-rédigés

- Phishing
- Mots de passe
- Télétravail
- Utilisation des espaces de stockage
- Fraude au président



- Former en duo, c'est impacter deux fois plus.
- Mieux expliquer les exigences techniques au regards des obligations réglementaires

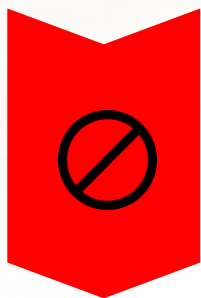
« des exigences de sécurité sans sensibilisation, c'est utiliser des ingrédients sans suivre de recettes. »

Quand notre binôme tranche



Feu vert

Participation conjointe au choix de notre futur DPI.
Exigences RGPD et sécurité respectées.



Feu rouge

Refus de l'hébergement CD73. Risques HDS et RGPD avérés.



« Dire non, c'est aussi protéger ceux qui ne savent pas encore pourquoi ils nous remercieront. »

L'homologation se joue dès à présent en binôme

Deux leviers stratégiques

DPO et RSSI ne sont pas deux cases à cocher.

Outil de transformation

L'homologation devient stratégique quand elle est pensée à deux.

Méthode duplicable

Osez la double authentification humaine.

« On est peut-être chiants... mais personne n'est jamais revenu nous dire qu'on avait eu tort de travailler ensemble »

