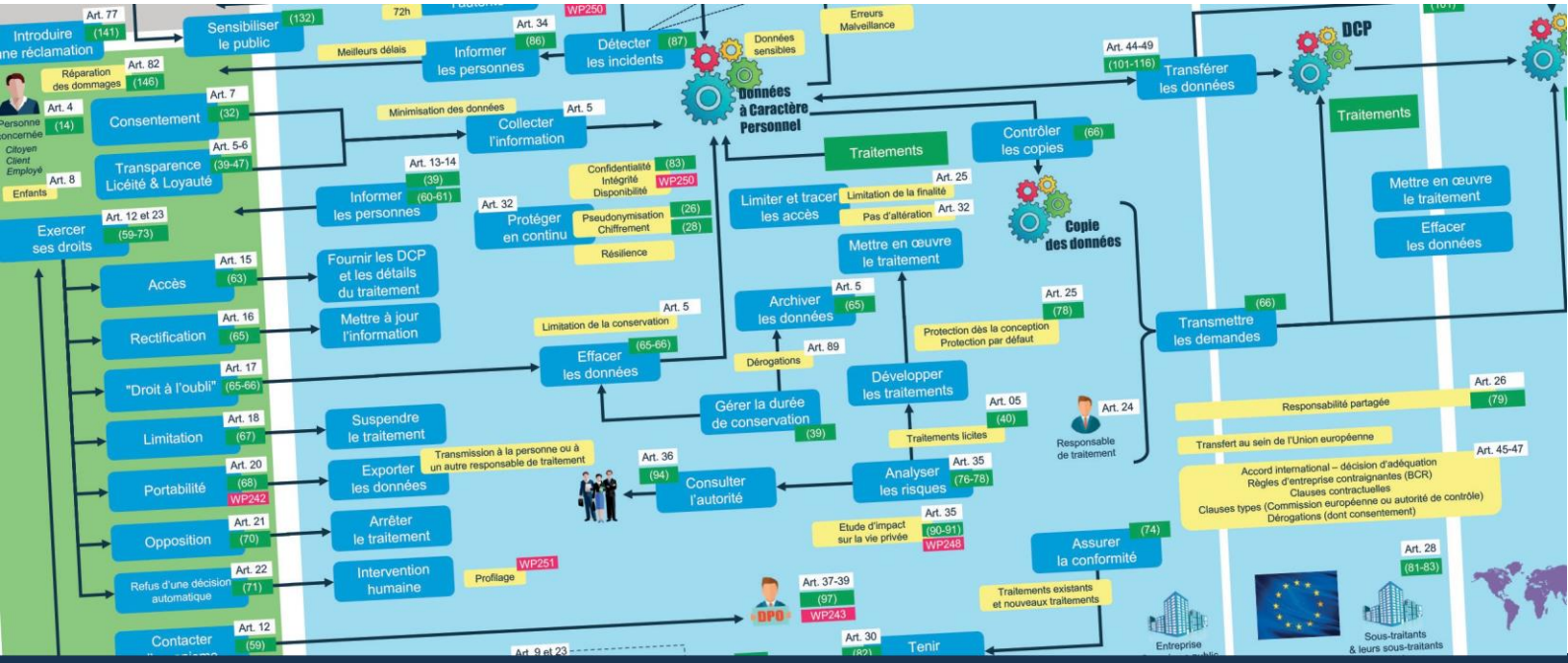
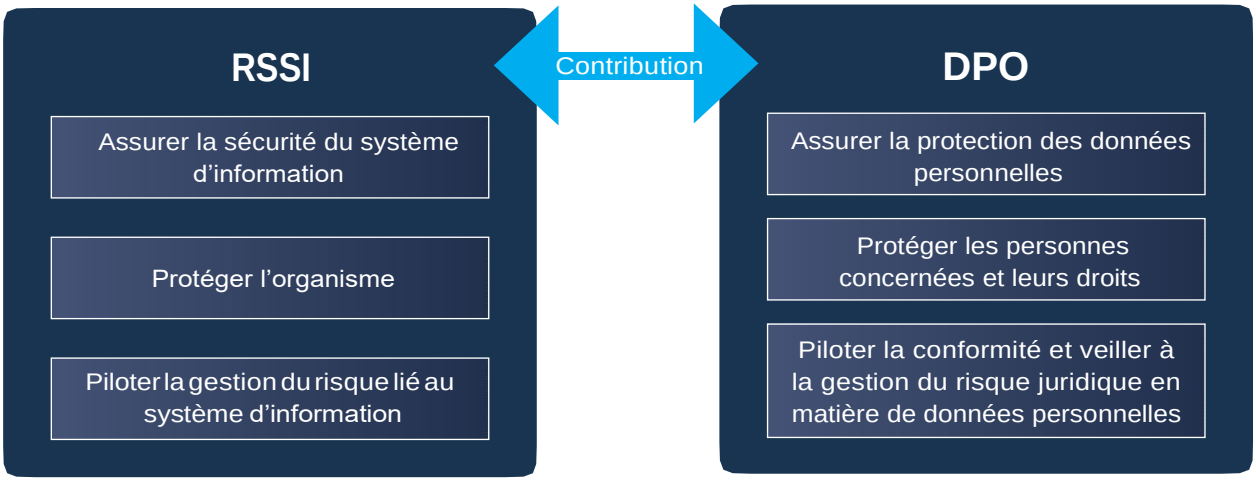
LES FICHES PRATIQUES du CLUSIF - RGPD



SYNERGIES ENTRE LE RSSI ET LE DPO

1. PÉRIMÈTRE ET OBJECTIFS

Le RSSI et le DPO sont deux chefs d'orchestre devant jouer la même partition, avec pour mission la préservation de l'organisme dans le respect des textes législatifs et règlementaires. La partition est celle initiée par le responsable de traitement (RT) mais avec des objectifs à court terme et des périmètres qui ne se recoupent pas toujours.



À première vue, ces deux acteurs n'ont pas le même objectif. Pourtant leurs missions sont similaires : préserver l'organisme des risques qui pèsent sur lui et sur les données qu'il manipule. La synergie entre ces deux acteurs est donc indispensable.

[1] Par organisme, on entend entreprises, établissements publics, associations…

2. MISSIONS ET SUJETS COMMUNS

Le RSSI doit garantir la sécurité logique et physique du système d'information. Tout comme le DPO, sa fonction est transverse. Le RSSI se préoccupe de la gestion des risques liés au système d'information, le DPO de celle liée à la protection des données personnelles. Ils se rejoignent sur le respect des principes de disponibilité, d'intégrité, de confidentialité des données, mais aussi sur la traçabilité des opérations afin de respecter les obligations de preuve et d'*accountability* qui s'imposent à leur organisme.

Le DPO et le RSSI doivent contribuer de manière complémentaire à la définition des méthodes d'identification et d'évaluation des risques en élaborant un référentiel commun, ainsi qu'aux actions de maîtrise de risques. Pour les entreprises qui avaient un CIL, cette bonne pratique est peut-être déjà existante, elle sera primordiale avec la nomination de ce nouvel acteur et les responsabilités qu'il aura à exercer.

Dans le cadre de leurs missions, les RSSI et DPO sont amenés à travailler de façon transverse au sein de l'organisme. Leurs sollicitations peuvent être mal perçues par les collaborateurs et chronophages pour l'organisme si elles ne sont pas mutualisées entre ces deux acteurs : il leur faudra partager l'information et mettre en place des processus communs.

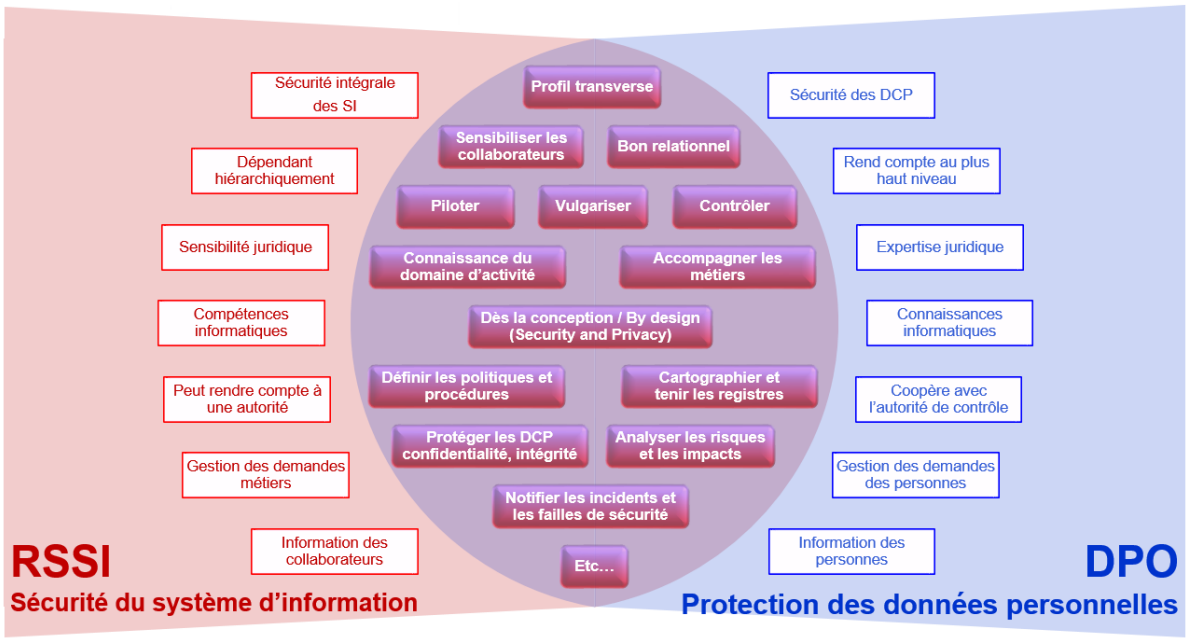


Figure 1 – Missions du RSSI et du DPO

3. CUMUL DES MISSIONS ENVISAGEABLE ?

Rien ne s'oppose à ce qu'un RSSI assure les missions de DPO. Toutefois il est important de tenir compte de son profil (expérience et compétences juridiques…) et des spécificités de son organisme.

Les éléments relatifs au DPO et à la notion de conflit d'intérêt sont abordés dans la fiche consacrée au DPO.

4. OUTILS COMMUNS ?

La gestion des risques sur les données personnelles pourra s'appuyer sur une méthode de gestion des risques déjà existante dans les organismes. Les méthodologies internes prendront en compte le critère de protection des données personnelles.

La CNIL a défini des guides permettant d'étudier les risques et leurs impacts vis-à-vis des personnes concernées, ainsi qu'un catalogue de mesures pour traiter les risques. Ces guides[2], découlant de la méthodologie EBIOS de l'ANSSI permettent une forte synergie avec l'analyse de risque du système d'information.

Le club EBIOS a aussi réalisé un cas pratique sur la géolocalisation des véhicules d'entreprise[3] et sur les impacts différenciés[4].

De plus, la mise en place des mesures recommandées dans la norme ISO/IEC 27001 va permettre au DPO en sus du RSSI d'avoir un catalogue de mesures de sécurité. Ces mesures techniques et organisationnelles permettront de réduire les risques sur le SI dont ceux pouvant avoir un impact sur la vie privée.

La CNIL, dans ses guides, fait ainsi bien le parallèle avec cette norme entre les mesures liées à la protection de la vie privée et les mesures pour la sécurité de l'information.

Ci-après un tableau repris du guide PIA-2 et enrichi des correspondances aux chapitres de la norme ISO/IEC 27002:2013

Thèmes	Mesures - guides PIA-2 (CNIL)	Norme ISO/IEC 27002 :2013
1. Mesures de nature juridique (obligatoires)	Finalité : finalité déterminée, explicite et légitime	18. Conformité
	Minimisation : réduction des données à celles strictement nécessaires	18. Conformité
	Qualité : préservation de la qualité des données à caractère personnel	18. Conformité
	Durées ou critères de conservation : durée nécessaire à l'accomplissement des finalités, à défaut d'une autre obligation légale imposant une conservation plus longue	18. Conformité
	Information : respect du droit à l'information des personnes concernées	18. Conformité
	Consentement : obtention du consentement des personnes concernées ou existence d'un autre fondement légal justifiant le traitement	18. Conformité
	Droit d'opposition : respect du droit d'opposition des personnes concernées	18. Conformité
	Droit d'accès : respect du droit des personnes concernées d'accéder à leurs données	18. Conformité
	Droit de rectification : respect du droit des personnes concernées de corriger leurs données et de les effacer	18. Conformité
	Transferts : respect des obligations en matière de transfert de données en dehors de l'Union européenne	18. Conformité
	Formalités : définition et accomplissement des formalités préalables applicables au traitement	18. Conformité
2. Mesures organisationnelles	Organisation	6. Organisation de la sécurité de l'information
	Politique (gestion des règles)	5. Politiques de sécurité
	Gestion des risques	6. Organisation de la sécurité de l'information

[2] https://www.cnil.fr/fr/gerer-les-risques ; on peut aussi se reporter aux fiches pratiques issues du guide https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles

[3] https://www.club-ebios.org/site/documents/ClubEBIOS-EtudeDeCas-Geolocalisation-2017-03-17-Approuve.pdf

[4] https://www.club-ebios.org/site/documents/ClubEBIOS-ImpactsDifferencies-2017-02-19-Approuve.pdf

Thèmes	Mesures - guides PIA-2 (CNIL)	Norme ISO/IEC 27002 :2013
	Gestion des projets	6. Organisation de la sécurité de l'information 14. Acquisition, développement et maintenance des systèmes d'information
	Gestion des incidents et des violations de données	16. Gestion des incidents liés à la sécurité de l'information
	Gestion des personnels	7. Sécurité des ressources humaines
	Relations avec les tiers	15. Relations avec les fournisseurs
	Maintenance	12. Sécurité liée à l'exploitation
	Supervision (audits, tableaux de bord…)	12. Sécurité liée à l'exploitation 18. Conformité
	Marquage des documents	8. Gestion des actifs
	Archivage	12. Sécurité liée à l'exploitation 17. Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité
3. Mesures de sécurité logique	Anonymisation	18. Conformité
	Chiffrement	10. Cryptographie
	Contrôle d'intégrité	12. Sécurité liée à l'exploitation 13. Sécurité des communications
	Sauvegardes	12. Sécurité liée à l'exploitation
	Cloisonnement des données	13. Sécurité des communications
	Contrôle d'accès logique	9. Contrôle d'accès
	Traçabilité	12. Sécurité liée à l'exploitation
	Exploitation	12. Sécurité liée à l'exploitation
	Surveillance (paramétrages, contrôles de configurations, surveillance en temps réel…)	12. Sécurité liée à l'exploitation
	Gestion des postes de travail	12. Sécurité liée à l'exploitation
	Lutte contre les codes malveillants (virus, logiciels espions, bombes logicielles…)	12. Sécurité liée à l'exploitation
	Protection des canaux informatiques (réseaux)	13. Sécurité des communications

Thèmes	Mesures - guides PIA-2 (CNIL)	Norme ISO/IEC 27002 :2013
4. Mesures de sécurité physique	Éloignement des sources de risques (produits dangereux, zones géographiques dangereuses…)	11. Sécurité physique et environnementale
	Contrôle d'accès physique	11. Sécurité physique et environnementale
	Sécurité des matériels	11. Sécurité physique et environnementale
	Sécurité des documents papier	11. Sécurité physique et environnementale
	Sécurité des canaux papier	11. Sécurité physique et environnementale
	Protection contre les sources de risques non humaines (feu, eau…)	11. Sécurité physique et environnementale