Club de la sécurité de l'information français

CLUSIF

Genèse et travaux du GT « Quelle synergie et quel partenariat entre RSSI et DPO »

Dominique SOULIER (Agence de la biomédecine)
Thierry MATUSIAK (IBM)

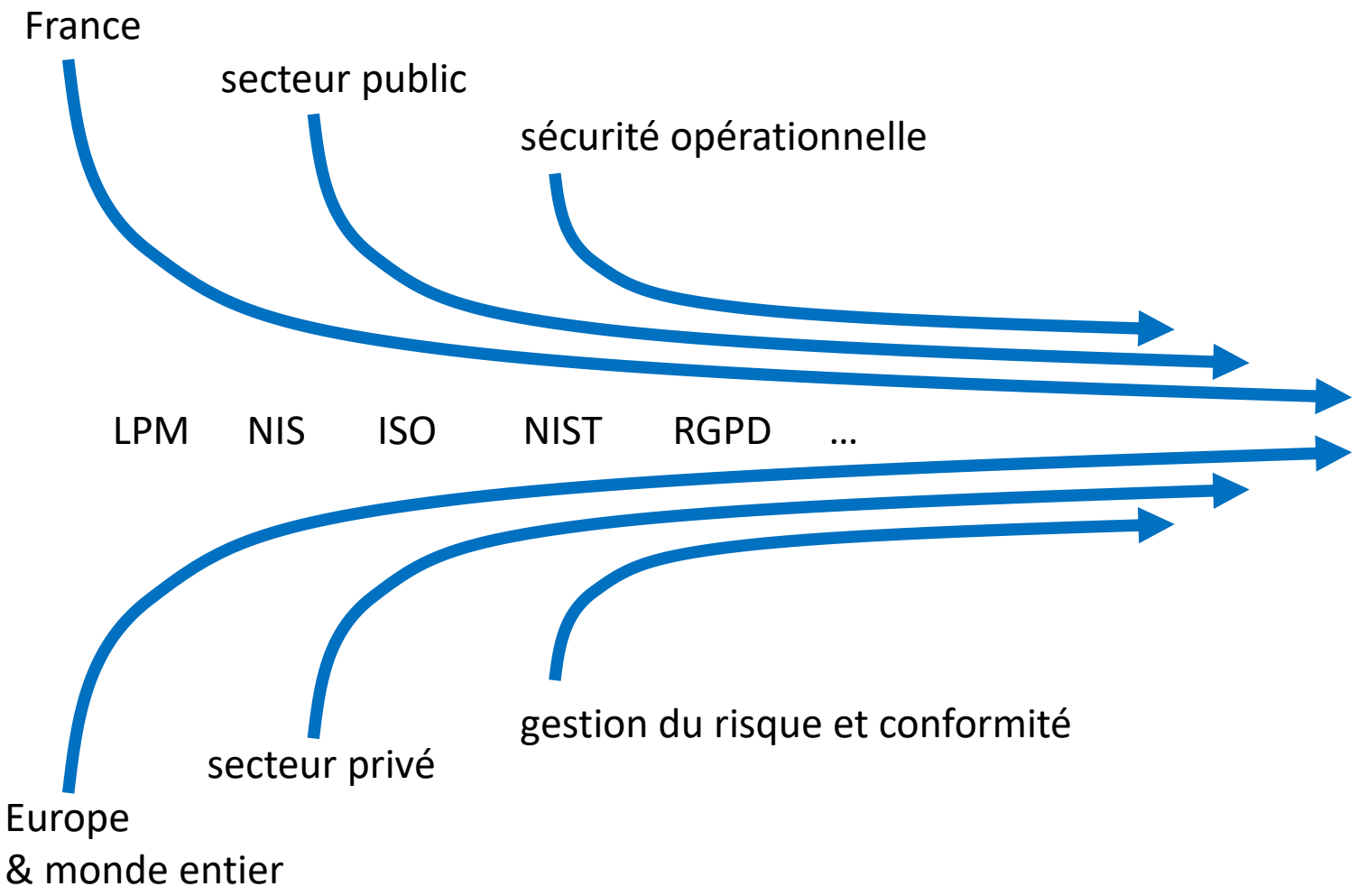
Le GT : historique & chiffres

- Issu des questions au sein de l'Espace RSSI, démarré fin 2016
  - 15 réunions depuis le 09/12/16 sur la base de réunion mensuelle
- Participants
  - 32 participants au total
  - 12 participants en moyenne à chaque réunion
- Lieu d'échange
  - Richesse des participants : RSSI, CIL, spécialistes techniques, juristes, avocats, …
  - Des réunions intéressantes et des discussions animées
- Travaux initiaux autour du profil du DPO :
  - annonces recrutement + fiches de poste + offres de formation

Le GT : les participants

David BARLOY	*MINISTERE DES ARMEES*	**Pierre-Emmanuel LERICHE**	*REXEL DEVELOPPEMENT SAS*
Isabelle BLOISE	*HERVE SCHAUER CONSULTANTS*	**Garance MATHIAS**	*MATHIAS AVOCATS*
Patrick BLUM	*ESSEC BUSINESS SCHOOL*	**Thierry MATUSIAK**	*IBM*
Daniel BRESSAN	*APPRENTIS D'AUTEUIL*	**Sophie MICHAS**	*GIE AGIRC-ARRCO*
Jean CHERIN	*HERVE SCHAUER CONSULTANTS*	**Amélie PAGET**	*HERVE SCHAUER CONSULTANTS*
Delphine DE SAINT CYR	*BOURSE DIRECT*	**Jean-Michel PATER**	*AIR CARAIBES*
Jérémy DERNONCOURT	*GIE AGIRC-ARRCO*	**Thierry PERROTIN**	*ENGIE*
Lumena DULUC	*CLUSIF*	**Thierry PERTUS**	*CONIX*
Afaf FAFI	*CONIX*	**Clara PETIT**	*ITEANU AVOCATS*
Benoit FUZEAU	*CASDEN BANQUE POPULAIRE*	**Ludovic PETIT**	*ALTRAN TECHNOLOGIES SA*
Stanislas GÉRARD	*MINISTERE DES ARMEES*	**Emilie SAINZ**	*SESAN*
Yeldy GUSTAVE	*IMS NETWORKS SAS*	**Hervé SCHAUER**	*HERVE SCHAUER CONSULTANTS*
Clothilde HACHIN	*AGENCE NATIONALE DE SANTE PUBLIQUE*	**Betty SFEZ**	*CABINET SFEZ AVOCATS*
Florence HANCZAKOWSKI	*CLUSIF*	**Dominique SOULIER**	*AGENCE DE LA BIOMEDECINE*
Didier HENIN	*BUT INTERNATIONAL*	**Isabelle THOMAS**	*ON-X SÉCURITÉ NUMÉRIQUE*
Fabrice IDIER	*CONSEIL DEPARTEMENTAL DE LA SEINE-SAINT-DENIS*	**Thomas VAN DEN HEUVEL**	*AGENCE DE LA BIOMEDECINE*

Une constatation majeure : la sécurité converge



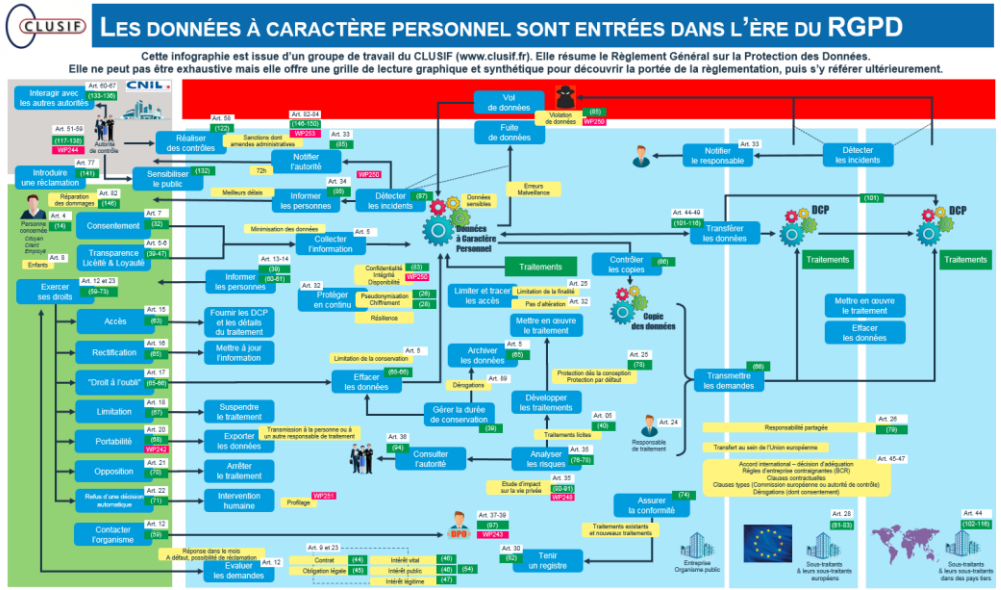
Démarche cohérente & pluridisciplinaire

RSSIs
CILs / DPOs
Avocats
Juristes
Spécialistes techniques
…

Premier livrable : une infographie

88 pages
173 considérants
99 articles

- Le RGPD est une réglementation complexe
- Notre objectif : faciliter et homogénéiser la lecture du règlement
- Un poster A2 distribué au FIC et au CLUSIF [+ pdf téléchargé plus de 5000 fois]



https://clusif.fr/publications/infographie-donnees-a-caractere-personnel-entrees-lere-rgpd/
https://clusif.fr/publications/infographic-personal-data-has-entered-the-gdpr-era/

Deuxième livrable : une FAQ

- En cours de finalisation
- Notre objectif : répondre à des questions précises et concrètes
- Une livraison progressive du contenu (à venir)

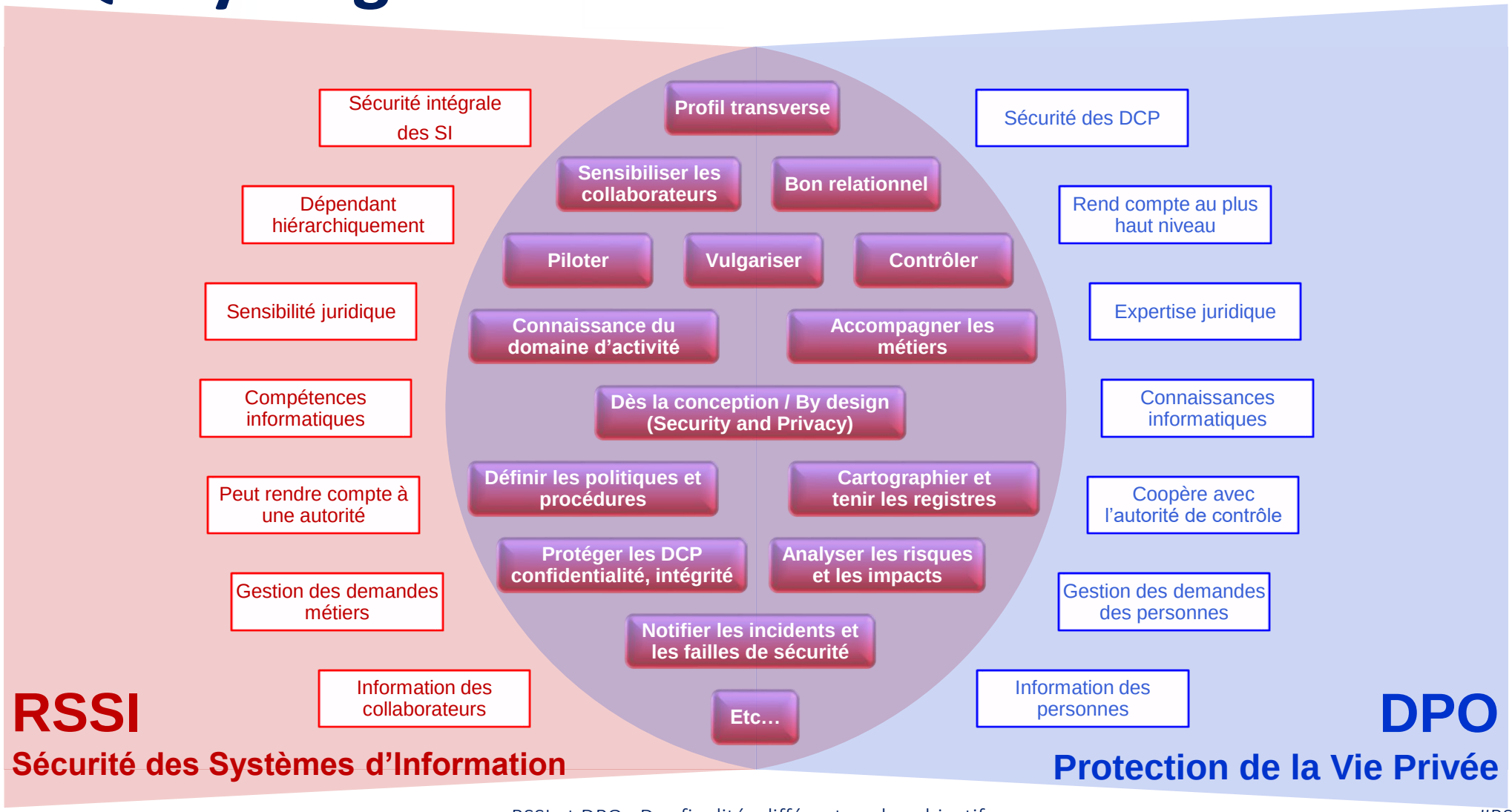
Qui est responsable de traitement ?
Quels sont les principes fondamentaux du règlement ?
Qu'est-ce qui change avec le RGPD ?

Comment réaliser un PIA ?
Comment gérer les transferts de données ?
Quelle responsabilité pour les sous-traitants ?

Quel est le rôle du DPO ? Quelles sont ses missions ?
Peut-on cumuler les missions ?
Quelles synergies DPO / RSSI ?

Club de la sécurité de l'information français

FAQ : Synergies RSSI et DPO



FAQ : autres exemples

- Cas de conflits d'intérêts
  - Lignes directrices du G29 concernant les délégués à la protection des données
  - Dans le cas du RSSI : distinguer RSSI « opérationnel » et RSSI « pilotage »

- Pour chaque thème abordé dans la FAQ, quand cela s'y prête, un focus « Du point de vue du RSSI »

Qu'est-ce qu'un traitement de données à caractère personnel ?

Du point de vue du RSSI :
Certains traitements (contrôle de la messagerie, de l'usage d'internet, …) prévus pour la protection de l'organisation, peuvent engendrer un risque pour les droits et libertés individuelles des collaborateurs. Il est important de recenser et d'analyser ces traitements induits par la sécurité au même titre que les traitements métiers de l'organisation.

Les suites

- Un GT qui souhaite poursuivre ses travaux au-delà du 25 mai
- La nouvelle loi Informatique et Libertés

- Travail qui se poursuit sur la FAQ avec une livraison itérative
- Une v2 de l'infographie en projet