CIPI Club Informatique Pour l'Immobilier

Les ateliers du CIPI

13 février 2018 10h-12h30

RGPD (2)

Chez SWISSLIFE REIM
153 Rue Saint Honoré , Paris 1er

Atelier préparé par :

- **Pour le CIPI:**
  - Philippe MINIER, DSI KAUFMAN & BROAD,
  - Henri BRAHY, HB CONSEIL
  - FCA Consulting

- **Intervenants:**
  - **Vision Infrastructure/data** :
  - Yann VALAINS , Président , ARCITEK
  - Yvan LANZADA, Hermitage Solutions
  - Christophe BADOT, Country Manager, VARONIS

  - **Vision Pilotage/ AMOA**
  - **Ol**ivier MARTIN (ATEPS / Privacy On Track)

1 – Introduction

- **1er atelier RGPD en juillet 2017 (Jean Maxime PEYRAT, H&P Avocats)**
  - Les textes et le plan d'action préconisé.

- **Le RGPD, Problème complexe:**
  - ✓ Interconnexion des sujets/acteurs
  - ✓ Encore des zones d'interprétation juridique à stabiliser
  - ✓ En résonnance avec les sujets sécurité et gouvernance, IT et Data
  - ✓ Un sujet Long Terme

- **RGPD et Immobilier**
  - ✓ Outres les sujets communs (SIRH, CRM,PRM,…) quelques points sensibles:
    - Données locataires
    - Prospection foncière
  - ✓ Atelier RGPD PRIMPROMO en cours

- **Un atelier RGPD concret et pragmatique**
  - ✓ Prestataires, outils et démonstration.
  - ✓ Sélection de deux intervenants:
    - Outils infra/data, Best practice et démonstration VARONIS
    - AMOA et outils de pilotage, démonstration Privacy On Track

Agenda de l'atelier

1 - Introduction : (10 ')

- Rappel démarche RGPD 2018
- Présentation de l'atelier CIPI

2 - Vision Infrastructure/data : (45 ')

- Best practice outils infra : les recommandations et Benchmark des outils sur la place
- Présentation (demo) d'un outil infra / Varonis

  --> intervenants : Messieurs Yann VALAINS (ARCITEK) - Christophe BADOT (VARONIS) - Yvan LANZADA (Hermitage Solutions)

3 - Vision pilotage /AMOA : (45 ')

- Pilotage RGPD, AMOA /outils fonctionnels
- Présentation (demo) de la plateforme KOEKOA RGPD

  --> intervenant : Monsieur Olivier MARTIN (ATEP Services – Privacy on Track)

4 - Présentation du retour du Benchmark RGPD CIPI (20 ')

5 – Conclusion - Discussions (30 ')

2 - Vision Infrastructure/data :

- **Best practice outils infra : les recommandations et Benchmark des outils sur la place**
- **Présentation (demo) d'un outil infra / Varonis**

--> intervenants : Messieurs Yann VALAINS (ARCITEK) - Christophe BADOT (VARONIS) - Yvan LANZADA (Hermitage Solutions)

3 - Vision pilotage /AMOA :

- **Pilotage RGPD, AMOA /outils fonctionnels**
- **Présentation (demo) de la plateforme KOEKOA RGPD**

--> intervenant : Monsieur Olivier MARTIN (ATEP Services – Privacy on Track)

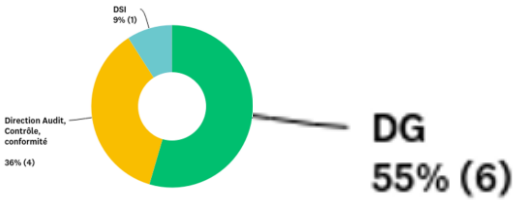
4 - BENCHMARK RGPD au sein du CIPI

Questionnaire en ligne du 5/1 au 9/2/2018

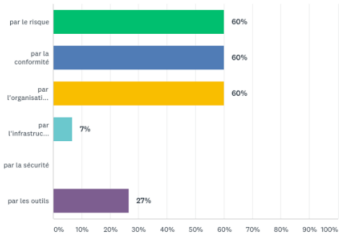
- ❑ 16 réponses / 19 adressés
- ❑ Des réponses partielles à certaines questions:
  - Non concerné
  - Le choix n'est pas encore arrêté
  - Autres (les outils…)

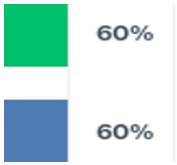
Mode de lecture

Question Choix unique



Question Choix Multiple

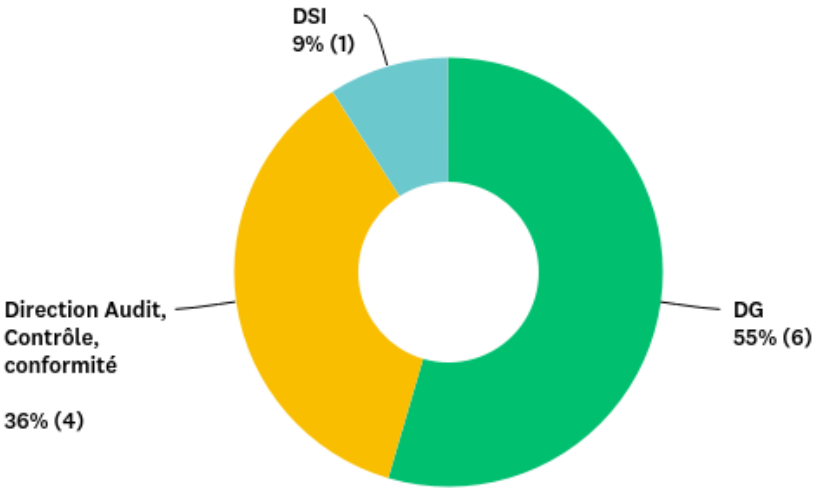




Réponses obtenues : 15
Question(s) ignorée(s) : 1

Benchmark : Sponsorship et Pilotage

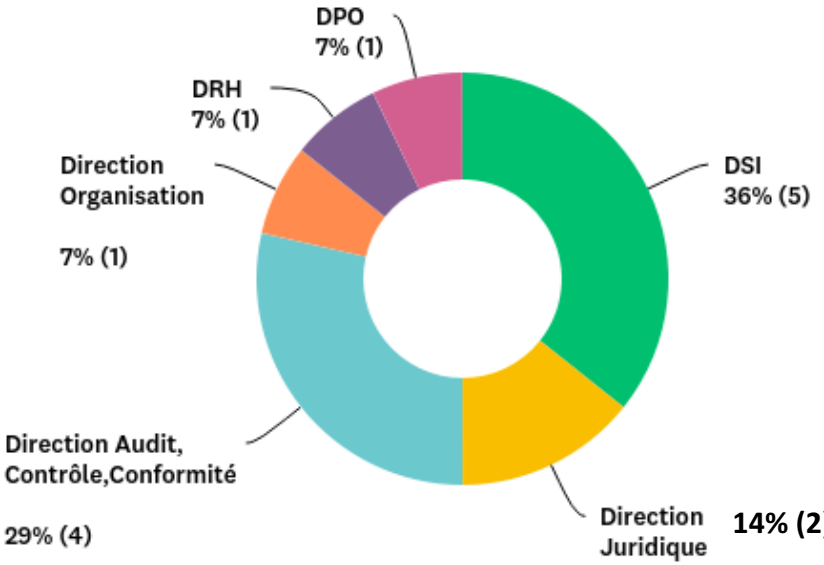
Q2: Qui est le sponsor du projet (niveau de responsabilité le plus haut) dans votre entreprise ?



Précisions /compléments:

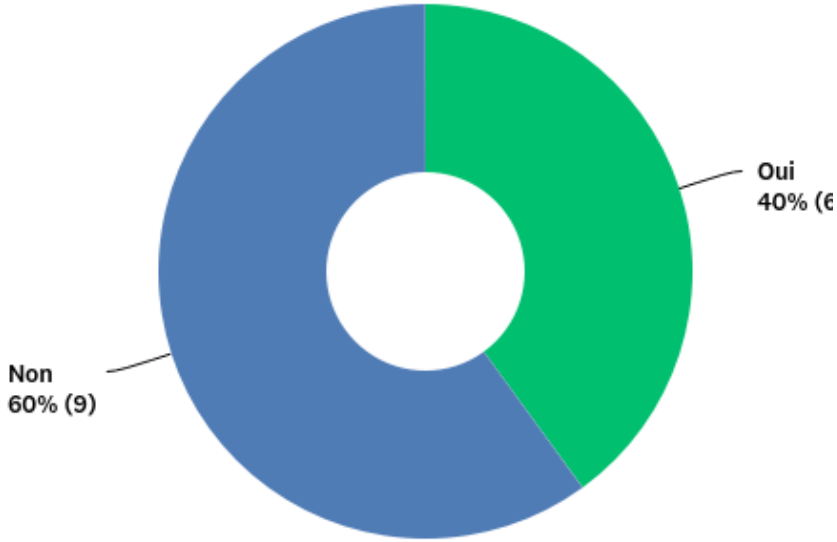
- **Dir. Transformation Digitale**
- **Secrétariat général(2)**

Q3: Qui ou quelle direction conduit le pilotage opérationnel du projet RGPD ?

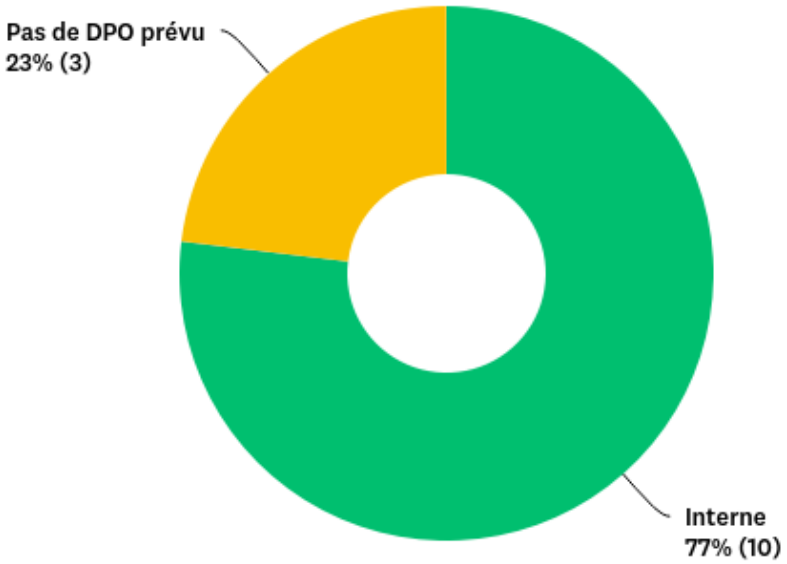


Benchmark : Le DPO (1/2)

Q4: Un DPO est-il désigné dans votre entreprise ?



Q5: Avez vous désigné ou envisagez vous la désignation d'un DPO ?

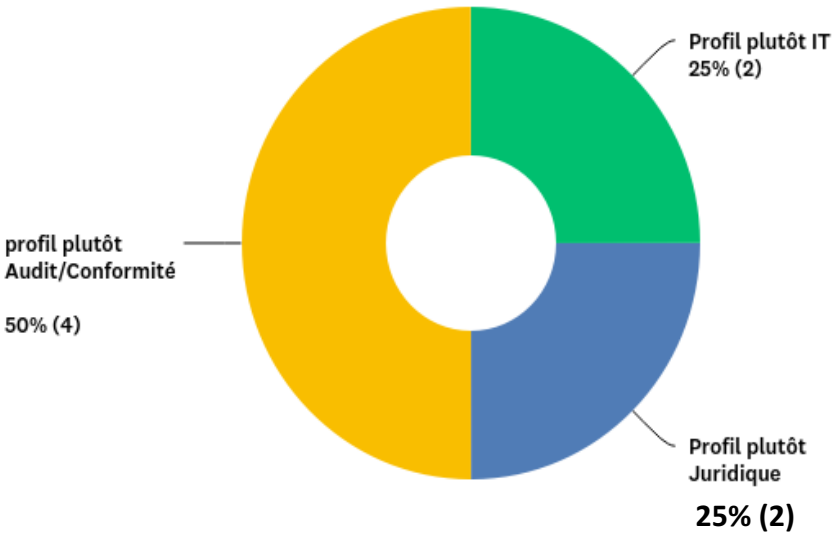


Remarques/commentaires:

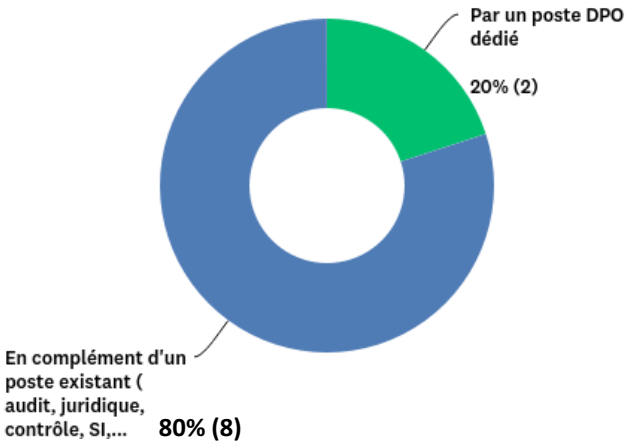
- Encore beaucoup de décisions en cours

Benchmark : Le DPO (2/2)

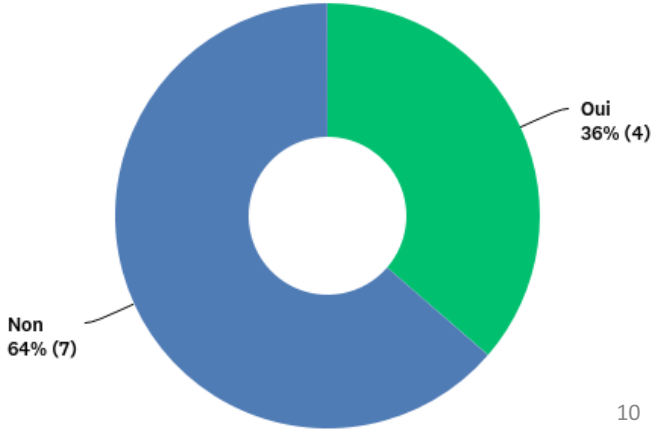
Q6: Pour un DPO interne, nommé ou en cours de désignation , quel est son profil ?



Q7: Pour un DPO interne, la fonction est (sera) **portée** ?



Q9: Pour un DPO interne, **s'agit** -il de l'ancien CIL ?



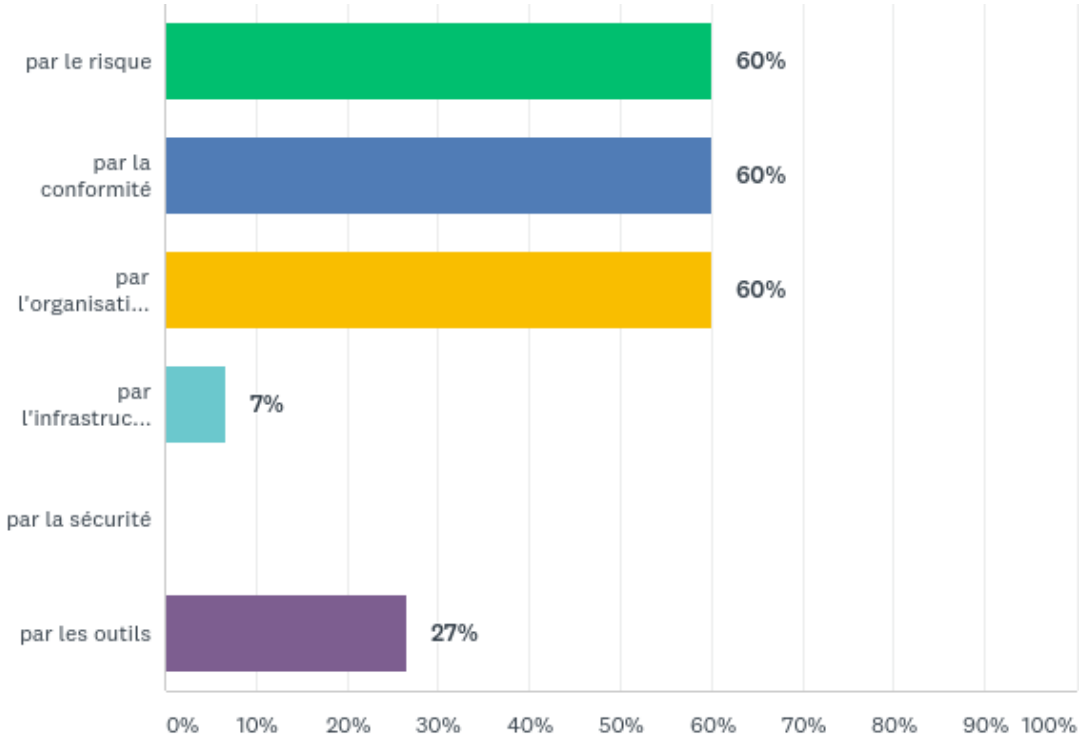
Remarques/commentaires:

- Idéalement, profil mixte, IT/juriste/metier
- double rattachement (gouvernance)

Benchmark : L'approche

Q10: Quelle type d'approche adopte votre entreprise pour la mise en conformité RGPD (choix multiple) ?

Réponses obtenues : 15 Question(s) ignorée(s) : 1

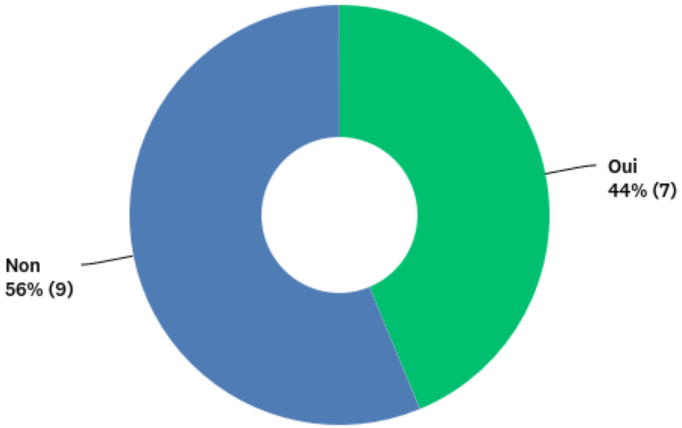


Remarques/compléments:

7 axes du règlement: projets, gouvernance, traitements, protection, droits, violations, sous traitants.

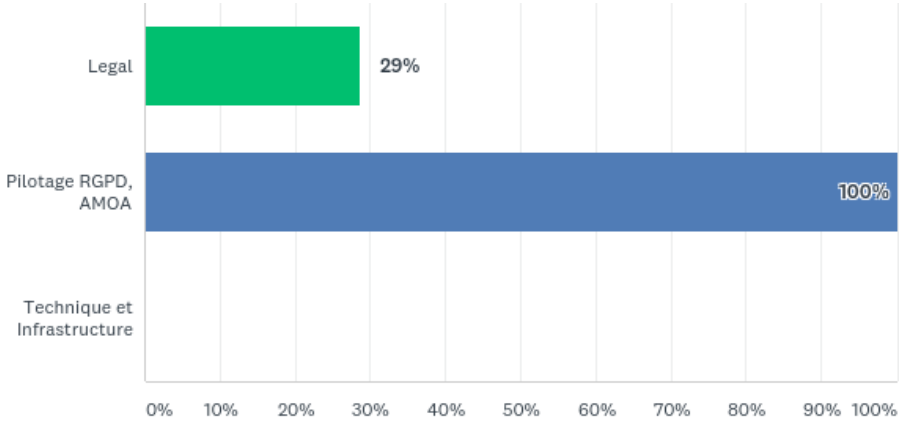
Benchmark : Accompagnement, prestataires et outils

Q11: Recherchez vous ou avez vous désigné des prestataires pour vous accompagner dans la mise en conformité RGPD ?



Q12: Si Oui, quel type de prestataire recherchez vous (Choix multiple) ?

Réponses obtenues : 7 Question(s) ignorée(s) : 9



Remarques/compléments:

- 50% ne prévoient pas d'etre accompagnés
- Pas de prestataire technique ?

Q13 SI vous avez déjà désigné des prestataires, pouvez vous nous indiquer lesquels et leur positionnement ? (nommer un prestataire dans plusieurs catégories s'il s'agit d'un prestataire polyvalent)

Réponses obtenues : 7 Question(s) ignorée(s) : 9

Legal	**ALTANA (Avocats) - Cabinet d'avocats**
Pilotage RGPD/AMOA	**Formind - Sia-partners - CIL Consulting - Wavestone - ITS Group - Pwc**
Infrastructure/technique	**VARONIS**

Q14 Quels outils pensez vous utiliser pour vous assister dans la démarche RGPD pour les aspects Pilotage démarche/AMOA ?

Réponses obtenues : 8 Question(s) ignorée(s) : 8

Pilotage de la mise en conformité	**bureautique - RETIL de la société CILEX - Bureautique**
Gestions des process/documentation	**sharepoint - RETIL de la société CILEX - l'intranet Processus - Bureautique**
Aide à la cartographie / audit de l'existant	**Visio - Outil interne - Outils CNIL - Bureautique**

Remarques/commentaires:
- Peu de réponses complètes
- Choix restant à faire
- Outils non spécifiques au RGPD

Quels outils pensez vous utiliser / implémenter pour traiter des problématiques RGPD (Infrastructure / data) ?

Réponses obtenues : 8 Question(s) ignorée(s) : 8

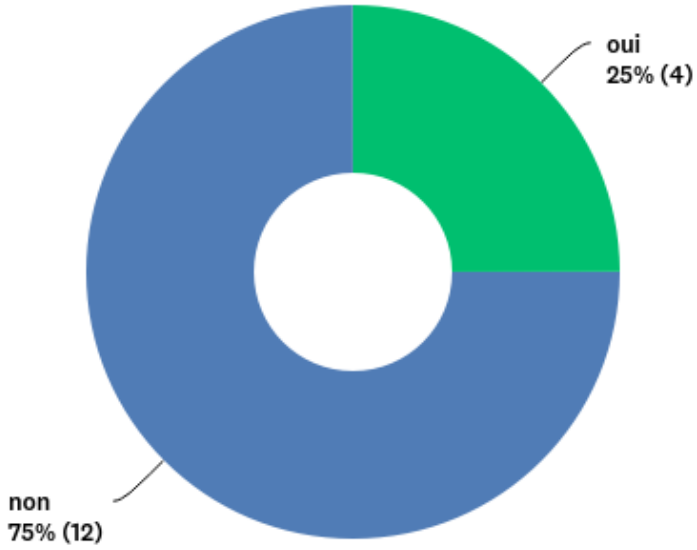
Gestion des Accès Authentification	**Brainwave - AD/ADFS/DUO/gestion des habilitations - Active Directory - Jalios**
Sécurité des poste de travail	**bitlocker - Landesk - sophos**
Sécurité des dispositifs mobiles	**Airwatch (2) - MDM intunes**
Télémaintenance des équipements	**TeamViewer**
Audit, traçabilité et gestion des incidents	**GLPI - Jalios et Reconet - Privacy on track**
Sensibilisation des utilisateurs	**portail cross knowledge (@learning) - 360learning.com - Intranet avec des vidéos et des messages**
Archivage - Stockage sécurisé	**interne - GED, Archives Outlook, ISeries**
Sécurité des locaux	**Badge - Badge et Visio**
Sécurité des serveurs et des applications	**Strandart - WSUS, Opmanager + divers outils de sécurité - Varonis**
Chiffrement	**zone central - smime**
Échange de données sécurisées	**SFTP**
Sécurité du réseau informatique interne	**sécurité périmètrique et cloisonnement réseau**
Sauvegarde et continuité d'activité	**Plan de continuiité informatique (VPLEX, COMVAULT) - PRA interne**

Remarques/commentaires:

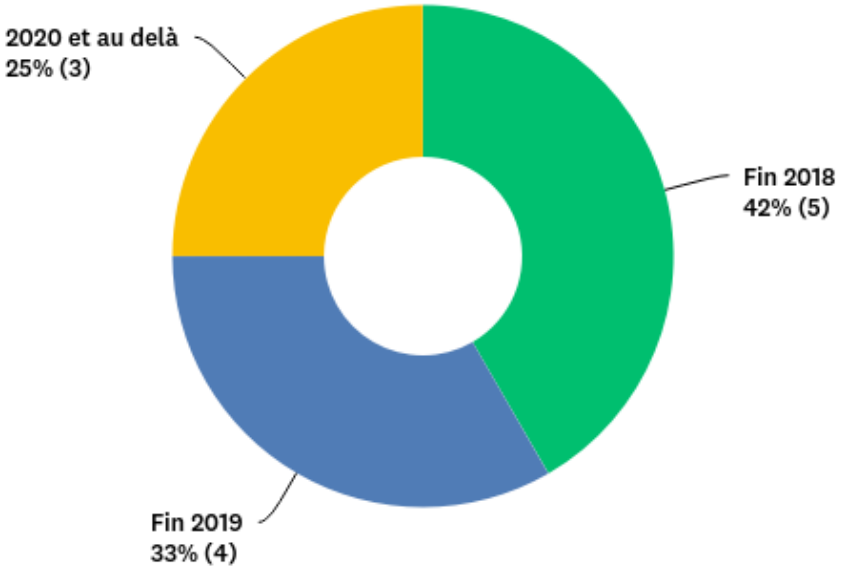
- Peu de réponses complètes
- Outils non spécifiques au RGPD, s'appuyer au maximum sur l'existant
- Choix restant à faire

Benchmark : Planning RGPD

Q16: Estimez vous que votre entreprise sera prête au 25 mai 2018 ?



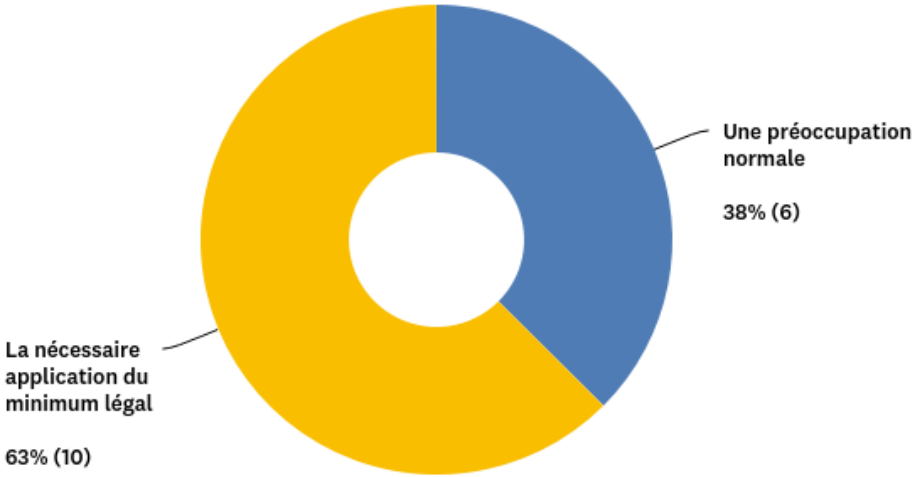
Q17: Si non, à quelle échéance pensez vous que la conformité au RGPD sera effective pour votre entreprise ?



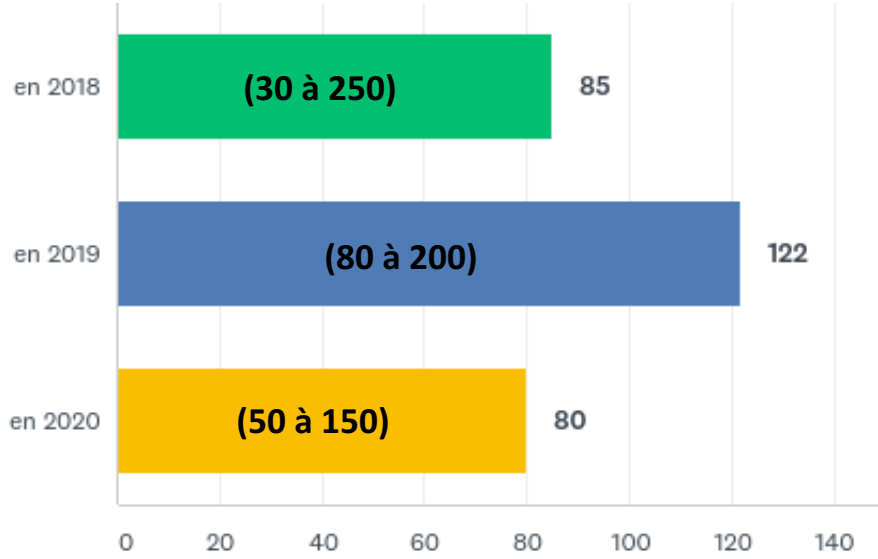
Remarques/commentaires:
- 25% en mai 2018, 42% fin 2018, une non urgence assumée
- Peut être jamais fini….

Benchmark : Enjeux et budgets

Q18: Selon vous la mise en conformité au RGPD est pour votre entreprise ?



Q19: Quel budget en K€ estimez vous que votre DSI consacrera à la mise en œuvre du RGPD ?



Remarques/commentaires:

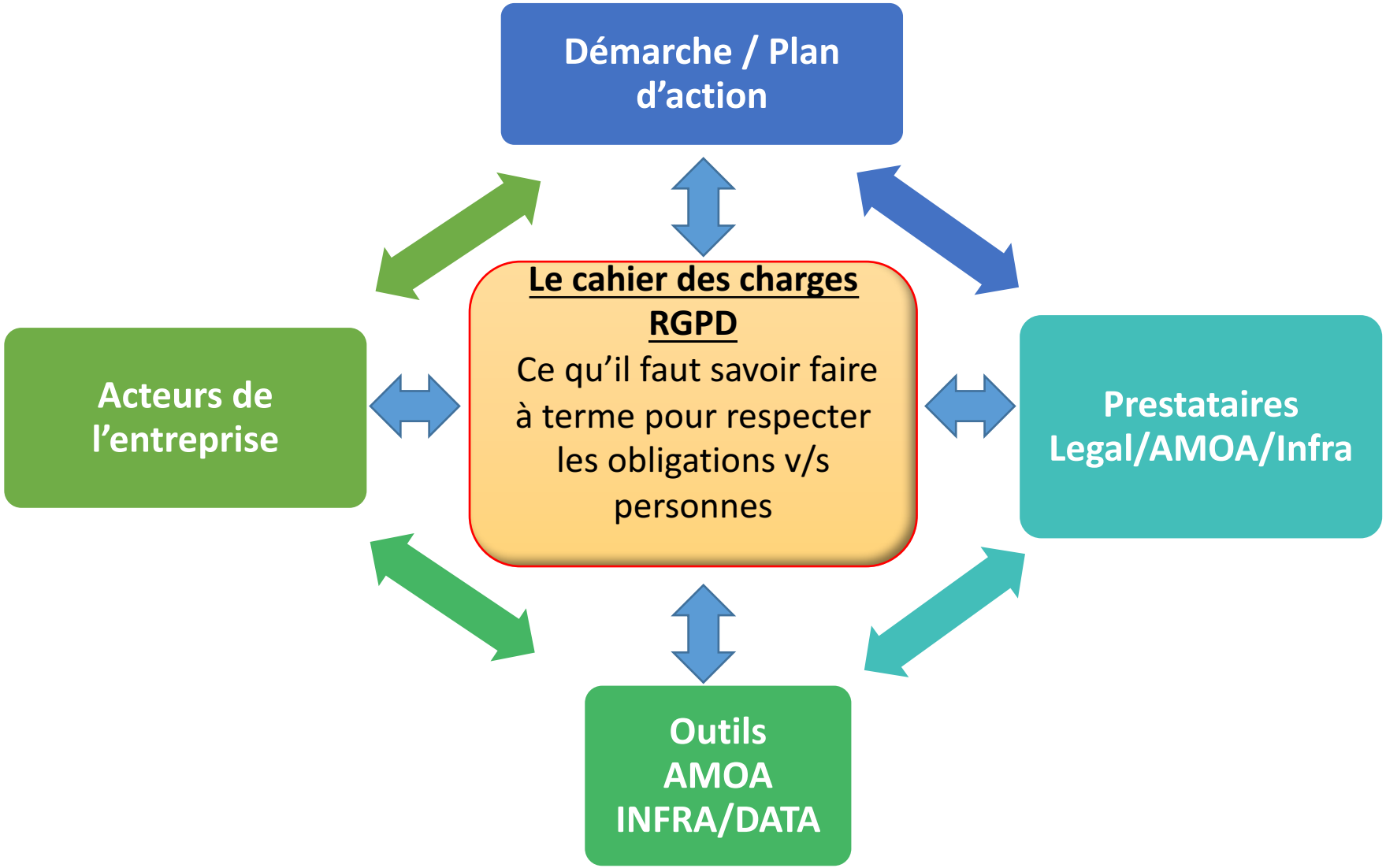
- « RGPD, Une priorité absolue » n'est retenu par personne
- Convergence avec des besoins de sécurité plus larges
- RGPD: Implication plus générale (métiers..) et transverse pour l'entreprise
- La cartographie Traitement/Données est le point clef à court terme.

5. Discussion, Conclusion

➔**Quelques suggestions (si besoin)**

- RGPD, Opportunité pour le DSI:
  - Contrôle du Shadow IT
  - Encadrement du BYOD
- Sous traitante métier et informatique: organisation, exigences, risques, formalisation contractuelle
- Missions impossibles (Fichier de prospection foncière, consentement par tel/call center…)
- Pb des logiciels, apport des éditeurs ?
  - Boite à outil technique et contractuelle, …
  - PRIMPROMO, SALES FORCES, DYN AMICS CRM, SAP, ORACLE, SIRH ….
- Convergence RGPD / Directive NIS (sécurité SI - 9/5/2018) / Directive e-Privacy (Vie privée et communications électronique – 25/5/2018 ?)

Annexe I - Vue globale – Le RGPD en 5 schémas



Le Plan d'action

Le délégué à la protection des données (DPO =Data Protection Officer) = « chef d'orchestre » en charge notamment :

- d'informer et de conseiller
- de contrôler le respect du règlement
- de conseiller l'organisme
- de coopérer avec l'autorité de contrôle

Pour établir un registre des différents traitements de données à caractère personnel, des catégories de données, des objectifs poursuivis, des acteurs (internes ou externes), des flux

Prioriser ces actions au regard des risques que font peser les traitements sur les droits et les libertés des personnes concernées.
- Révisez les mentions d'information
- Vérifiez que les sous-traitants connaissent leurs nouvelles obligations,

Mener, pour chacun de ces traitements, une analyse d'impact sur la protection des données (DPIA) si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées

Mettre en place des procédures internes qui garantissent la prise en compte de la protection des données à tout moment, (ex : notification violation de données idéalement au plus tard 72h après l'identification, modification des données collectées, changement de prestataire,…).

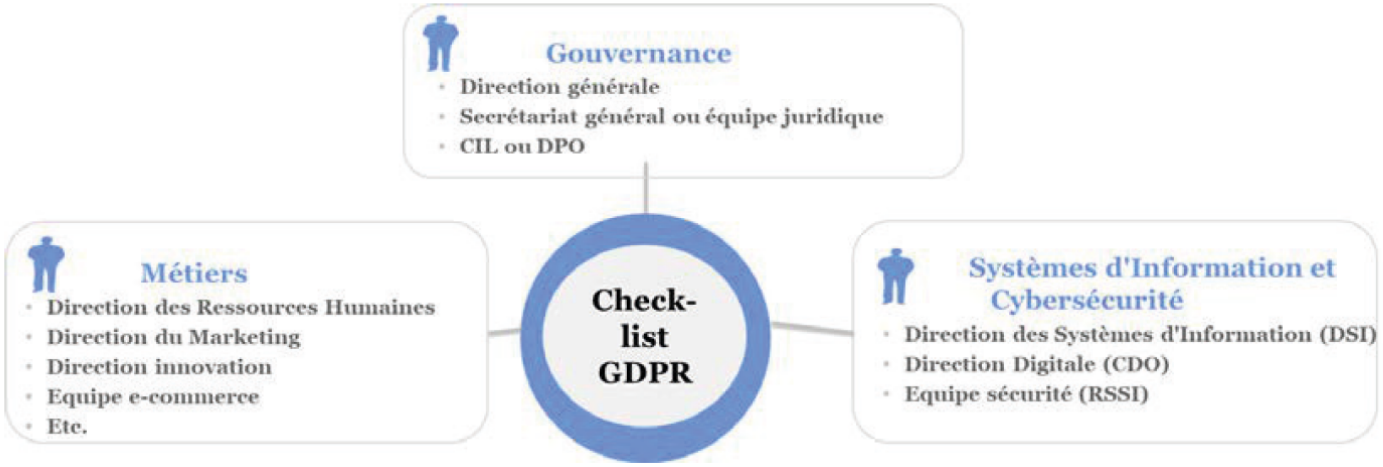
Constituer et regrouper la documentation nécessaire pour prouver votre conformité au règlement

Actualiser régulièrement pour assurer une protection des données en continu.

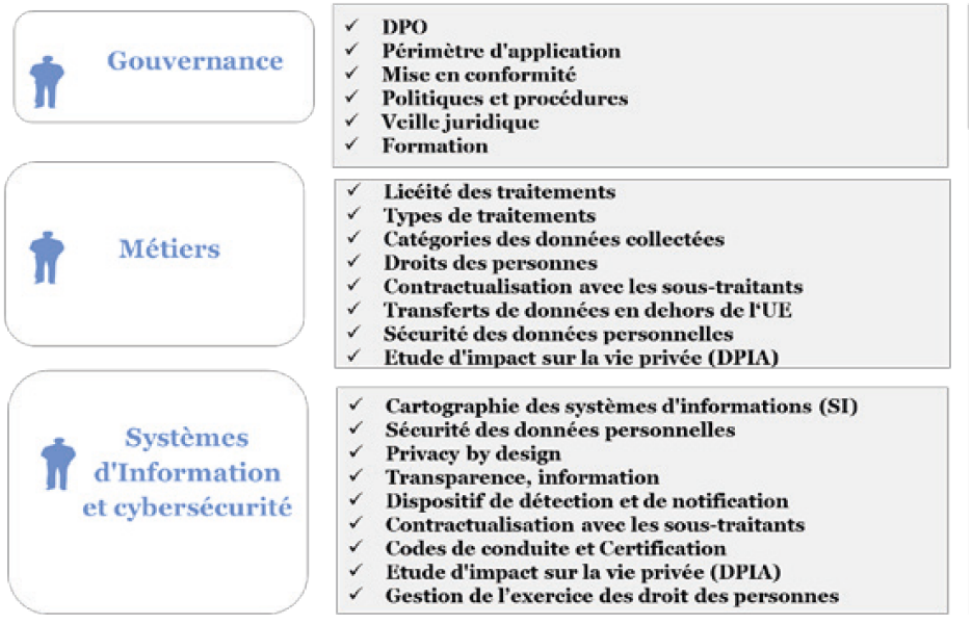
L'echo-système des prestataires

Avocats	• Legal + support documentaire, • Legal + AMOA, • Legal+AMOA+outils,
Prestataires AMOA	• Conseil classique • Démarche AMOA dédiée RGPD • Démarche AMOA + Legal
Prestataires INFRA/DATA	• Intégrateurs Outils Infra/data généraux • Conseil/Intégrateurs Outils dédiés RGPD,

Les acteurs de l'entreprise concernés



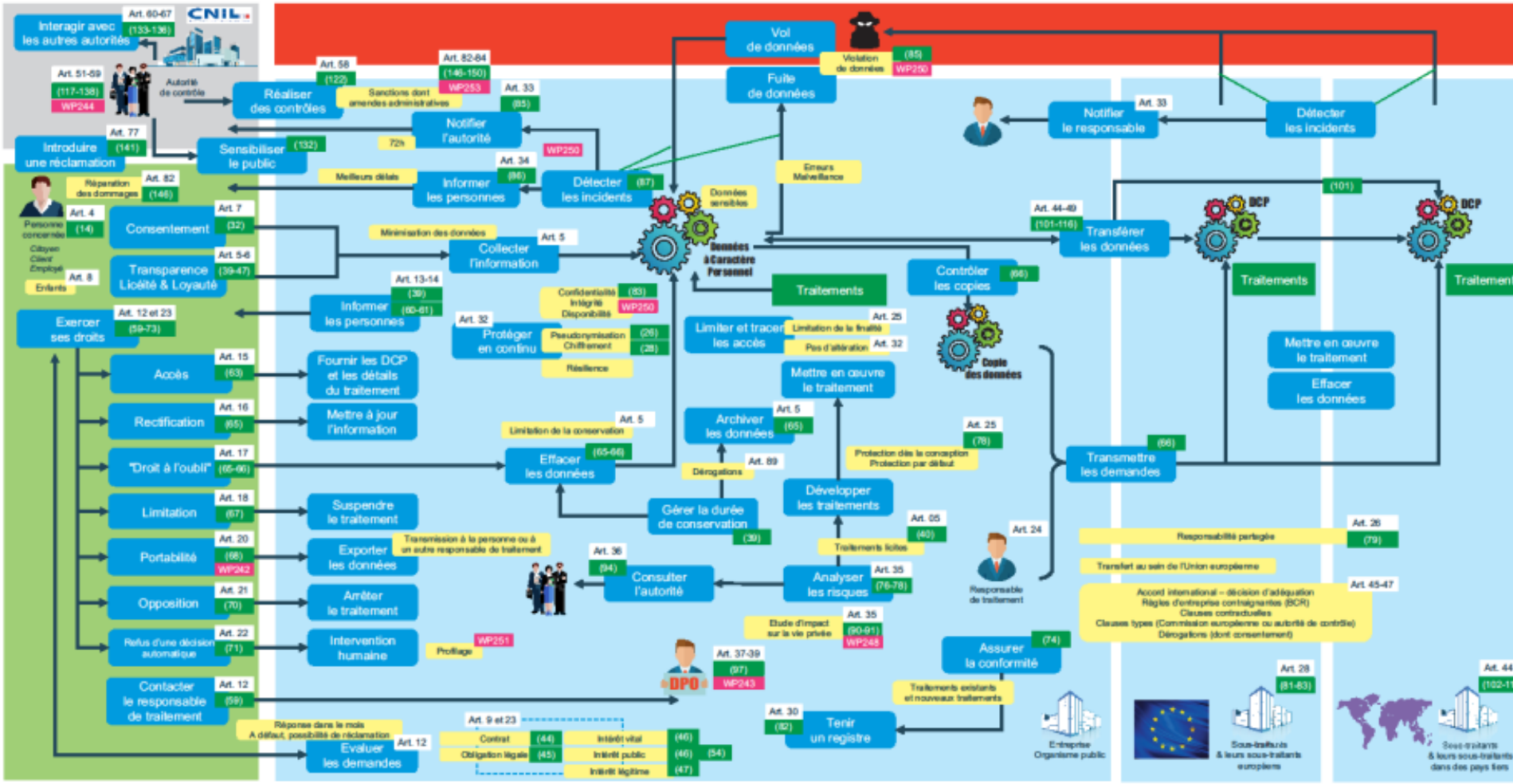
Thèmes et sous thèmes :



Le cahier des charges RGPD

Ce qu'il faut savoir faire à terme pour respecter les obligations v/s personnes

Elle ne peut pas être exhaustive mais elle offre une grille de lecture graphique et synthétique pour découvrir la portée de la règlementation, puis s'y référer ultérieurement.



CLUSIF

Le CLUSIF (Club de la Sécurité de l'Information Français) est le 1er club de professionnels de la sécurité de l'information français, réunissant plus de 300 entreprises et collectivités issues de tous les secteurs de l'économie. L'objectif principal du CLUSIF est de favoriser les échanges d'idées et de retours d'expériences à travers des groupes et espaces de travail, comme Espace RSSI, des publications de référence et des conférences thématiques organisées tout au long de l'année. Quelques exemples de sujets abordés dans les groupes de travail : applications mobiles, cyberassurance, étude MIPS (menaces informatiques et pratiques de la sécurité), internet des objets, panorama de la cybersécurité, RGPD, sécurité numérique au quotidien, signature électronique, systèmes industriels, tableaux de bords de sécurité…

Pour toute information complémentaire, vous pouvez contacter : Luména Duluc, déléguée générale : 01 53 25 08 80 (clusif@clusif.fr)

Légende

- Art. 51 — Article du Règlement européen
- (145) — Considérant du Règlement européen
- WP244 — Ligne directrice du G29

Global Security Mag
THE LOGICAL & PHYSICAL SECURITY MAGAZINE