Le Règlement européen n°2016/679

du Parlement européen et du Conseil du 27 avril 2016

relatif à la protection des personnes physiques

à l'égard du traitement des données à caractère personnel

et à la libre circulation de ces données

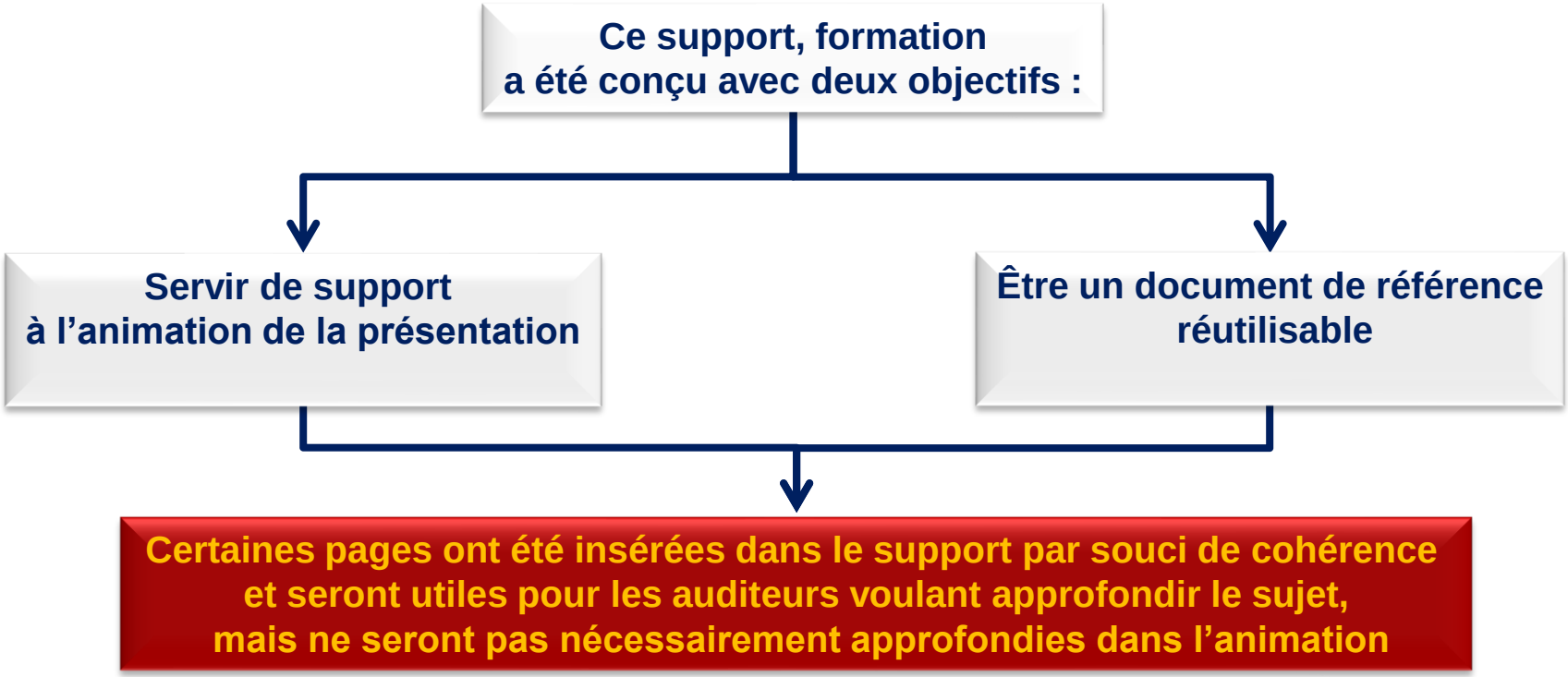
Impact sur l'organisation et plan d'actions

Denis Virole

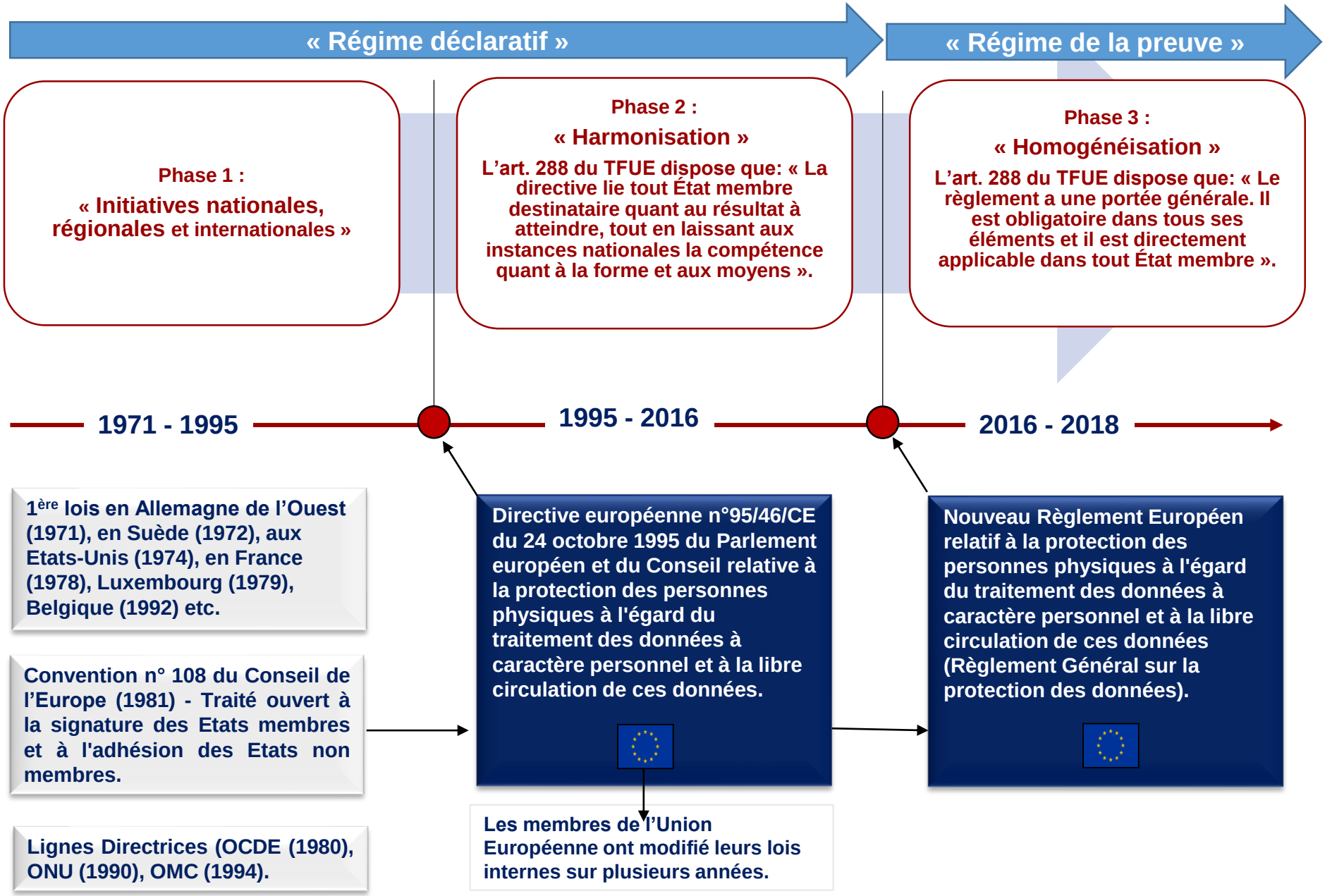
Version 0.3 du 28/09/201 extrait de la présentation du 3/10/2017

ANSSI	Agence Nationale Sécurité Système d'Information / France
CIL	Correspondant Informatique et Libertés
CNIL	Commission Nationale Informatique et Libertés / France
DCP	Donnée à caractère personnel
DPO	Data Protection Officer
EM	Etat Membre
LIL	Loi Informatique et Libertés
OCDE	Organisation de Coopération et de Développement Économiques
PC	Personne concernée
RSSI	Responsable Sécurité Système d'Information / CISO
RT	Responsable du Traitement
UE	Union Européenne
ST	Sous Traitant
T	Traitement
TFUE	Traité sur le Fonctionnement de l'Union Européenne

Avertissement

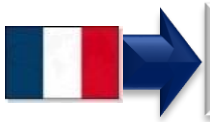


Introduction



**« L'informatique doit être au service de chaque citoyen.
[…] Elle ne doit porter atteinte
ni à l'identité humaine,
ni aux droits de l'homme,
ni à la vie privée, ni aux libertés individuelles ou publiques. »**

Article 1 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

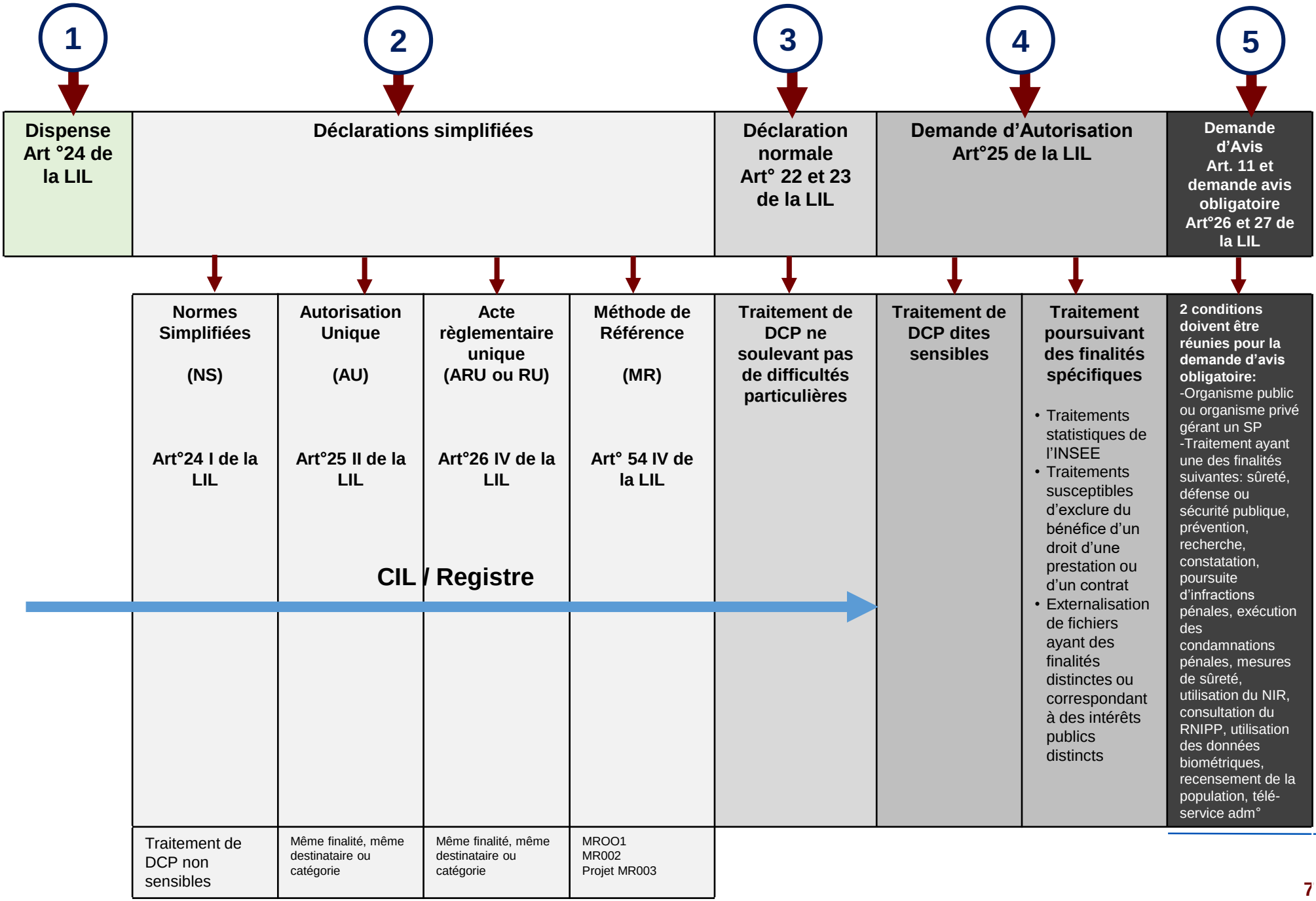


**Prévenir les atteintes aux droits et aux libertés,
Donner aux individus un droit de regard sur l'usage et la qualité des données les concernant.**

Concilier les valeurs fondamentales du respect de la vie privée et la protection des données à caractère personnel avec la libre circulation de l'information entre les Etats.

Introduction

Régime déclaratif / Schéma récapitulatif - 5 procédures



Le traitement des DCP doit être conduit pour servir l'humanité

Le droit à la protection des DCP n'est pas un droit absolu
Il doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité

Le Règlement respecte **tous les droits fondamentaux et observe les libertés** et les principes reconnus par la **Charte des droits fondamentaux de l'Union Européenne**, consacrés par les traités, en particulier le respect de la vie privée et familiale, du domicile et des communications, la protection des DCP, la liberté de pensée, de conscience et de religion, la liberté d'expression et d'information, la liberté d'entreprise, le droit à un recours effectif et accéder à un tribunal impartial, et la diversité culturelle et religieuse

Le GDPR : Vision synthétique régime de la preuve

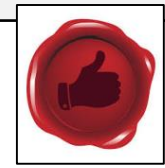
Le Règlement européen n°2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

Renforcement des responsabilités du Responsable du Traitement et du Sous traitant

Renforcement des droits de la Personne Concernée
+ La Loi pour la République Numérique

Renforcement des obligations de sécurité

Obligation de prouver la conformité



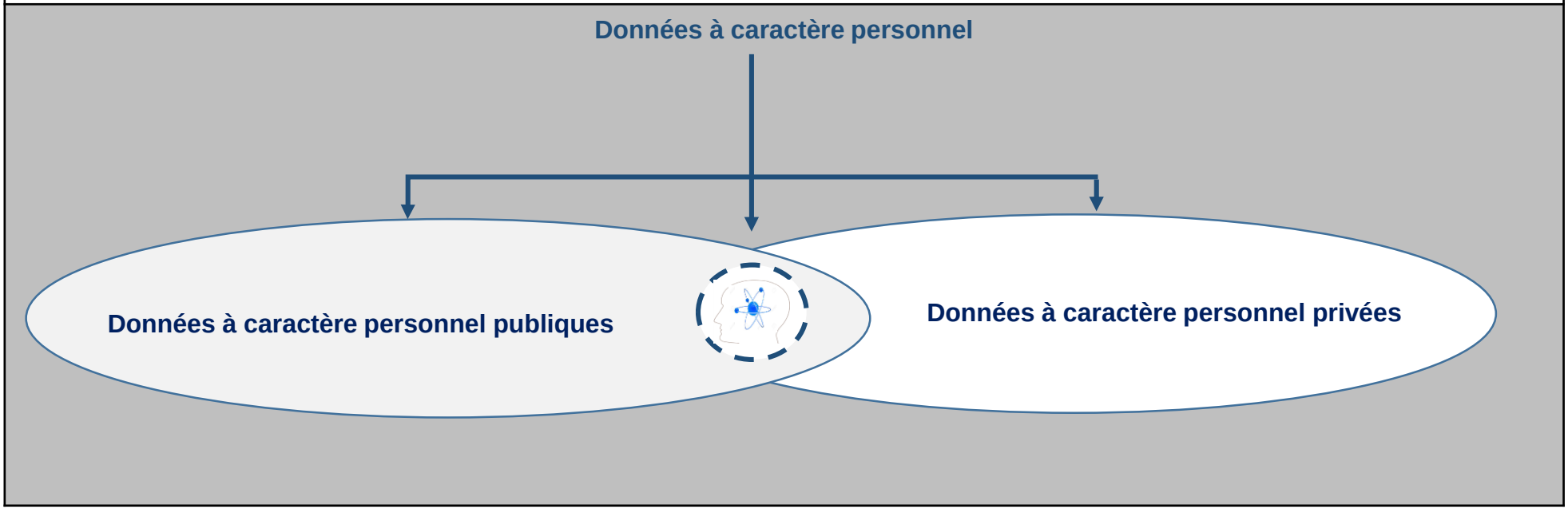
Une donnée à caractère personnel

Règlement européen

Chapitre 1: Dispositions générales

Article 4 1): Définitions

« ***Toute information*** *se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée"); est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment* ***par référence à un identifiant****, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* ».



Définitions

Traitement

Règlement européen

Chapitre 1: Dispositions générales

Article 4 1): Définitions

*« **(…) toute opération** ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et **appliquées à des données ou des ensembles de données à caractère personnel**, telles que :*

- ***la collecte***
- ***l'enregistrement***
- ***l'organisation***
- ***la structuration***
- ***la conservation***
- ***l'adaptation***
- ***la modification***
- ***l'extraction***
- ***la consultation, l'utilisation***
- ***la communication par transmission***
- ***la diffusion ou toute autre forme de mise à disposition***
- ***le rapprochement ou l'interconnexion, la limitation***
- ***l'effacement ou la destruction »***

Définitions

Champ d'application matériel

A la différence de la Loi Informatique et Libertés, le Règlement européen propose une liste plus exhaustive des cas dans lequel ce dernier s'applique et/ou ne s'applique pas.

Le Règlement s'applique:

- **Au traitement de DCP automatisé ou non figurant dans un fichier,**
- **Au traitement de DCP mis en place par les institutions de l'UE,**
- **Au traitement de DCP mis en œuvre par les prestataires de services intermédiaires.**

Le Règlement ne s'applique pas:

- **À une activité ne relevant pas du champ d'application du droit de l'Union,**
- **Aux traitements de DCP par les EM dans le cadre d'activités relevant du traité sur l'Union européenne (Chapitre 2, titre V: Politiques relatives aux contrôles aux frontières, à l'asile et à l'immigration),**
- **Dans le cadre d'une activité strictement personnelle,**
- **Aux traitements de DCP mis en œuvre par les autorités compétentes à des fins de prévention et de détection des infractions pénales etc.**

Champ d'application territorial

Le nouveau texte indique les différents types d'activités de traitement qui sont susceptibles d'être soumis à la législation européenne dans le cas où le RT ou le ST n'est pas établi au sein de l'Union européenne mais que les PC par le T s'y trouvent, à savoir :

- Une offre de biens ou de services aux PC dans l'Union, qu'un paiement soit exigé ou non desdites personnes,
- Le suivi du comportement de ces personnes lorsque ce comportement a lieu au sein de l'Union.

Indépendamment de leur nationalité et de leur lieu de résidence

Définitions

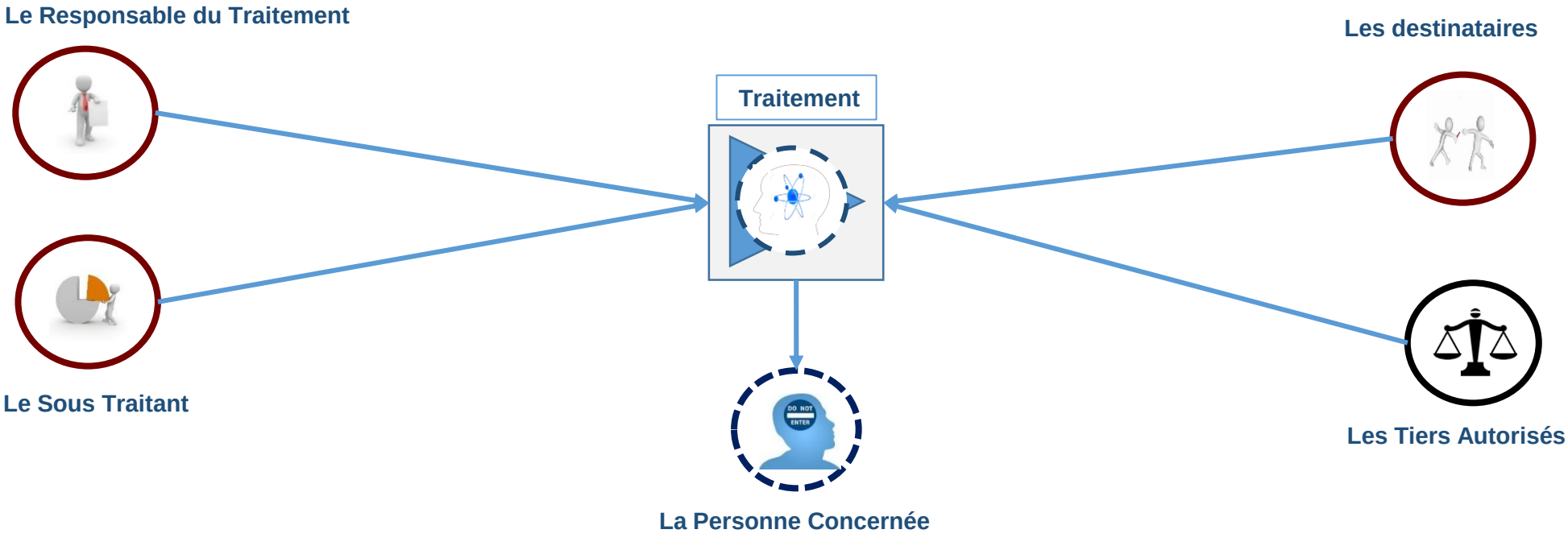
Les intervenants sur un traitement

Commentaires

Les définitions proposées par le règlement concernant les destinataires et les tiers sont légèrement différentes des définitions fournies par la CNPD

A noter que la définition du service en charge de la mise en œuvre du traitement n'est pas fournie mais simplement mentionné dans la définition du tiers.

Concernant le ST, la définition ne précise pas s'il peut s'agir d'un ST interne ou externe.



Principes

	Nouveautés
Principe de licéité et de loyauté	Un terme important a été ici ajouté, celui de « transparence » au regard de la personne concernée Le T : • Doit avoir une base légale ou remplir une des conditions nous le verrons dans l'article 6 du Règlement, • Ne doit pas se faire à l'insu de la personne concernée, • Le RT doit faciliter l'accès à l'information, le droit de savoir
Principe de sécurité et de confidentialité	La notion de « sécurité » est érigée en véritable principe.

Le RT est en mesure de démontrer l'application des principes

T des DCP

Traitées de manière licite, loyale et transparente	Finalité déterminée Explicite et légitime Ne pas être traitées ultérieurement	Adéquates pertinentes, limitées	Exactes et mise à jour	Conservées pendant une durée limitée

Consentement

Prise en compte de l'enfant

Sécurité du Traitement

Droits des Personnes Concernées

Le Règlement européen

Les droits

Droits existants mais renforcés par le Règlement

Droit d'information	Droit d'accès	Droit de rectification	Droit à l'effacement	Droit d'opposition et Profilage
Art. 13 et 14	Art. 15	Art. 16	Art. 17	Art. 21 et 22

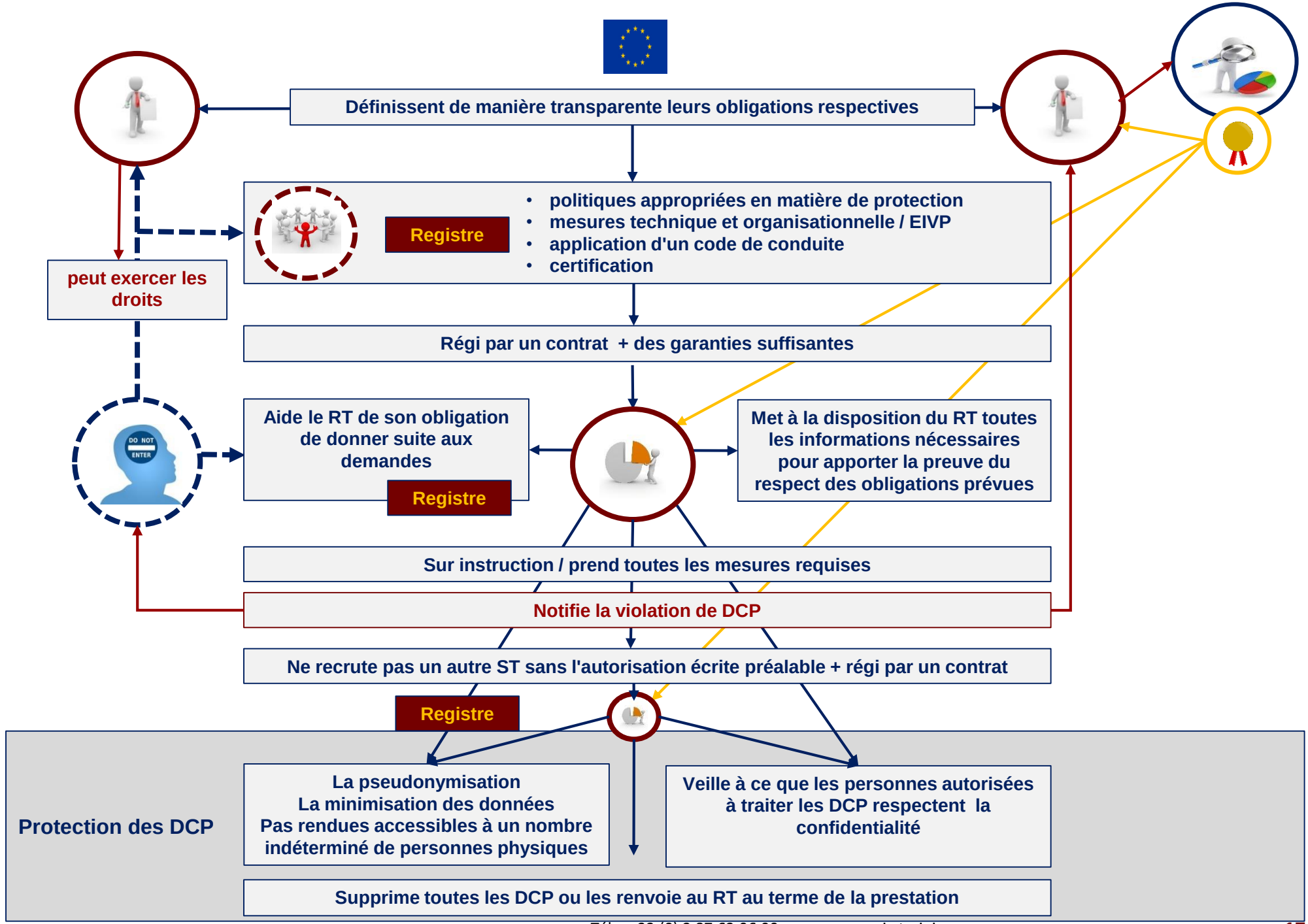
Nouveaux droits

Droit à la limitation du traitement	Obligation de notification rectification effacement limitation du T	Droit à la portabilité
Art. 18	Art. 19	Art. 20

Les droits de recours

Droit d'introduire une réclamation auprès d'une autorité de contrôle	Droit à un recours juridictionnel effectif contre un responsable du traitement ou un sous-traitant	Droit à réparation et responsabilité	Droit à un recours juridictionnel effectif contre une autorité de contrôle	Représentation des personnes concernées
Art. 77	Art. 79	Art. 82	Art. 78	Art. 80

Obligations du RT et du ST

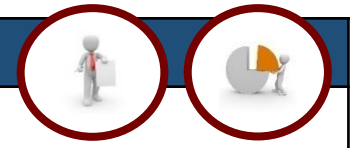


Obligations du RT et du ST

	Nouveautés
Sécurité	**L'article 24 du Règlement parle de « mesures techniques et organisationnelles appropriées ».** **Le Règlement propose de se référer aux mécanismes de certification et aux codes de conduite.** **D'autre part, le texte européen évoque la protection des DCP dès la conception (« privacy by design ») ou par défaut, c'est-à-dire après la conception (« privacy by default »).** **Les différentes mesures techniques et organisationnelles que le RT est susceptible de mettre en œuvre, à savoir (liste non-exhaustive):** **1. Pseudonymisation, chiffrement des DCP** **2. Garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services** **3. Des moyens permettant de rétablir la disponibilité des DCP et leur accès en cas d'incident physique ou technique,** **4. Procédure visant à tester, analyser et à évaluer régulièrement l'efficacité des mesures organisationnelles et techniques**

Contrat	**1. Le RT doit choisir un sous-traitant qui présente des garanties suffisantes quant à la mise en œuvre de mesures organisationnelles et techniques appropriées (idem que dans la LIL),**
	2. Le sous-traitant ne doit pas recruter un autre sous-traitant sans l'autorisation écrite préalable, du RT
	3. La relation entre le RT et le sous-traitant doit être régie par un contrat,
	4. Lorsqu'un ST recrute un autre ST , ce dernier est soumis aux mêmes obligations que le ST
	5. Le sous-traitant ne doit traiter les DCP que sur instruction documentée du RT
	• **Les personnes autorisées à traiter les DCP s'engagent à respecter la confidentialité**
	• **Aide le RT :**
	  • **à faire suite aux demandes dont les PC le saisissent en vue d'exercer leurs droits**
	  • **à garantir la sécurité du T, à notifier à l'autorité de contrôle d'une violation de DCP, à communiquer à la PC une violation de DCP,**
	  • **à effectuer une EIVP**
	  • **à consulter une autorité de contrôle préalablement au T lorsqu'une analyse d'impact relative à la protection des DCP a été effectuée,**
	• **Supprime toutes les DCP ou les renvoie au RT au terme de la prestation de services relatifs au T**
	• **Le sous-traitant met à la disposition du RT toutes les informations nécessaires pour apporter la preuve du respect des obligations légales et également pour la réalisation d'audits.**

Obligations du RT et du ST

	Nouveautés 
Registre	**C'est au RT ou au représentant du RT de tenir un registre des activités de traitement effectuées sous leur responsabilité.**
Violation de DCP	**Le texte européen prévoit une notification à l'autorité de contrôle dans les meilleurs délais et si possible dans les 72 heures au plus tard après en avoir pris connaissance.** • **Description de la nature de la violation de DCP** • **Communication du nom et coordonnées du DPO** • **Description des conséquences probables de la violation,** • **Description des mesures prises ou celles que le RT propose de prendre**
EIVP / PIA	**L'EIVP doit être effectuée par le RT avec l'aide du DPO** • **L'évaluation d'aspects personnels concernant les PC y compris le profilage,** • **Le T à grande échelle de catégories particulières de DCP visées à l'article 9 paragraphe 1, soient les données révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, les données biométriques, les données de santé, la vie sexuelle ou l'orientation sexuelle d'une personne, ainsi que les données relatives aux condamnations pénales ou infractions visées à l'article 10** • **La surveillance systématique à grande échelle d'une zone accessible au public.**

Transfert de DCP hors UE

https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-n

La protection des données ...

CNIL.

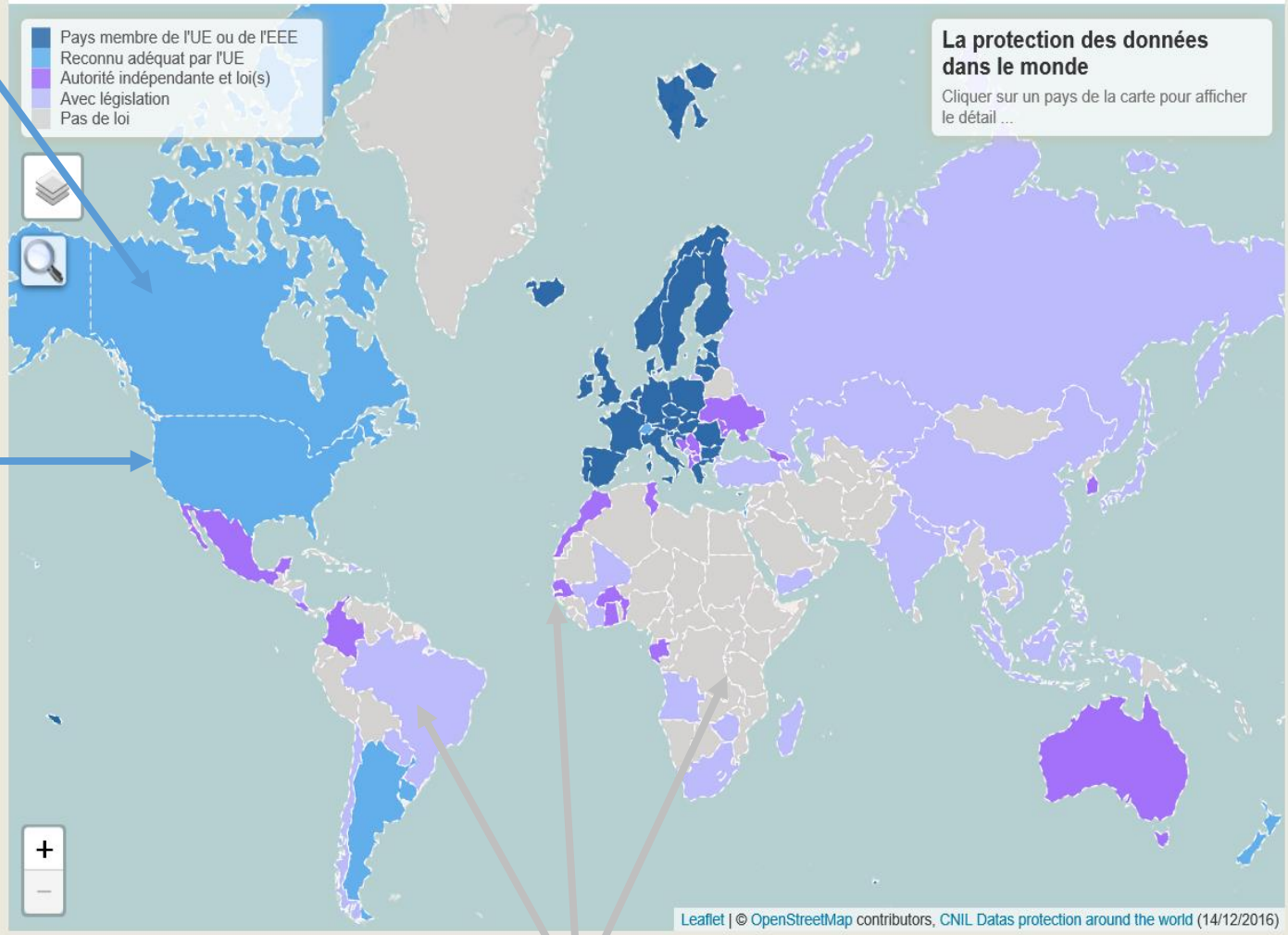
PARTICULIER | PROFESSIONNEL

MES DÉMARCHES | THÉMATIQUES | À LA UNE | RÈGLEMENT EUROPÉEN | LA CNIL

Article 45 Transferts fondés sur une décision d'adéquation

Privacy Shield

- **des obligations strictes pour les entreprises qui traitent des DCP européennes, et un contrôle rigoureux**
- **un accès par les autorités américaines étroitement encadré et transparent**
- **une protection effective des droits des PC de l'Union et plusieurs voies de recours.**



Article 46 Transferts moyennant des garanties appropriées Contrat / BCR

Article 49 Dérogations pour des situations particulières

Le consentement de la PC,

L'exécution d'un contrat entre la PC et le RT,

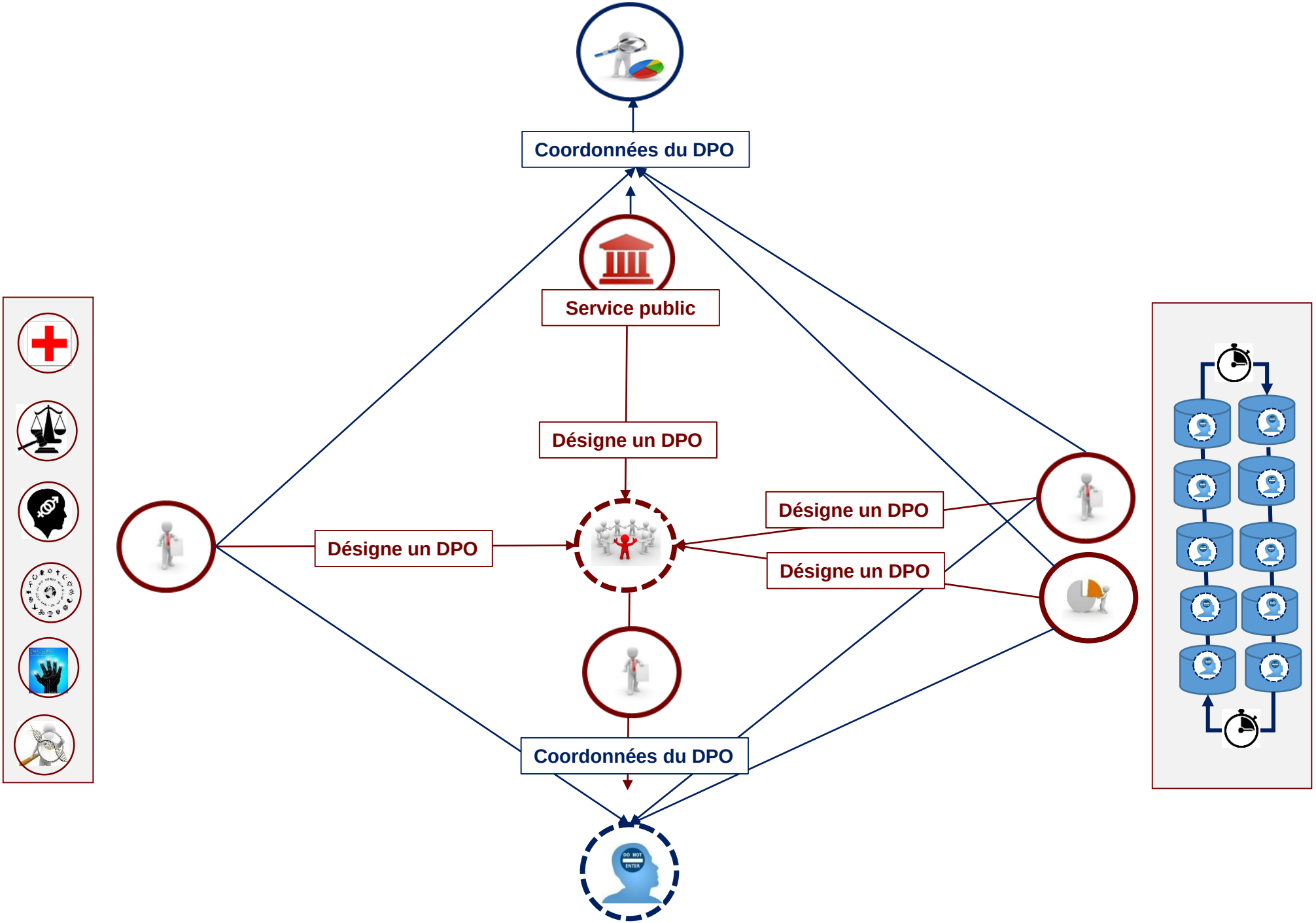
La conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la PC,

Des motifs importants d'intérêt public,

Nécessaire à la constatation, à l'exercice ou à la défense de droits en justice,

Nécessaire à la sauvegarde des intérêts vitaux de la PC ou d'autres personnes lorsque la PC se trouve dans l'incapacité physique ou juridique de donner son consentement

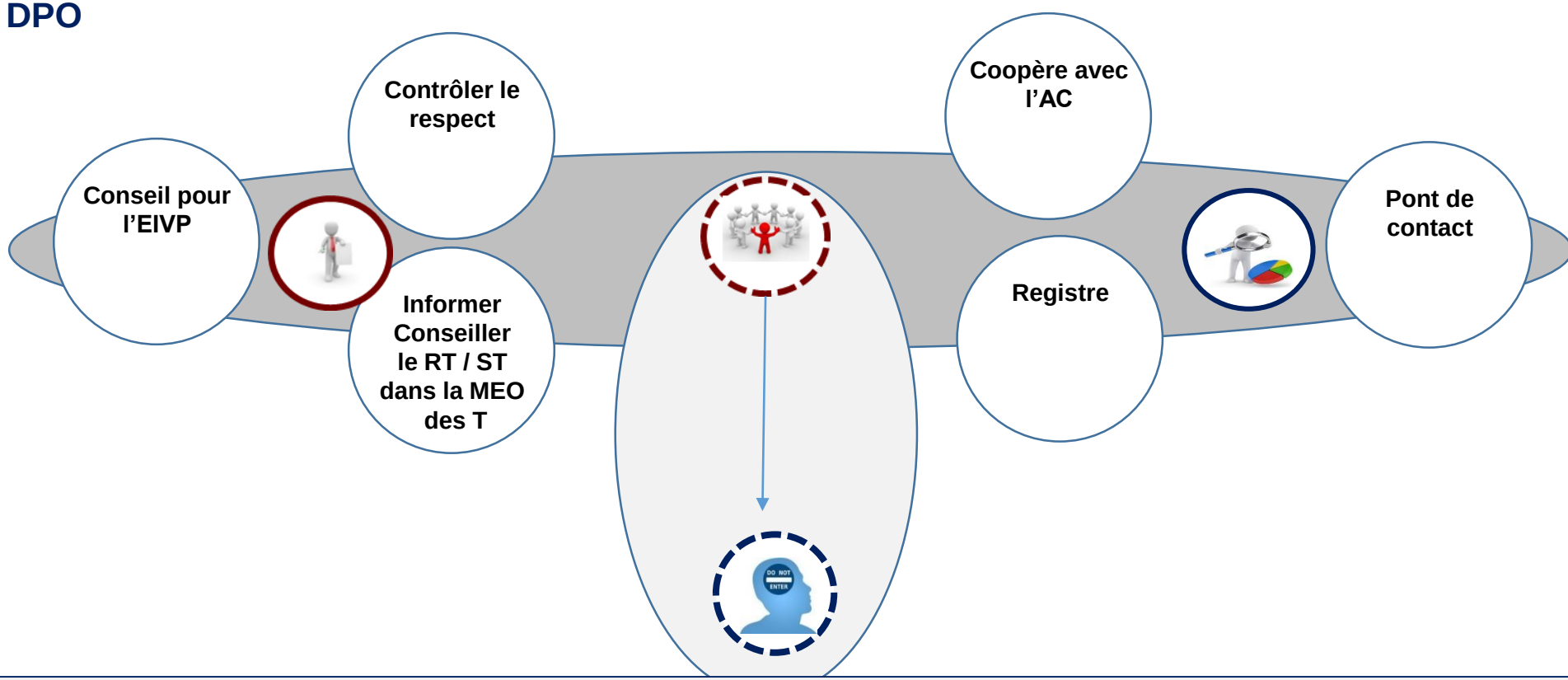
DPO


Coordonnées du DPO
Service public
Désigne un DPO
Désigne un DPO
Désigne un DPO
Désigne un DPO
Coordonnées du DPO

DPO

	Nouveautés
Désignation	**La désignation d'un DPO est obligatoire:** • **Le traitement est effectué par une autorité publique ou un organisme public,** • **Les activités de base du RT ou du sous-traitant consistent en des opérations de traitement qui exigent un suivi régulier et systématique à grande échelle des PC ,** • **Il s'agit de traitement de DCP particulières (condamnations pénales et infractions et données de santé, convictions religieuses, vie ou orientation sexuelle, données biométriques, données génétiques, origine raciale ethnique etc.).** **Le Règlement précise que le RT ou le sous-traitant (aucune mention dans le Décret) publient les coordonnées du DPO à l'autorité de contrôle.** **Connaissances spécialisées du droit et des pratiques en matière de protection des données.**
Missions	• **Informer et conseiller le RT ou le sous-traitant** • **Contrôler le respect du présent Règlement** • **Dispenser sur demander des conseils relatifs à l'EIVP** • **Coopérer avec l'autorité de contrôle** • **Faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement.** **Ainsi la nouvelle réglementation insiste sur la dispense de conseil en ce qui concerne l'EIVP et la coopération et être le point de contact avec l'autorité de contrôle.** **Cependant, le Règlement ne mentionne pas l'établissement du bilan annuel**

DPO



les fonctions suivantes sont susceptibles de donner lieu à un conflit d'intérêts :

- **secrétaire général,**
- **directeur général des services,**
- **directeur général,**
- **directeur opérationnel,**
- **directeur financier,**
- **médecin-chef,**
- **responsable du département marketing,**
- **responsable des ressources humaines ou**
- **responsable du service informatique,**
- **mais également d'autres rôles à un niveau inférieur de la structure organisationnelle si ces fonctions ou rôles supposent la détermination des finalités et des moyens du traitement.**

Conclusion

Les principales évolutions sont les suivantes :

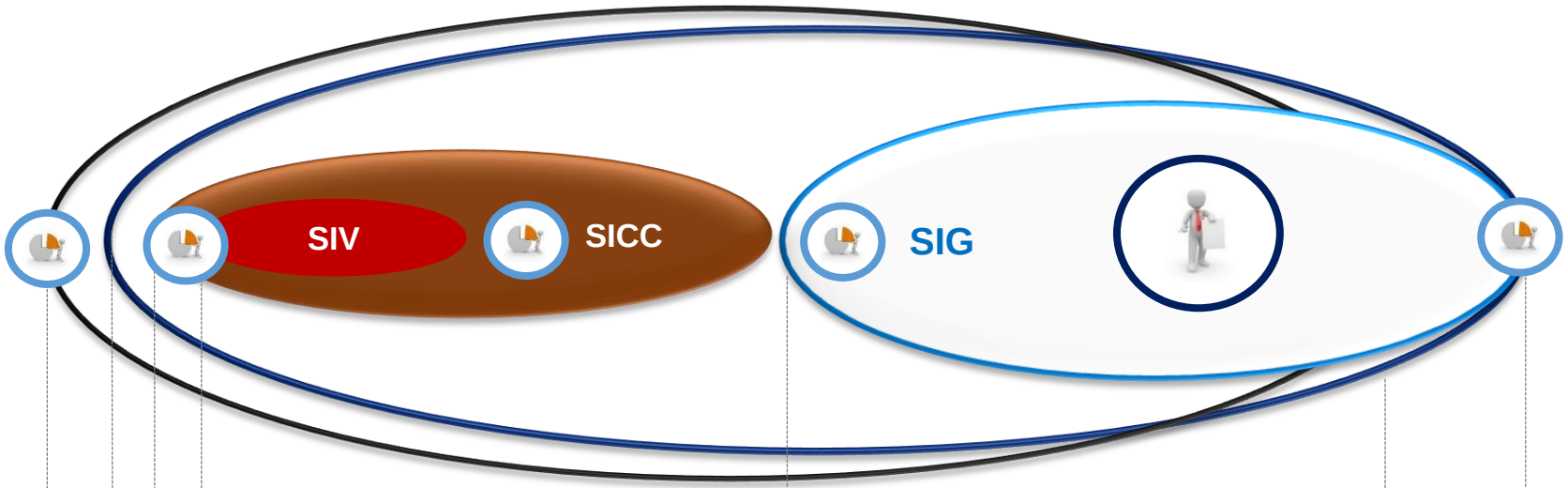
- Création de nouveaux droits pour les PC
- La responsabilité des RT est renforcée et le RT doit apporter les preuves de mise en conformité
- La responsabilité et les obligations des ST sont renforcées
- La sécurité des DCP devient un principe fondamental de la protection de la vie privée
    - De nouveaux concepts sont à appliquer : EIVP / PIA, Sécurité par défaut, Privacy By Design, …
- Les missions du DPO évoluent vers le contrôle
- Les amendes administratives ont considérablement augmenté
- La coopération entre les autorités de contrôle se renforce
- Les autorités de contrôle vont définir des codes de conduite et des certifications / labels

Le délai de mise en conformité est fixé à fin mai 2018 : ce délai est cours.

Il convient de mettre en œuvre un plan d'actions permettant d'atteindre cet objectif dans les meilleurs délais : 2017 est une année importante pour la mise en conformité

Le Plan d’actions

LES PÉRIMÈTRES



Système d'Information Vital

Système d'Information Contrôle de Commande

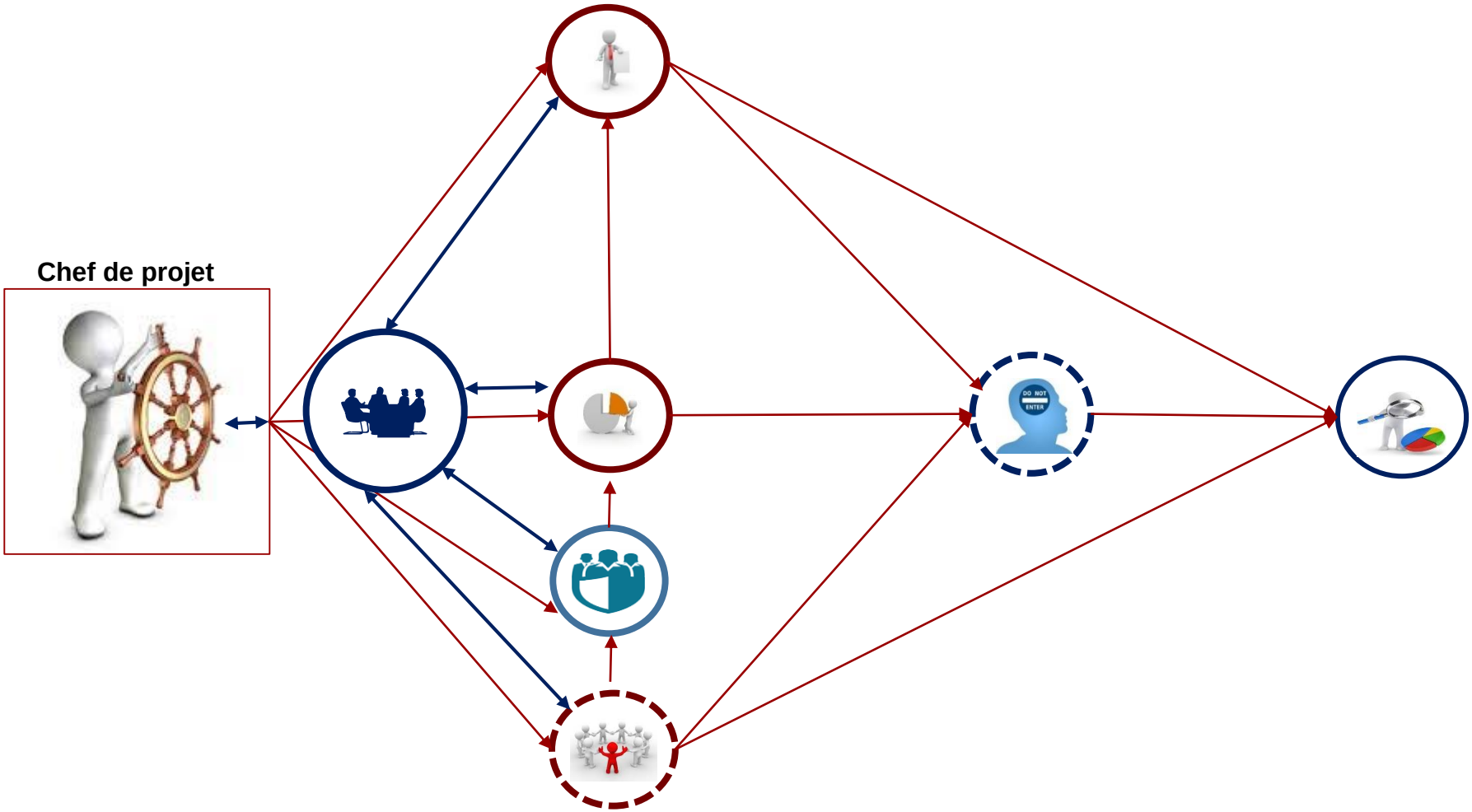
Système d'Information Gestion (sédentaire, nomade ou externalisé)

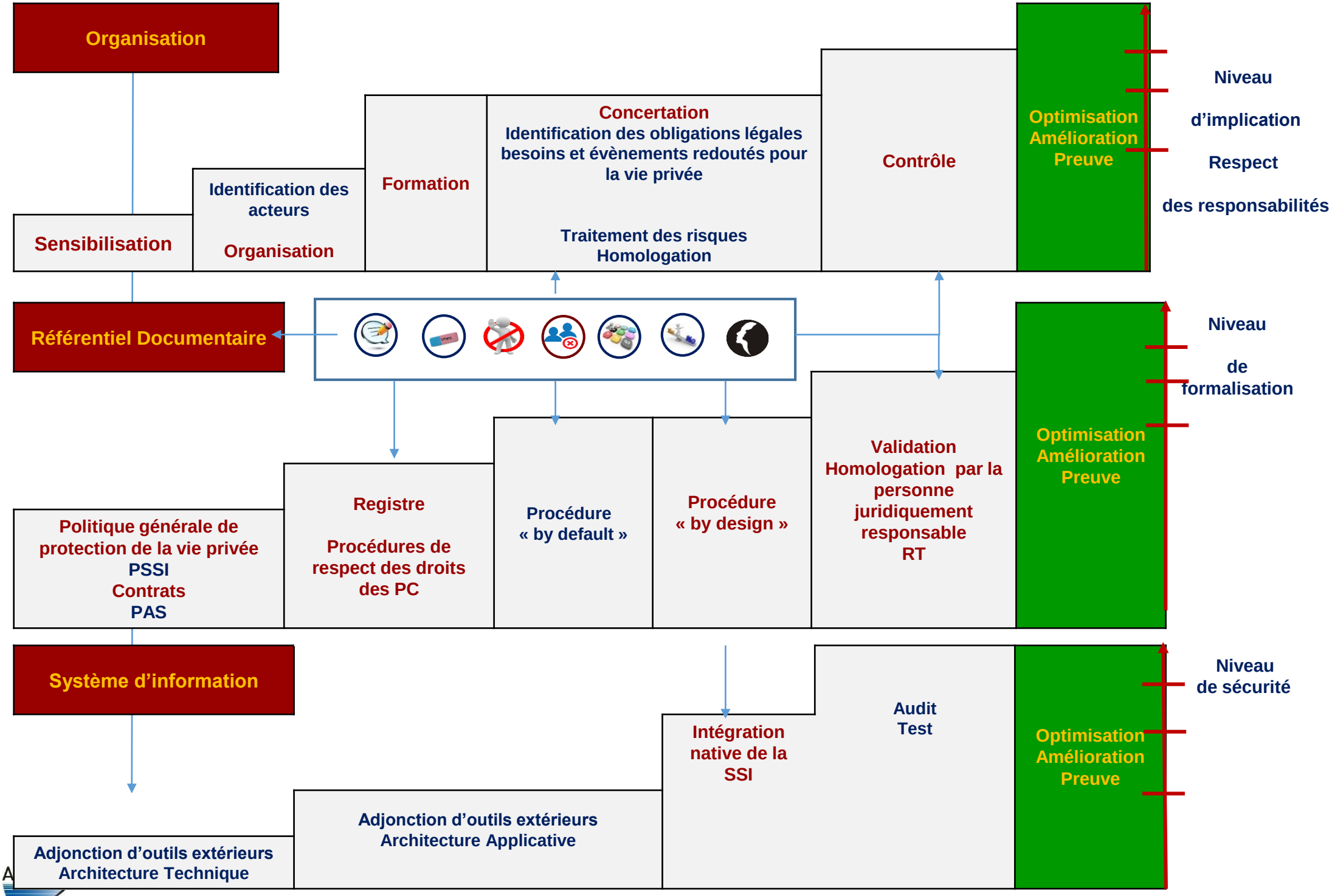
Installations

Patrimoine Informationnel Organisme

DCP

Le Plan d'actions : La démarche / Identifier les acteurs




Organisation
Sensibilisation
Identification des acteurs
Organisation
Formation
Concertation
Identification des obligations légales besoins et évènements redoutés pour la vie privée
Traitement des risques
Homologation
Contrôle
Optimisation
Amélioration
Preuve
Niveau d'implication
Respect des responsabilités
Référentiel Documentaire
Politique générale de protection de la vie privée
PSSI
Contrats
PAS
Registre
Procédures de respect des droits des PC
Procédure « by default »
Procédure « by design »
Validation Homologation par la personne juridiquement responsable
RT
Optimisation
Amélioration
Preuve
Niveau de formalisation
Système d'information
Adjonction d'outils extérieurs
Architecture Technique
Adjonction d'outils extérieurs
Architecture Applicative
Intégration native de la SSI
Audit
Test
Optimisation
Amélioration
Preuve
Niveau de sécurité

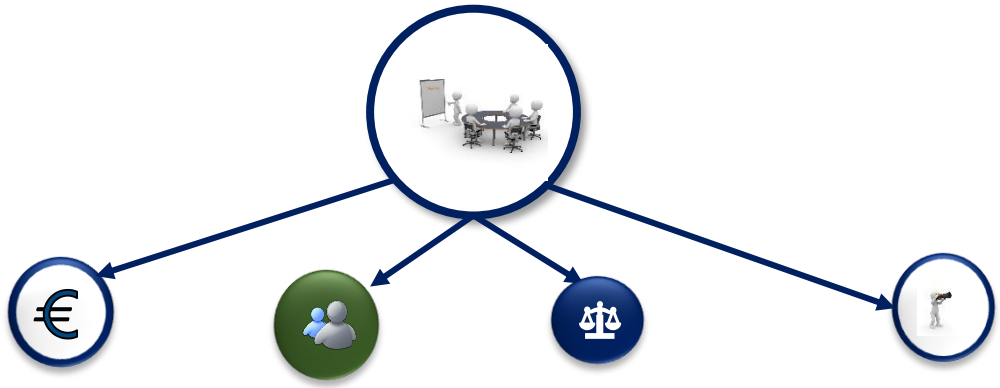
Le Plan d'actions : Les mesures juridiques / Sensibilisation du RT

Analyses et commentaires d'AGERIS Group

Le montant des sanctions administratives a considérablement augmenté, ce qui démontre la volonté des autorités compétentes de renforcer la protection de la vie privée des citoyens européens et de pousser les organismes à se mettre en conformité avec la législation.

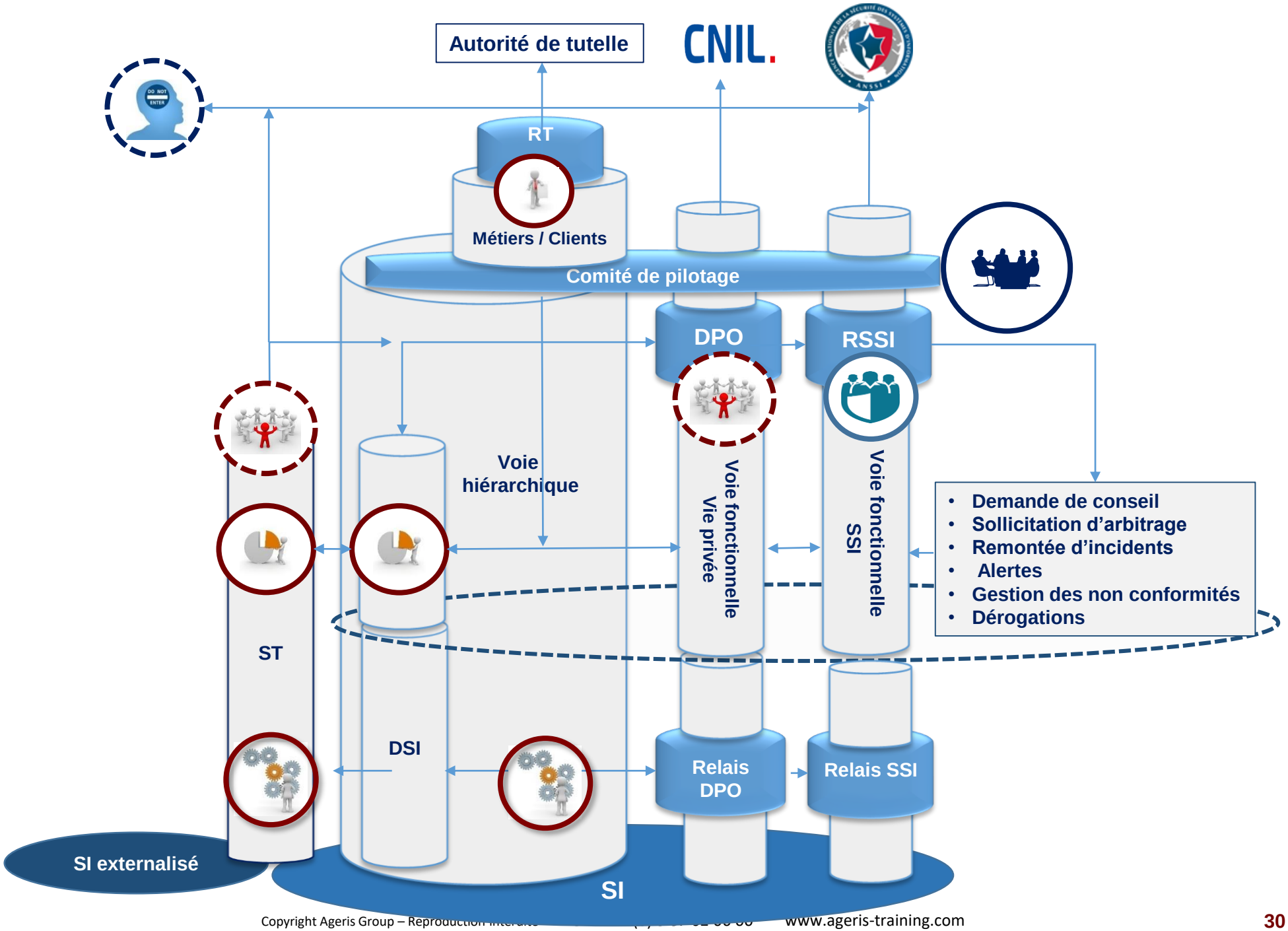
Il est fort probable (en tout les cas il faut le souhaiter) que la médiatisation des actions engagées par une autorité de contrôle et cette augmentation du montant des actions deviennent dissuasives et poussent les responsables d'organismes à engager les démarches nécessaires de mise en conformité.

Une sensibilisation sur ces risques juridiques, médiatiques, …. est à engager en interne pour pousser à la mise en œuvre de la gouvernance adéquate et renforcer les démarche de mise en conformité.

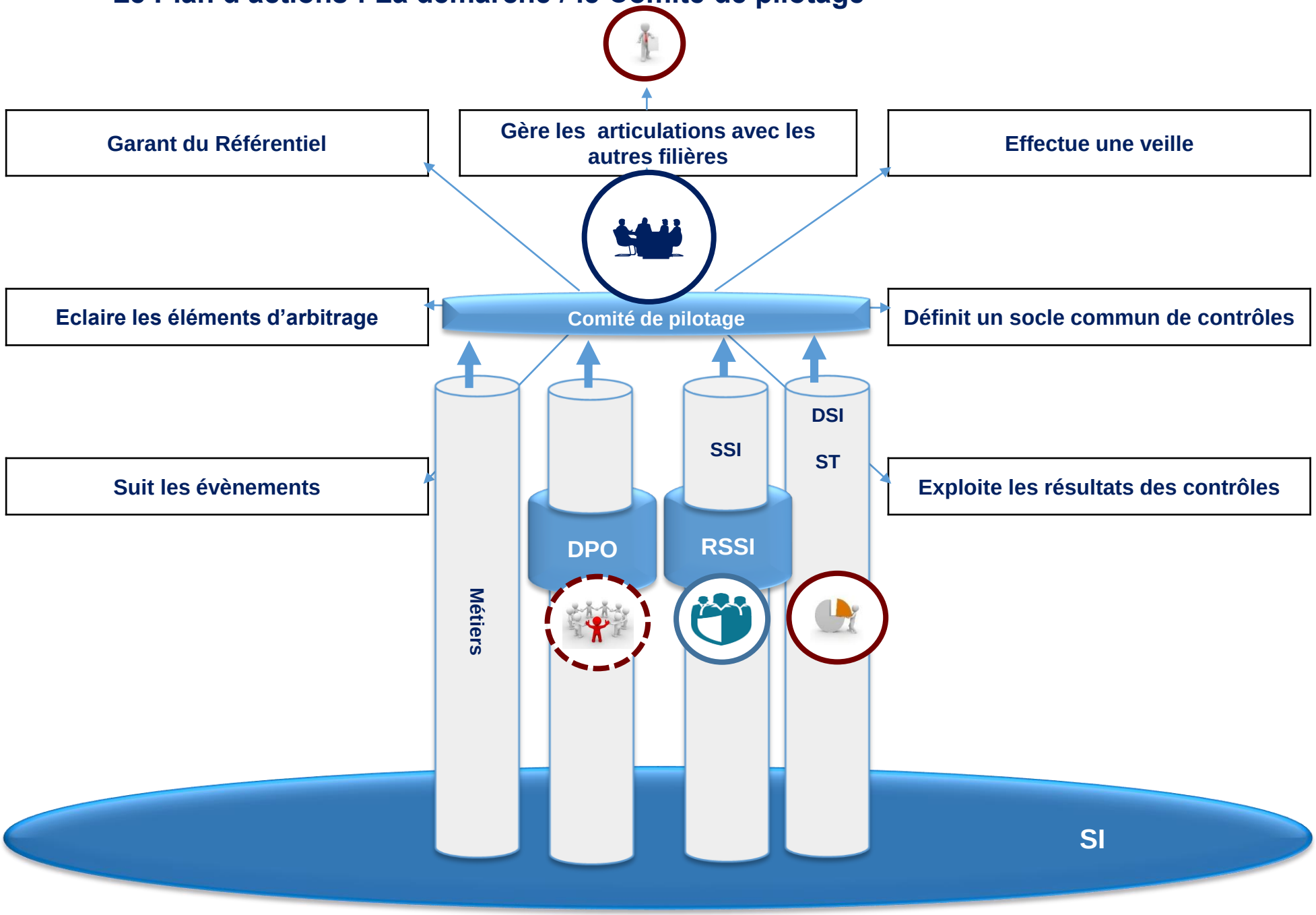


Les responsabilités du RT : «responsable du traitement», la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement

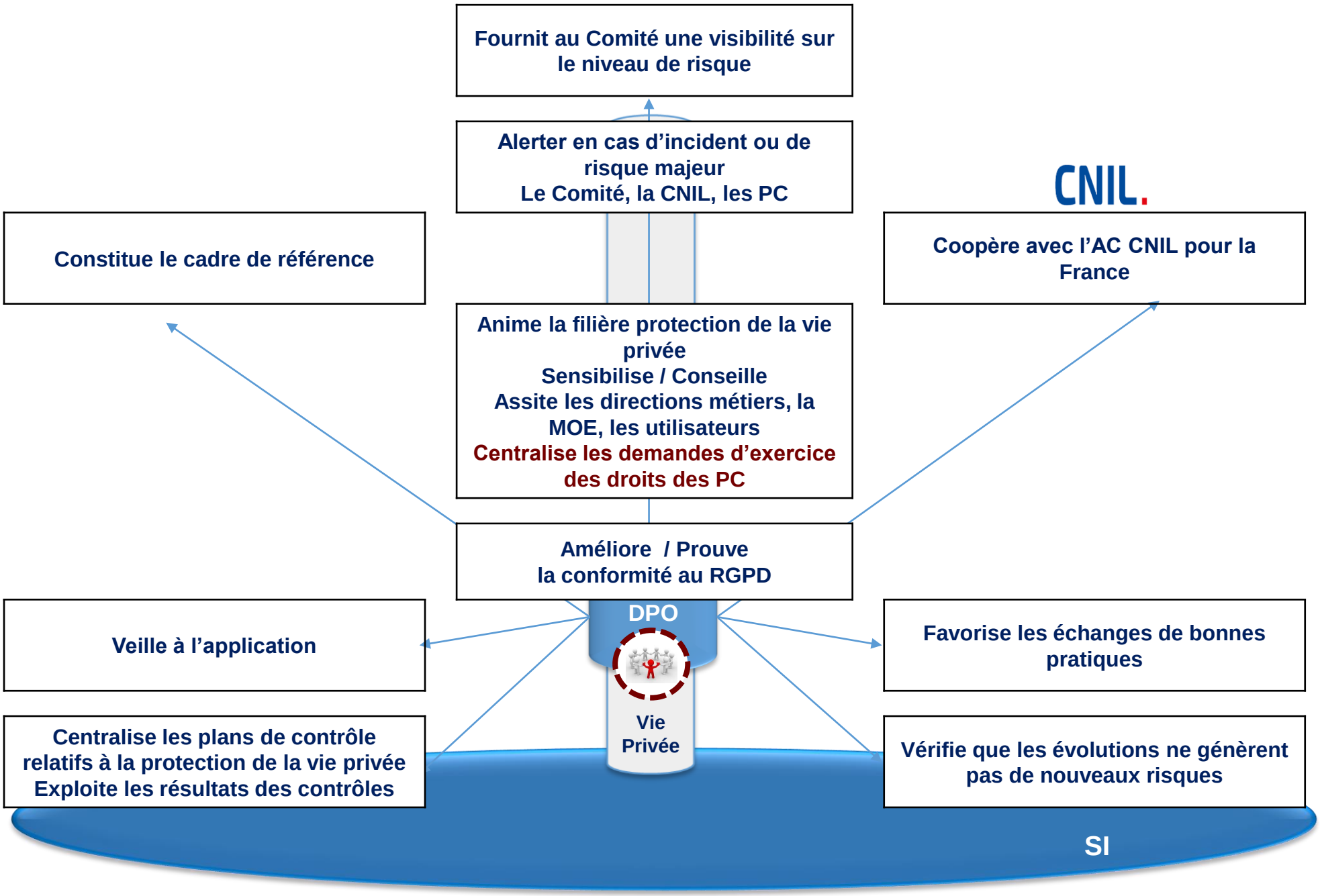
Le Plan d'actions : La démarche / Identifier les acteurs / Les voies fonctionnelles / Comité de pilotage



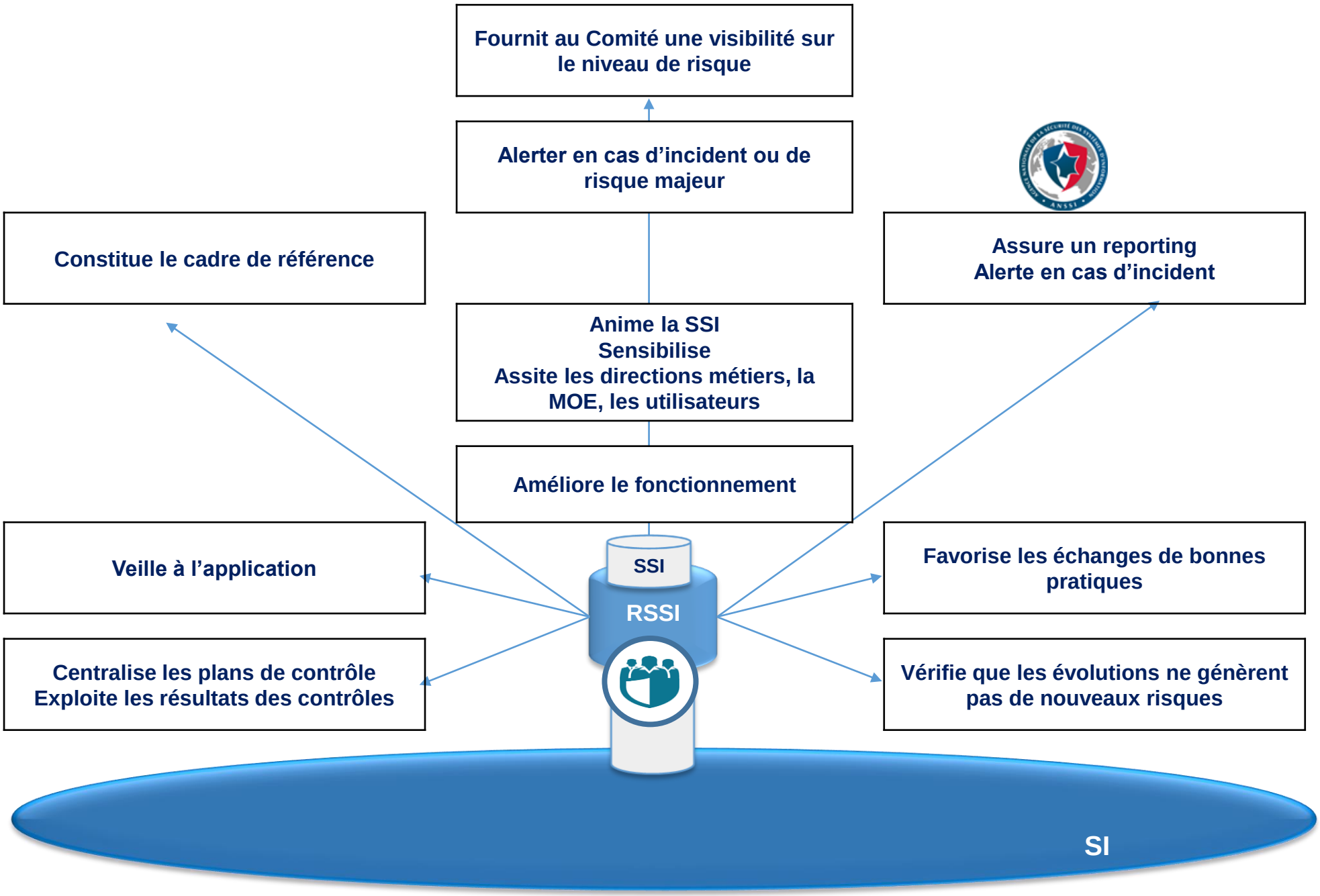
Le Plan d'actions : La démarche / le Comité de pilotage



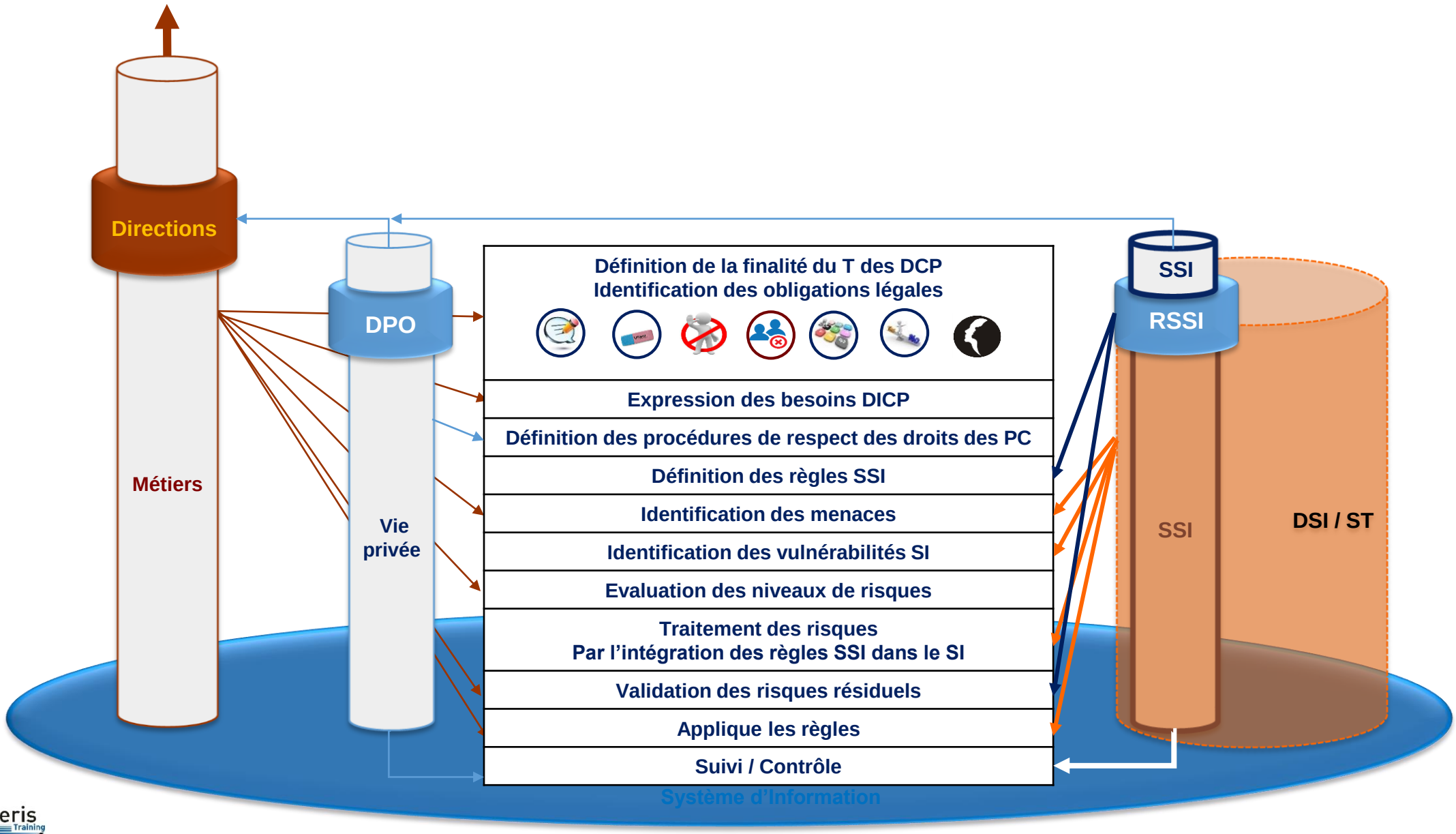
Le Plan d'actions : La démarche / Identifier les acteurs / Le DPO

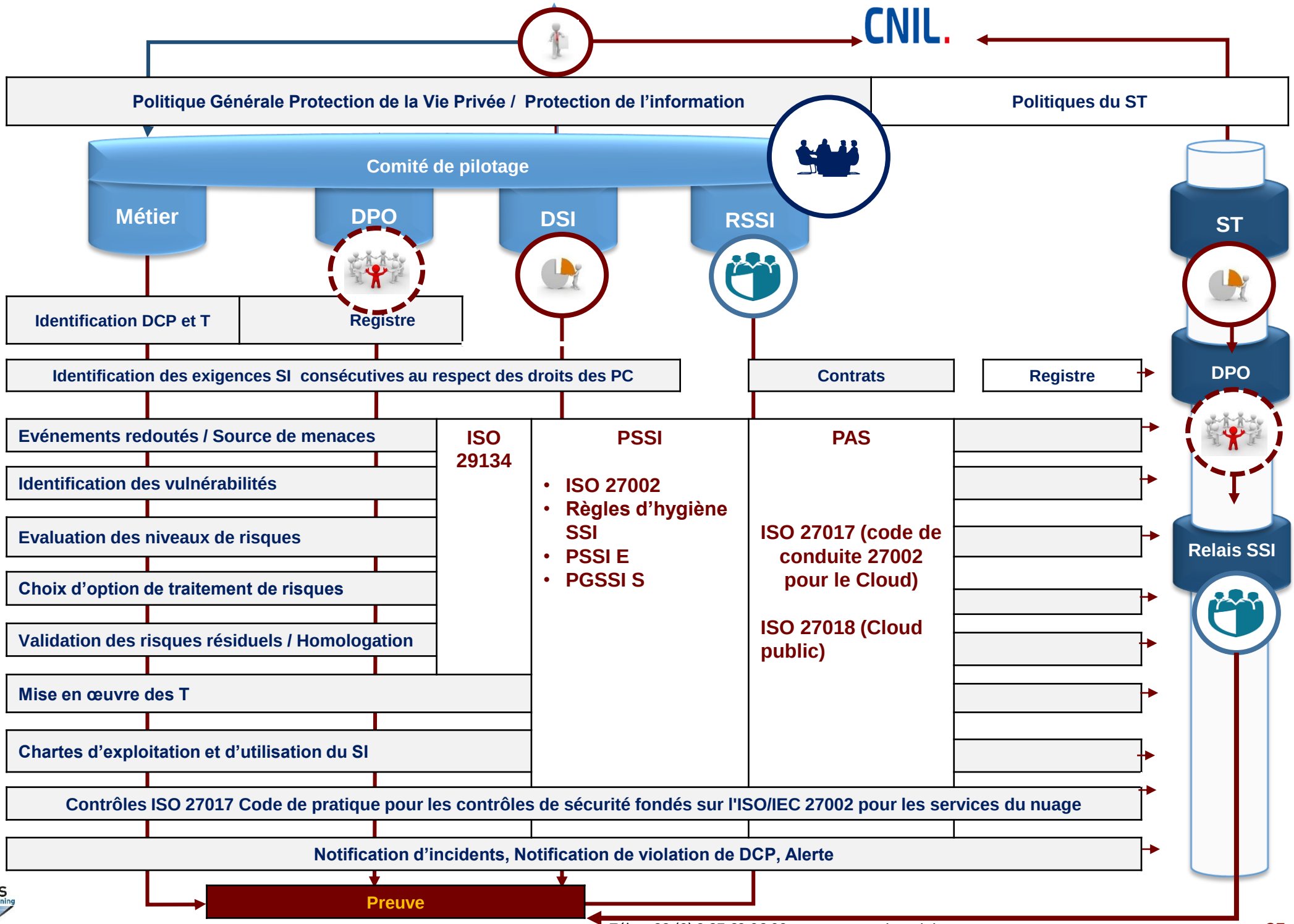


Le Plan d'actions : La démarche / Identifier les acteurs / L'organisation / Le RSSI

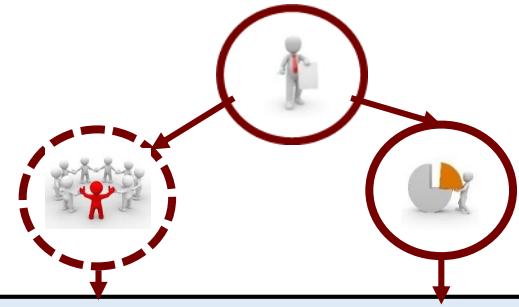


Le Plan d'actions : L'articulation entre les voies hiérarchiques et fonctionnelles




CNIL.
Politique Générale Protection de la Vie Privée / Protection de l'information
Politiques du ST
Comité de pilotage
Métier
DPO
DSI
RSSI
ST
Identification DCP et T
Registre
Identification des exigences SI consécutives au respect des droits des PC
Contrats
Registre
DPO
Evénements redoutés / Source de menaces
Identification des vulnérabilités
Evaluation des niveaux de risques
Choix d'option de traitement de risques
Validation des risques résiduels / Homologation
ISO 29134
PSSI
ISO 27002
Règles d'hygiène SSI
PSSI E
PGSSI S
PAS
ISO 27017 (code de conduite 27002 pour le Cloud)
ISO 27018 (Cloud public)
Relais SSI
Mise en œuvre des T
Chartes d'exploitation et d'utilisation du SI
Contrôles ISO 27017 Code de pratique pour les contrôles de sécurité fondés sur l'ISO/IEC 27002 pour les services du nuage
Notification d'incidents, Notification de violation de DCP, Alerte
Preuve

Le Plan d'actions : Les mesures organisationnelles et techniques / Politique de sécurité



Le renforcement de la sécurité

La mise en œuvre de politiques :

Engagement pour la protection de l'information
Politique générale de protection de l'information
Politique générale pour la protection de la vie privée et la sécurité des DCP

- Enjeux stratégiques
- **Engagement de responsabilité**
- Périmètre
- démarche

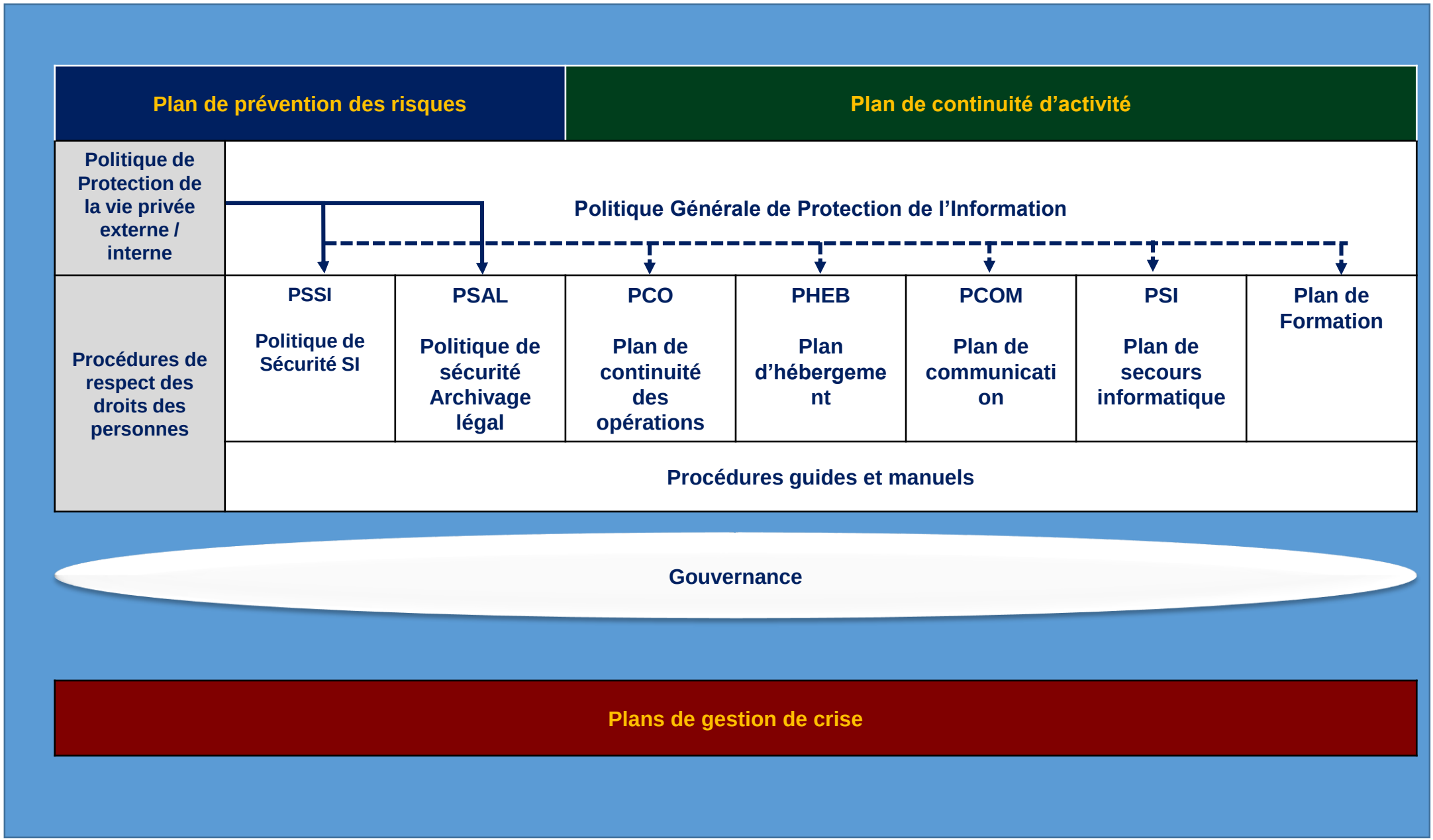
Politique de Sécurité Système d'Information

- Les règles fonctionnelles et organisationnelles

Plans de Sécurité
Guides et manuels EIVP / PIA
Chartes utilisateurs
Procédures de respect des droits des PC

- La mise en œuvre opérationnelle des règles fonctionnelles et la définition des procédures notamment pour le respect des droits des PC et , consignes et règles de sécurité

Le Plan d'actions : Le référentiel documentaire



Le Plan d'actions : Le référentiel documentaire

Type d'impact	Non significatif (Niveau1)	Significatif (Niveau 2)	Grave (Niveau 3)	Très grave (Niveau 4)	Catastrophique Niveau 5
Incapacité à réaliser la mission ou le contrat	Non significatif (Exemple une heure)	Accès internet indisponible pour un temps donné (Exemple trois heures)	Non fonctionnement des logiciels métiers pour un temps donné (Exemple une journée)	Non fonctionnement des logiciels métiers pour un temps donné (Exemple une semaine)	Paralysie des services suite à un arrêt complet du SI (Exemple plus d'une semaine)
Non-respect des obligations légales	Non significatif	Contentieux juridiques simples hors procédure pénale.	Nombreux contentieux juridiques hors procédures pénales	Engagement des responsabilités juridiques des dirigeants	Engagement des responsabilités juridiques des dirigeants
Perte d'image	Non significatif	Rumeurs locales auprès des clients pendant une courte durée	Affectation de l'image dans les médias locaux pendant une journée	Affectation de l'image dans les médias locaux pendant plusieurs jours	Affectation de l'image pendant plusieurs jours dans les médias nationaux
Perte financière	Perte financière inférieur à 0,1%	Perte financière entre 0,1 à 1% du budget	Perte financière entre 1 à 10% du Budget	Perte financière supérieure à 10% au budget	Perte financière supérieure au budget
Climat de travail	Mécontentement isolé	Mécontentement d'une équipe ou d'un service	Mécontentement d'une ou plusieurs directions	Grève limitée	Grève illimitée

Le Plan d'actions : Le référentiel documentaire

Evènements redoutés	Types d'impacts	Donnés courantes	Données sensibles	Données très sensibles
Accès illégitime aux DCP **Modification non désirée des DCP** **Disparition des DCP**	**Corporel** 	Etat civil, identité, données d'identification Vie personnelle habitude de vie, situation familiale, hors données sensibles, très sensibles ou dangereuses Informations d'ordre économique et financier revenus, situation financière, situation fiscale Données de connexion (adresses IP, journaux d'évènements, Données de localisation,	Numéro de sécurité sociale (NIR) Données biométriques	Opinions philosophiques, politiques, religieuses, syndicales, vie sexuelle, données de santé, origine raciales ou ethniques, relatives à la santé ou la vie sexuelle.
	Matériel 			
	Moral 			

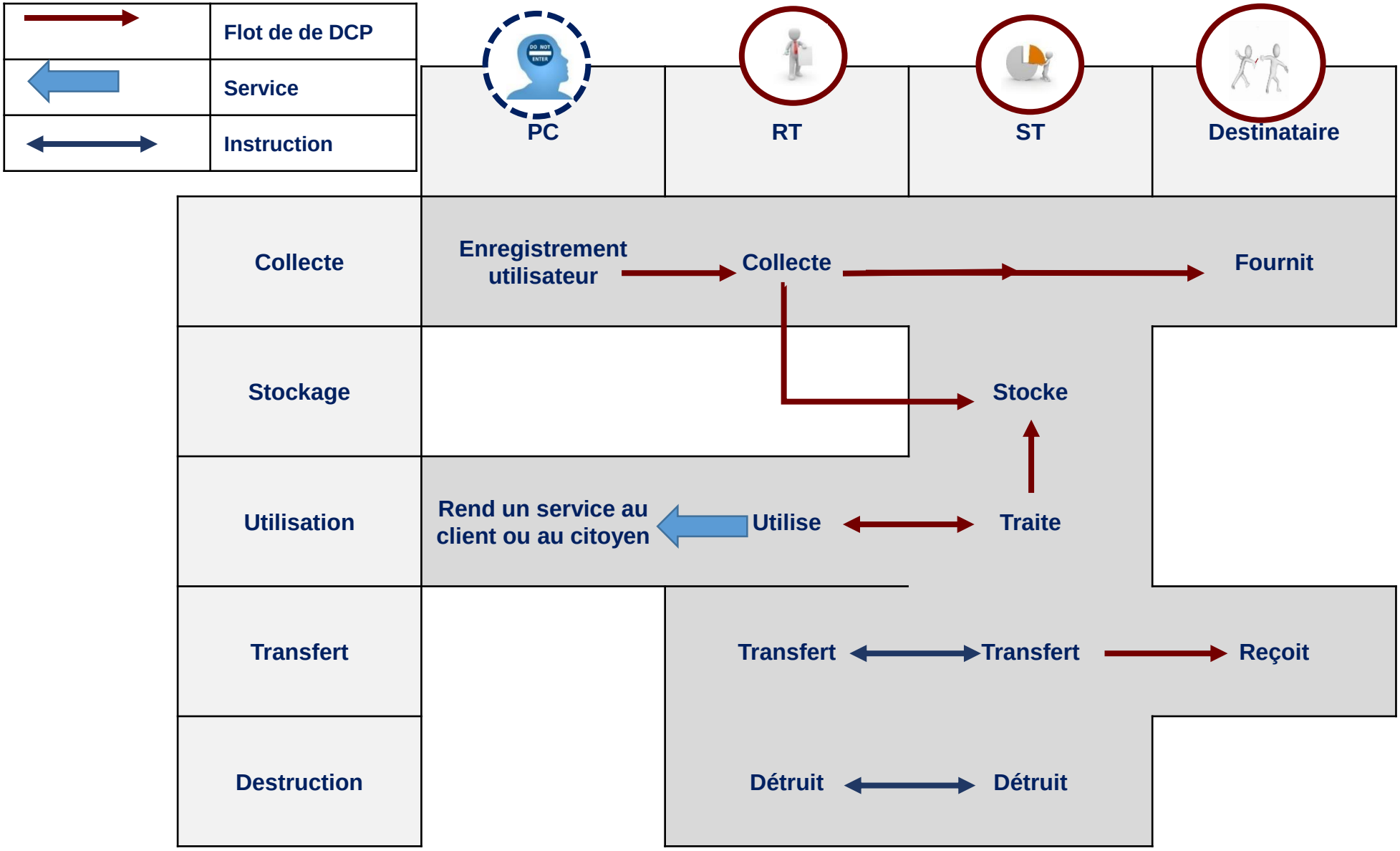
Le Plan d'actions : Le référentiel documentaire

Impact / Gravité	Potentialité / Vraisemblance				
	0	1	2	3	4
4	N/A	3	3	4	4
3	N/A	2	2	3	4
2	N/A	1	2	2	3
1	N/A	1	1	1	2

Gravité					
	Catastrophique	Niveau 2	Niveau 2	Niveau 3	Niveau 3
	Très grave	Niveau 2	Niveau 2	Niveau 2	Niveau 3
	Grave	Niveau 1	Niveau 2	Niveau 2	Niveau 2
	Significatif	Niveau 1	Niveau 1	Niveau 2	Niveau 2
	Non significatif	Niveau 1	Niveau 1	Niveau 1	Niveau 1
		Très faible	Faible	Moyenne	Forte
		Vraisemblance			

Gravité					
	4. Maximal				
	3. Important				
	2. Limitée				
	1. Négligeable				
Cartographie des risques		1. Négligeable	2. Limitée	3. Important	4. Maximal
		Vraisemblance			

Le Plan d'actions : Le Registre / Identifier les traitements et les flux



Le Plan d'actions : Le Registre

Le nom et les coordonnées du RT et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du DPO	
Les finalités du T	**Gestion de clientèle, gestion du personnel, dispositif de vidéosurveillance ayant pour finalité la sécurité des biens et des personnes, dispositif biométrique reposant sur un stockage des gabarits en base mis en œuvre pour contrôler l'accès aux locaux, appareils et applications informatiques utilisés sur les lieux de travail.**
Une description des catégories de PC et des catégories de DCP	**Les salariés, les clients de l'entreprise etc.** **Nom, prénom, date de naissance, adresse postale, adresse courriel, relevé d'identité bancaire etc.**
Les catégories de destinataires auxquels les DCP personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales	**Les personnes gérant la sécurité d'accès aux locaux, les personnes gérant le restaurant d'entreprise, les personnes chargées de la gestion du personnel (RH par ex.), les instances représentatives du personnel etc.**
Les transferts de DCP vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'art. 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées.	**Binding Corporate Rules (BCR), Clause contractuelle type (CCT), pays assurant un niveau de protection suffisant.**
Les délais prévus pour l'effacement des différentes catégories de données	**1 mois pour la vidéosurveillance, le temps de la période d'emploi de la personne concernée (après possibilité d'archivage) etc.**
Une description générale des mesures de sécurité techniques et organisationnelles	**Contrôle d'accès, habilitation, cloisonner les DCP, réduire les vulnérabilités des logiciels, lutte contre les codes malveillants, chiffrer les DCP, anonymiser les DCP, contrôler l'accès physique aux locaux, prévenir les risques (incendie, inondation etc.) etc.**

Le Plan d'actions : Les mesures juridiques / Le Contrat

Contrat	
La gestion des DCP – art. 28 du Règlement européen	**Les mentions légales obligatoires / Les mentions légales facultatives (liste non-exhaustive)**
1.Traitement des données que sur instruction documentée du RT, **2.Respect de la confidentialité,** **3.Mise en place de mesures techniques et organisationnelles afin d'assurer la sécurité des DCP,** **4.Demander l'autorisation au RT avant de recruter un autre ST,** **5.Aider le RT à répondre aux demandes de droit d'accès, de rectification, de suppression et d'opposition des PC,** **6.Veiller au respect de certaines obligations légales (sécurité du traitement, notification à l'autorité de contrôle en cas de violation de DCP, communication à la personne concernée, EIVP, consultation préalable).** **7.Suppression des DCP au choix du RT,** **8.Mise à la disposition du RT de toutes les informations nécessaires afin d'apporter la preuve du respect des obligations.**	**Objet du contrat:** quelles prestations le ST s'engage à fournir au RT**.** • **Rémunération et modalités de paiement:** virement, chèque etc. • **Délais d'exécution de la prestation:** respect des délais d'exécution etc. • **Exécution, vérification et acceptation: les** obligations du ST sont réputées exécutées lorsque ce dernier aura effectué les prestations auxquelles il s'est engagée; le RT devra vérifié sans délai l'exécution des prestations convenues; le RT est réputé avoir accepté les prestations effectuées lorsque celles-ci correspondent aux résultats des prestations convenues. • **Obligations du ST:** le ST s'engage à fournir les prestations convenues avec toute la diligence requise; à effectuer un suivi des prestations; un devoir de formation en matière de sécurité auprès de ses collaborateurs; une obligation d'informer, de conseiller et d'alerter le client à la bonne compréhension des services fournis etc. • **Obligations du RT:** communication au ST de tous les documents et informations nécessaires pour l'exécution des prestations etc. • **Responsabilités du ST: Engagement de sa responsabilité** • **Responsabilités du RT: Engagement de sa responsabilité** • **Confidentialité et obligations communes:** le ST s'engage à respecter les exigences de sécurité et de confidentialité du client dans le cadre de la prestation. Le ST s'engage à considérer comme strictement confidentiels au sein de sa propre organisation ainsi que vis-à-vis des tiers les informations, documents de toute nature et savoir-faire qui lui seront transmis par le RT dans le cadre de la prestation. • **Propriété et utilisation des droits,** • **Lutte contre la contrefaçon,** • **Respect de la PSSI:** engagement du PAS. • **Clause de réversibilité,** • **Résiliation,** • **Maintien en vigueur du contrat,** • **Audibilité ,** • **Loi applicable, Juridiction compétente.**

Le Plan d'actions : Les mesures organisationnelles et techniques / le PAS

Le Plan d'Assurance Sécurité est un document contractuel décrivant l'ensemble des dispositions spécifiques mises en œuvre pour garantir le respect des exigences de sécurité du donneur d'ordre, le RT .

Il doit être annexé au contrat

Externalisation des services liés aux ressources du SI/ Le PAS : Le Plan d'Assurance Sécurité

	ACHETEUR	PRESTATAIRE
	Structure de l'organisation relative à la Sécurité	
	Interfaces Gestion de la communication	
	Rôles et responsabilités des intervenants	
Domaine d'application /		Transcription effective des Mesures de sécurité
Objectif et périmètre de la prestation	Identification des DCP Classification des besoins DICP / évènements redoutés	• La gestion du personnel • La gestion de la prestation pendant le différentes phases avant, en cours, en sortie de la prestation • Le contrôle d'accès logique et aux habilitations • La sécurité physique des installations et sites • Liées à l'exploitation • Flux d'informations • Documentation d'exploitation • Gestion des vulnérabilités / traitement des risques • Gestion des changements et des évolutions • Surveillance et traçabilité • Gestion des alertes, incidents et anomalies • Gestion de la continuité d'activité • Conformité à la réglementation

Garantie de la licéité et le consentement de la personne concernée: l'ex. des « cookies »

1. **Le consentement doit être préalable à l'insertion ou à la lecture des cookies.**

Tant que la personne n'a pas donné son consentement, ces cookies ne peuvent être déposés ou lus sur son terminal.
Il doit être requis à chaque fois qu'une nouvelle finalité vient s'ajouter aux finalités initialement prévues.

2. **La validité du consentement est liée à la qualité de l'information reçue.**

L'information doit être visible, mise en évidence et complète.
Elle doit être rédigée en des termes simples et compréhensibles pour tout utilisateur.
Elle doit permettre aux internautes d'être parfaitement informés des différentes finalités des cookies.

3. **Le consentement n'est valide que si la personne exerce un choix réel.**

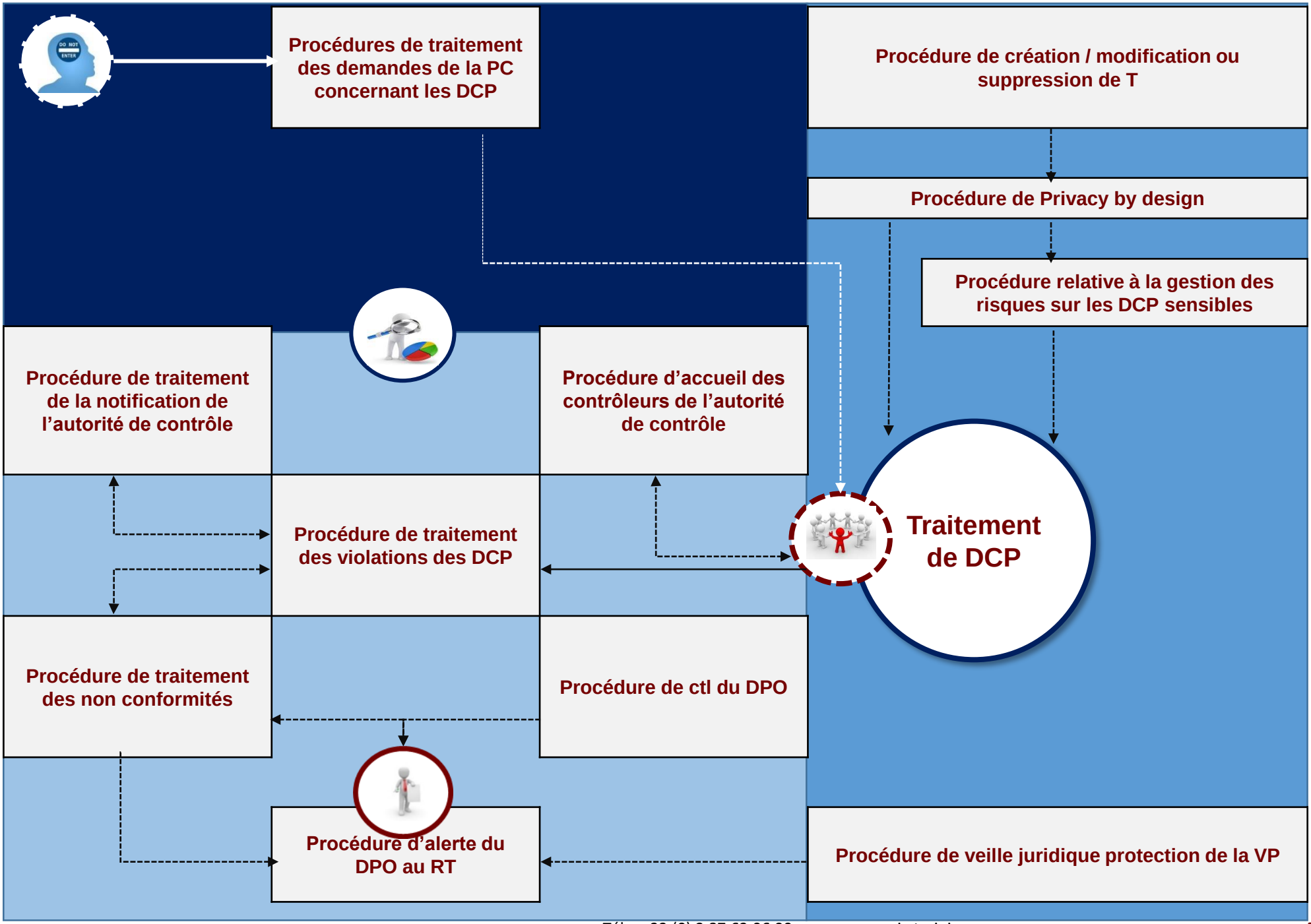
L'utilisateur doit pouvoir accepter ou refuser le dépôt des cookies.
Le consentement ne peut être valable que si la personne concernée est en mesure d'exercer valablement son choix et n'est pas exposée à des conséquences négatives importantes si elle refuse de donner son consentement. La personne qui refuse un cookie nécessitant un consentement doit pouvoir continuer à bénéficier du service (l'accès à un site internet par exemple).

Le choix doit pouvoir être effectué pour chaque application et chaque site internet.

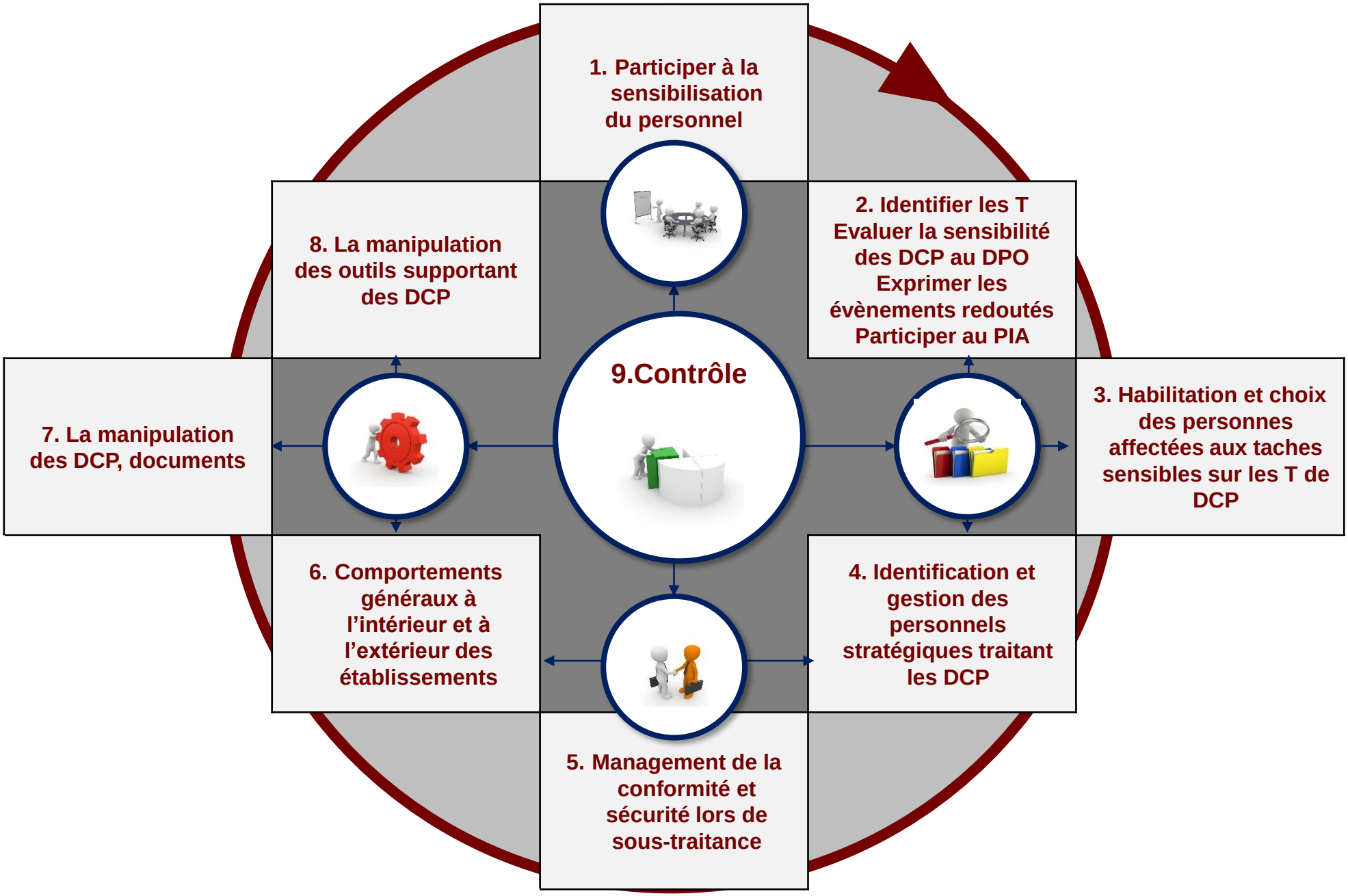
4. **Le consentement doit pouvoir être retiré par l'internaute.**

Des solutions conviviales doivent être mises en œuvre pour que la personne puisse retirer, à tout moment, son consentement aussi facilement qu'elle a pu le donner.

Le Plan d'actions : Les mesures organisationnelles et techniques / les procédures



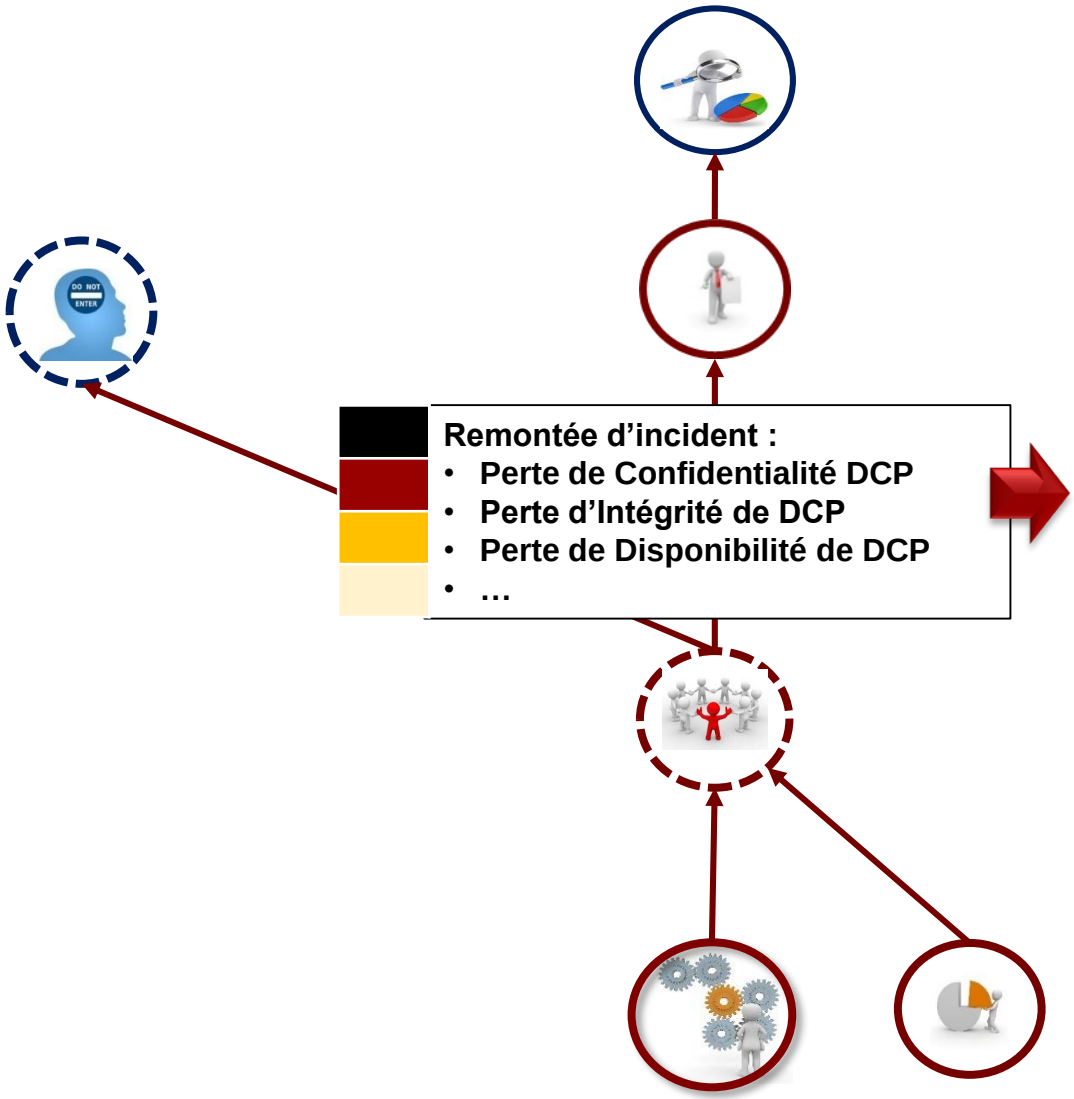
Le Plan d'actions : Les mesures organisationnelles et techniques
La sensibilisation de l'encadrement



Le Plan d'actions : Les mesures juridiques / Sensibilisation des collaborateurs

Devoirs	Droits
Respecte le Règlement engage sa responsabilité Définit des règles Informe les personnels sur: Les risques Les règles Les dispositifs de surveillance Les éventuels contrôles Les niveaux de responsabilité individuelle Met en place les dispositifs de protection Valide les risques résiduels Contractualise avec le ST Répond aux demandes des PC Analyse / Contrôle Informe l'autorité de contrôle des violations de DCP	Droit de connaitre : • Les règles • Les responsabilités • Les dispositifs de surveillance • Les contrôles Droit d'exercer les droits de la personne concernée
Respecte les lois et les règles Devoir de loyauté Informe le RT des éventuels incidents	Définit des règles Met en place des dispositifs de surveillance Met en place des dispositifs de contrôle Engage la responsabilité des utilisateurs Engage la responsabilité du sous traitant

Le Plan d'actions : Les mesures juridiques / La notification de violation de DCP



Le texte européen prévoit une notification à l'autorité de contrôle dans les meilleurs délais et si possible dans les 72 heures au plus tard après en avoir pris connaissance.

Cette notification n'est pas ici cantonnée à un acteur en particulier mais à tous les acteurs dès lors qu'une atteinte aux DCP est intervenue.

- **Description de la nature de la violation de DCP,**
- **Communication du nom et coordonnées du DPO,**
- **Description des conséquences probables de la violation,**
- **Description des mesures prises ou celles que le RT propose de prendre.**

Et l'article 34 du Règlement prévoit la communication à la PC dans les meilleurs délais.
Cette disposition prévoit trois cas dans lesquels la communication n'est pas nécessaire:

- **Le RT a mis en place le chiffrement etc.**
- **Le RT a pris des mesures ultérieures garantissant le respect des droits et libertés afin qu'une nouvelle violation ne soit plus susceptible de se matérialiser,**
- **La communication exigerait des efforts disproportionnés.**

Le Plan d'actions : Les mesures organisationnelles et techniques / EIVP /Security by design

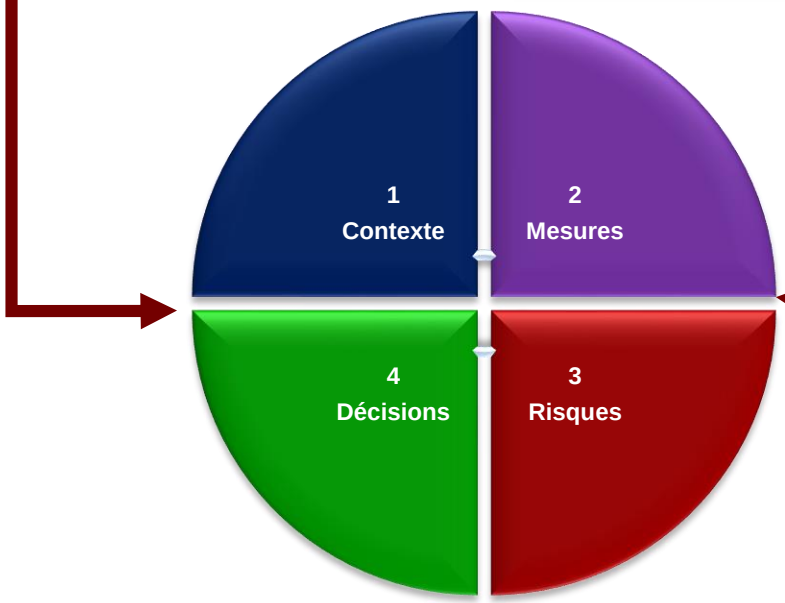
Une AIPD repose sur deux piliers :

Les principes et droits fondamentaux « non négociables »

qui sont fixés par le Règlement et doivent être respectés et ne peuvent faire l'objet d'aucune modulation, quels que soient la nature, la gravité et la vraisemblance des risques encourus

La gestion des risques sur la vie privée des personnes concernées

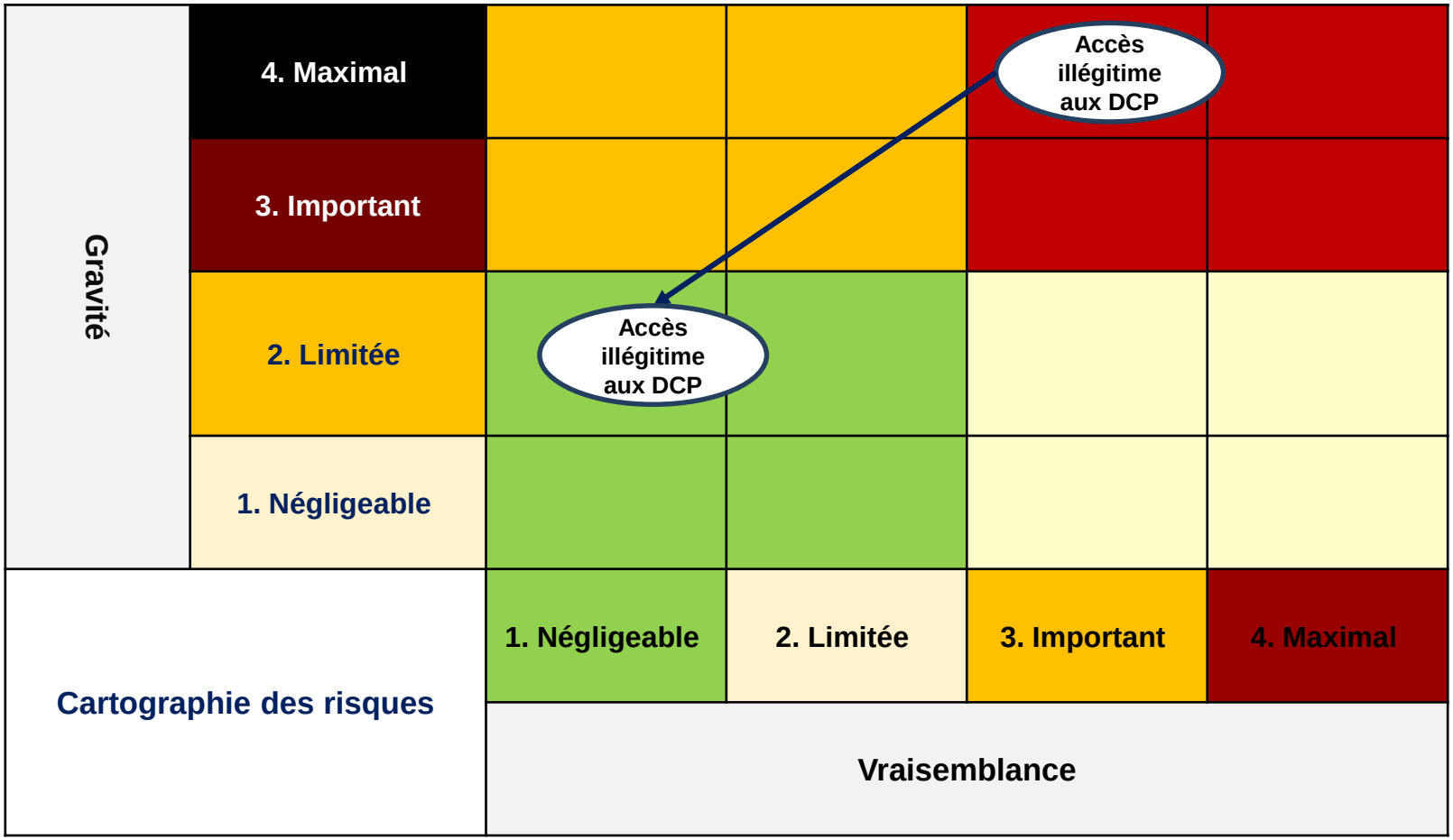
qui permet de déterminer les mesures techniques et d'organisation appropriées pour protéger les DCP



Source : – CNIL http://www.cnil.fr

Le Plan d'actions : EIVP /Security by design / Evaluation du n° du risque

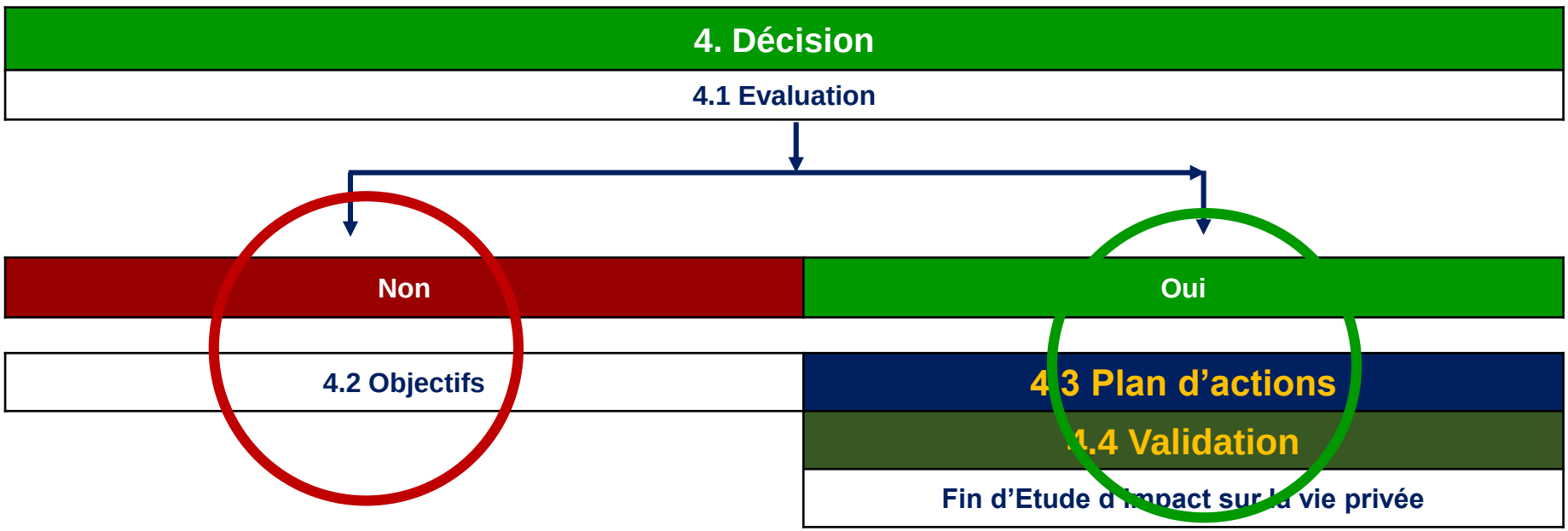
Un schéma tel que ci-dessous peut être utilisé pour présenter la cartographie des risques



Le Plan d'actions : EIVP /Security by design / la validation

Décision : la validation de l'étude d'impact sur la vie privée

L'Objectif est de décider d'accepter ou non la manière dont l'étude a été gérée et les risques résiduels.



Source : – CNIL http://www.cnil.fr

Les mesures organisationnelles et techniques / Security by default

- **La pseudonymisation et le chiffrement des données à caractère personnel;**
- **des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;**
- **des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;**
- **une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.**

Le Plan d'actions : Security by default / Pseudonymisation

Objectif : faire perdre le caractère identifiant des données à caractère personnel (DCP).

Déterminer ce qui doit être anonymisé selon le contexte, la forme de stockage des DCP (champs d'une base de données, extraits de textes…) et les risques identifiés.

Anonymiser de manière irréversible ce qui doit l'être, selon la forme des données à anonymiser (base de données, documents textuels…) et les risques identifiés.

Une « véritable » anonymisation implique nécessairement une perte (irréversible) d'information. Dans certains cas, **le simple fait d'effacer ou de noircir une partie des données peut suffire à atteindre l'objectif souhaité.**

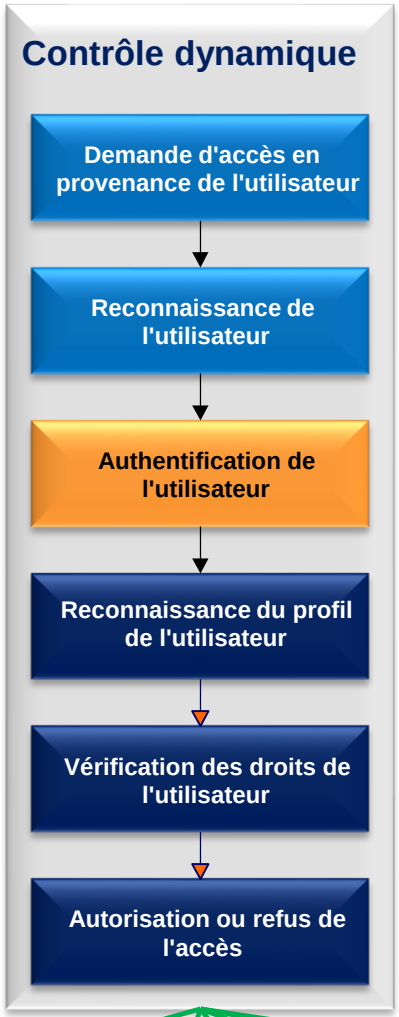
La « pseudonymisation » peut être définie comme le remplacement d'un nom par un pseudonyme. C'est le processus par lequel les DCP perdent leur caractère identifiant (de manière directe).

Les DCP restent liées à la même personne dans tous les dossiers et SI sans que l'identité ne soit révélée. Elle peut être opérée avec ou sans la possibilité de retour vers les noms ou identités (pseudonymisation réversible ou irréversible).

Recommandations :

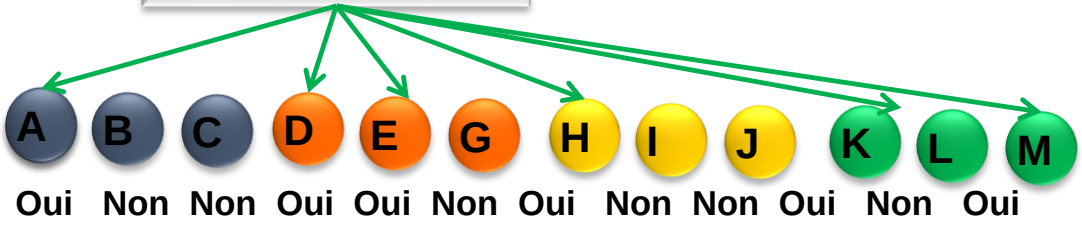
- **s'il est nécessaire que des personnes habilitées puissent vérifier que des données pseudonymisées correspondent à des données originales qu'ils ont en leur possession, pratiquer une double pseudonymisation avec deux clés secrètes détenues par deux organismes / acteurs différents**
- **s'il est nécessaire à des personnes habilitées de pouvoir retrouver les données originales (levée d'anonymat), utiliser une fonction de chiffrement, éventuellement en partageant une clé en trois parties confiées à trois personnes différentes (par exemple sur un CD ou un carte à puce) avec l'obligation qu'au moins deux des trois personnes se réunissent pour reconstituer la clé, afin de protéger la confidentialité du secret…**
- **Utiliser uniquement des DCP anonymisées ou des données fictives pour les phases de développement et de test.**

Le Plan d'actions : Les mesures organisationnelles et techniques / Les habilitations



Après avoir déterminé le niveau de sensibilité des DCP, le besoin de diffusion et de partage des ressources, les droits d'accès aux ressources doivent être gérés suivant les principes suivants :

- **besoin d'en connaître (chaque utilisateur n'est autorisé à accéder qu'aux ressources pour lesquelles on lui accorde explicitement le bénéfice de l'accès),**
- **moindre privilège (chaque utilisateur accède aux ressources avec le minimum de privilèges lui permettant de conduire les actions explicitement autorisées pour lui);**
- **la séparation des pouvoirs,**

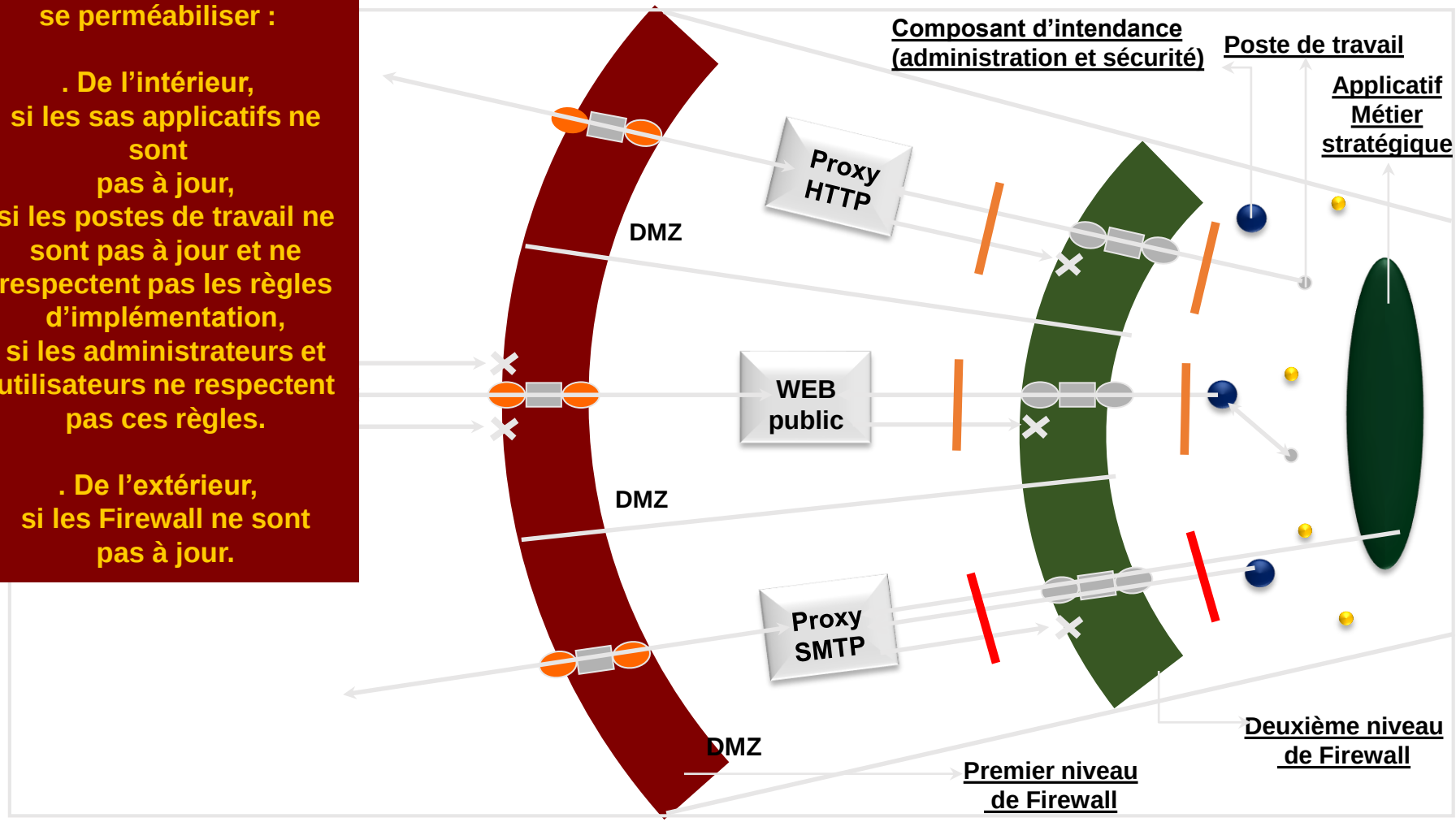


Le Plan d'actions : EIVP /Security by default / la sécurité périphérique

Le risque est de se perméabiliser :

. De l'intérieur, si les sas applicatifs ne sont pas à jour, si les postes de travail ne sont pas à jour et ne respectent pas les règles d'implémentation, si les administrateurs et utilisateurs ne respectent pas ces règles.

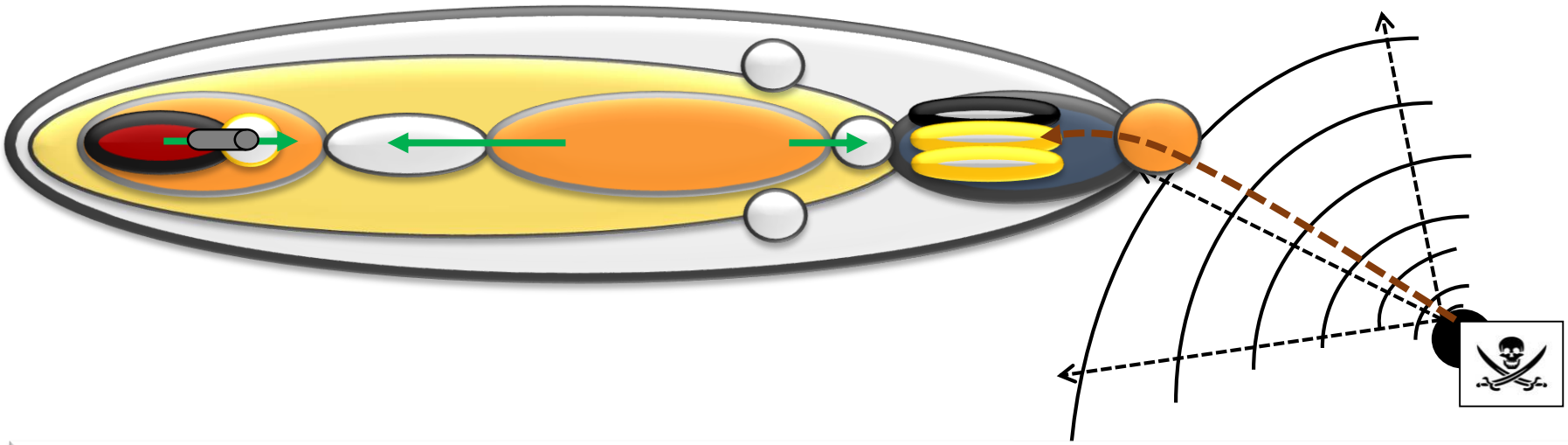
. De l'extérieur, si les Firewall ne sont pas à jour.



Le Plan d'actions : EIVP /Security by design / la sécurité en profondeur

Appliquer les principes de défense en profondeur à l'architecture matérielle et logicielle des centres informatiques.

Le principe de défense en profondeur doit être respecté, en particulier par la mise en œuvre successive de « zones démilitarisées » (DMZ), d'environnements de sécurité en zone d'hébergement, de machines virtuelles ou physiques dédiées, de réseaux locaux virtuels (VLAN) appropriés, d'un filtrage strict des flux applicatifs et d'administration.

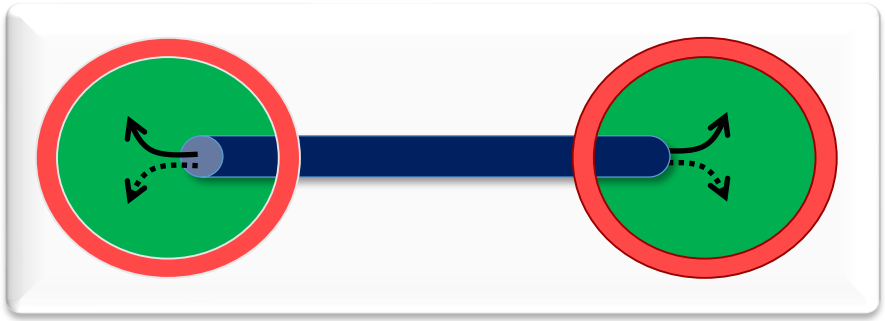


Les premiers niveaux de défense protègent les ressources de niveaux inférieurs contre les attaques à large spectre
Les niveaux inférieurs assurent la protection contre les attaques ciblées sur un objectif précis

La sécurisation d'une architecture doit être assurée mais de façon distribuée, tout au long de la chaîne de liaison, en prenant en compte l'ensemble des composants de l'architecture (réseau, système, applicatif)

Le Plan d'actions : Les mesures organisationnelles et techniques / Security by default / Security by design / Chiffrement

- **La sécurité des échanges : comment garantir l'authentification, la confidentialité, l'intégrité, la non répudiation des échanges :**
  - **Comment échanger des informations avec des niveaux de confidentialité différents, relatifs à la classification ?**



Des algorithmes

- Symétrique
- Asymétrique

Des protocoles combinant les algorithmes

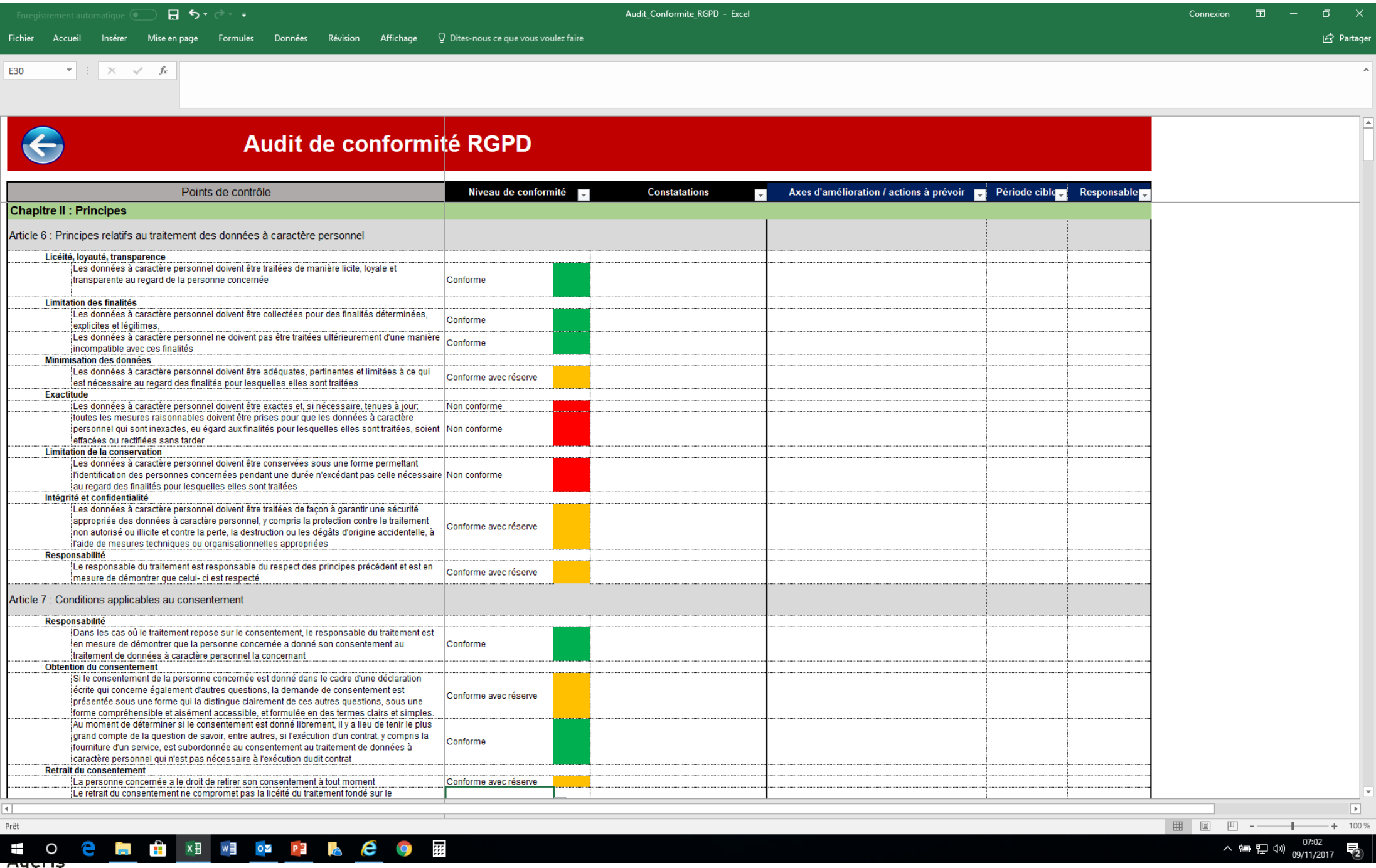
- IPSEC
- SSL
- SMIME / PGP

Des architectures de certificats

- Des choix organisationnels
- Des choix d'outils
- IGCP / PKI

Le Plan d'actions : Les mesures juridiques / Le Contrôle

Contrôle de la Commission	Des Déclarations Du Registre Du Bilan		
CNIL. Contrôle des mesures	**Les actions transverses** • L'organisation de protection de la VP • Le comité de suivi, validation • La politique de protection de la VP • Les contrats avec le ST • La communication de la politique PDCP aux personnes qui doivent l'appliquer. • L'Intégration de la protection de la VP dans les projets • La supervision de la protection de la VP	Sur les éléments	La Minimisation des DCP La Gestion de la durée de conservation des DCP Le respect des droits de la PC Le consentement des PC L'exercice du droit d'opposition L'exercice du droit d'accès direct L'exercice du droit de rectification Le Cloisonnement des DCP Le Chiffrement des DCP Pseudonymisation des DCP
		Sur les sources de risques	L'éloignement des sources de risques Le marquage des documents contenant des DCP La gestion des personnes qui ont un accès légitime Le contrôle de l'accès logique des personnes La gestion des tiers qui ont un accès légitime aux DCP La lutte contre les codes malveillants Le contrôle de l'accès physique des personnes La protection contre les sources de risques non humaines
		Sur les supports	La réduction des vulnérabilités : • des logiciels • des matériels • des canaux informatiques • des personnes • des documents papier
		Sur les impacts	Sauvegarder les DCP Protéger les archives de DCP Contrôler l'intégrité des DCP Tracer l'activité sur le SI Gérer les violations de DCP
Contrôle des PIA		Du contexte du PIA Des mesures du PIA De l'analyse des risques Des décisions	



Enregistrement automatique — Audit_Conformite_RGPD - Excel — Connexion

Fichier Accueil Insérer Mise en page Formules Données Révision Affichage Dites-nous ce que vous voulez faire Partager

E30

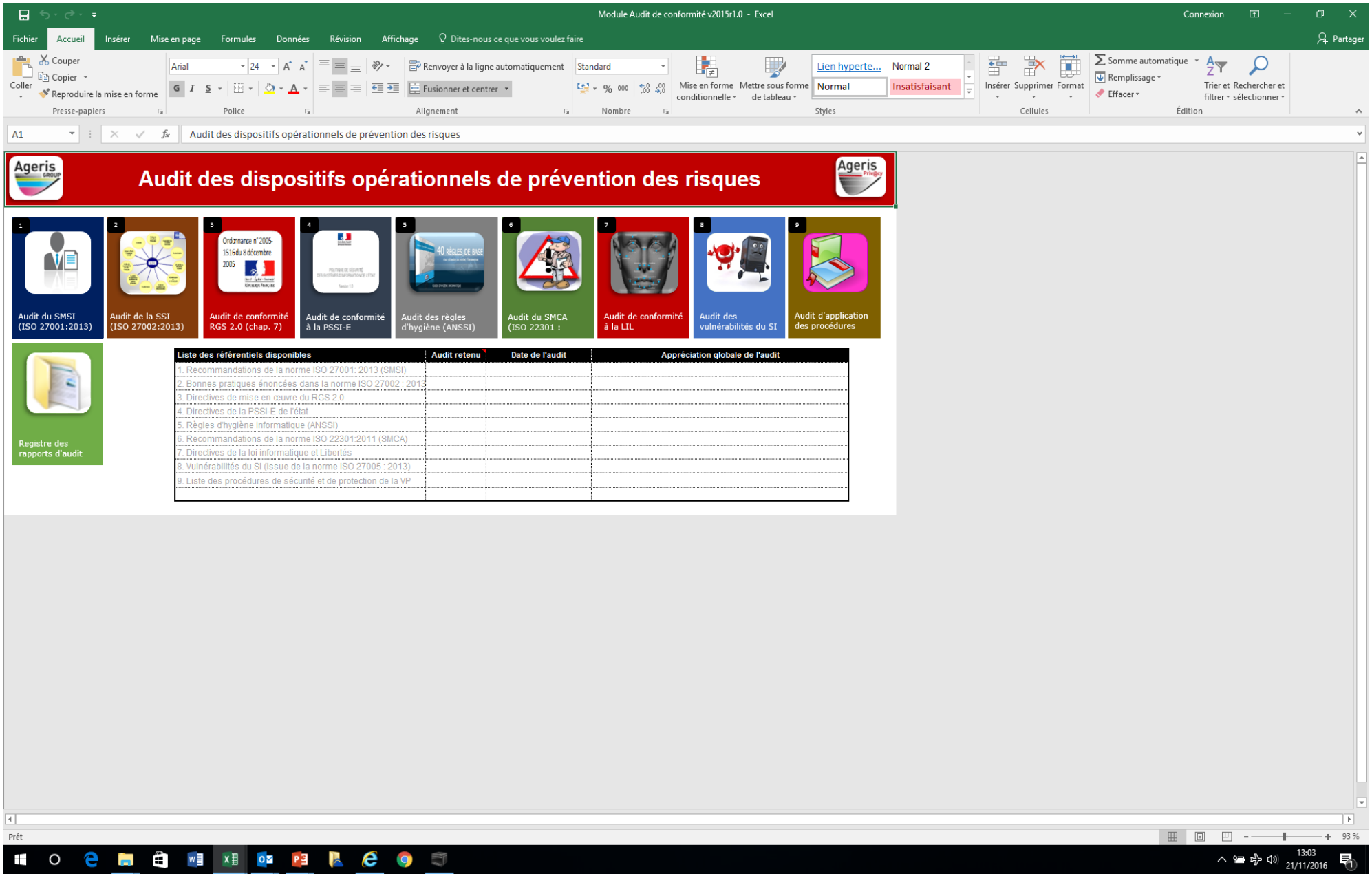
Audit de conformité RGPD

Points de contrôle	Niveau de conformité	Constatations	Axes d'amélioration / actions à prévoir	Période cible	Responsable
Chapitre II : Principes					
Article 6 : Principes relatifs au traitement des données à caractère personnel					
Licéité, loyauté, transparence					
Les données à caractère personnel doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée	Conforme				
Limitation des finalités					
Les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes,	Conforme				
Les données à caractère personnel ne doivent pas être traitées ultérieurement d'une manière incompatible avec ces finalités	Conforme				
Minimisation des données					
Les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées	Conforme avec réserve				
Exactitude					
Les données à caractère personnel doivent être exactes et, si nécessaire, tenues à jour;	Non conforme				
toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder	Non conforme				
Limitation de la conservation					
Les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées	Non conforme				
Intégrité et confidentialité					
Les données à caractère personnel doivent être traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées	Conforme avec réserve				
Responsabilité					
Le responsable du traitement est responsable du respect des principes précédent et est en mesure de démontrer que celui- ci est respecté	Conforme avec réserve				
Article 7 : Conditions applicables au consentement					
Responsabilité					
Dans les cas où le traitement repose sur le consentement, le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant	Conforme				
Obtention du consentement					
Si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples.	Conforme avec réserve				
Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat	Conforme				
Retrait du consentement					
La personne concernée a le droit de retirer son consentement à tout moment	Conforme avec réserve				
Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le					

Prêt 100 %

07:02 09/11/2017

Le Plan d'actions : Les mesures organisationnelles et techniques / Contrôle des mesures



Le Plan d'actions : Les mesures juridiques / Le Code de conduite

La réalisation de Codes de conduite

Les associations (CNIL, AFCDP, ADPL etc.) ou des organismes représentant des RT ou ST peuvent élaborer des Codes de conduite

Objectifs:

L'élaboration d'un Code de conduite a pour objectif d'encourager la bonne application du Règlement européen relatif à la protection des DCP en prenant en compte la spécificité des différents secteurs de T et des besoins spécifiques des micro, petites et moyennes entreprises.

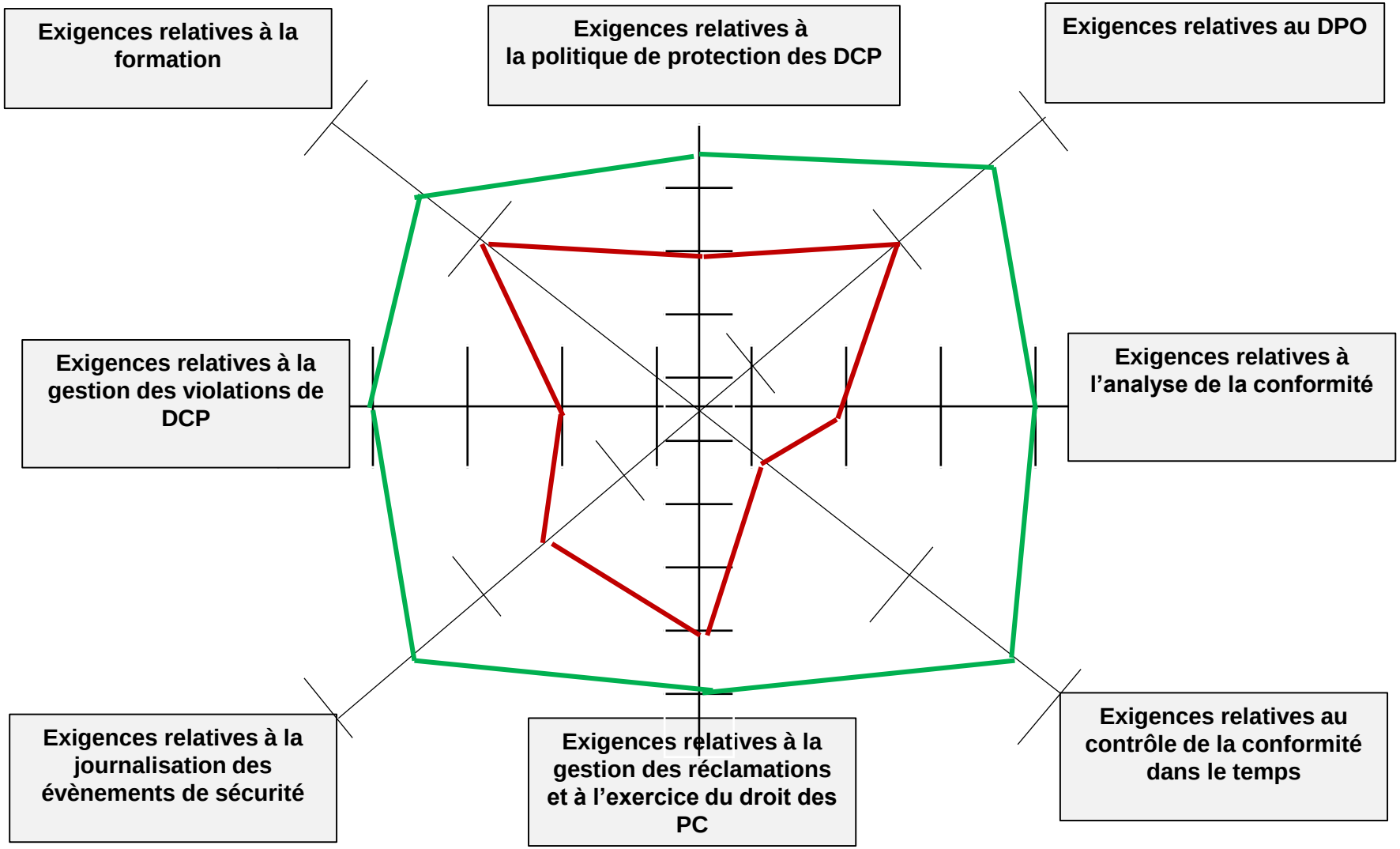
Ce que doit contenir le Code:

le traitement loyal et transparent;

- **les intérêts légitimes poursuivis par les RT dans les contextes spécifiques;**
- **la collecte des DCP; la pseudonymisation des DCP;**
- **les informations communiquées au public et aux personnes concernées;**
- **l'exercice des droits des personnes concernées;**
- **les informations communiquées aux enfants et la protection dont bénéficient les enfants;**
- **les mesures et les procédures concernant la sécurité du traitement;**
- **la notification aux autorités de contrôle des violations de DCP; le transfert de DCP vers des pays tiers;**
- **les procédures extrajudiciaires et autres procédures de règlement des litiges**

Une fois que le Code de conduite est approuvé par l'AC, celle-ci l'enregistre et le publie.

Le Plan d'actions : La Labellisation CNIL pour la Gouvernance



Le Plan d'actions : Les mesures organisationnelles et techniques /Amélioration continue

Pourquoi mettre en œuvre un Système de Management de Sécurité des DCP ?

Pour protéger, dans la durée, les DCP, les T et les systèmes d'information qui les hébergent

Pour renforcer la confiance (vis-à-vis PC /des clients / usagers et des fournisseurs ou en interne).

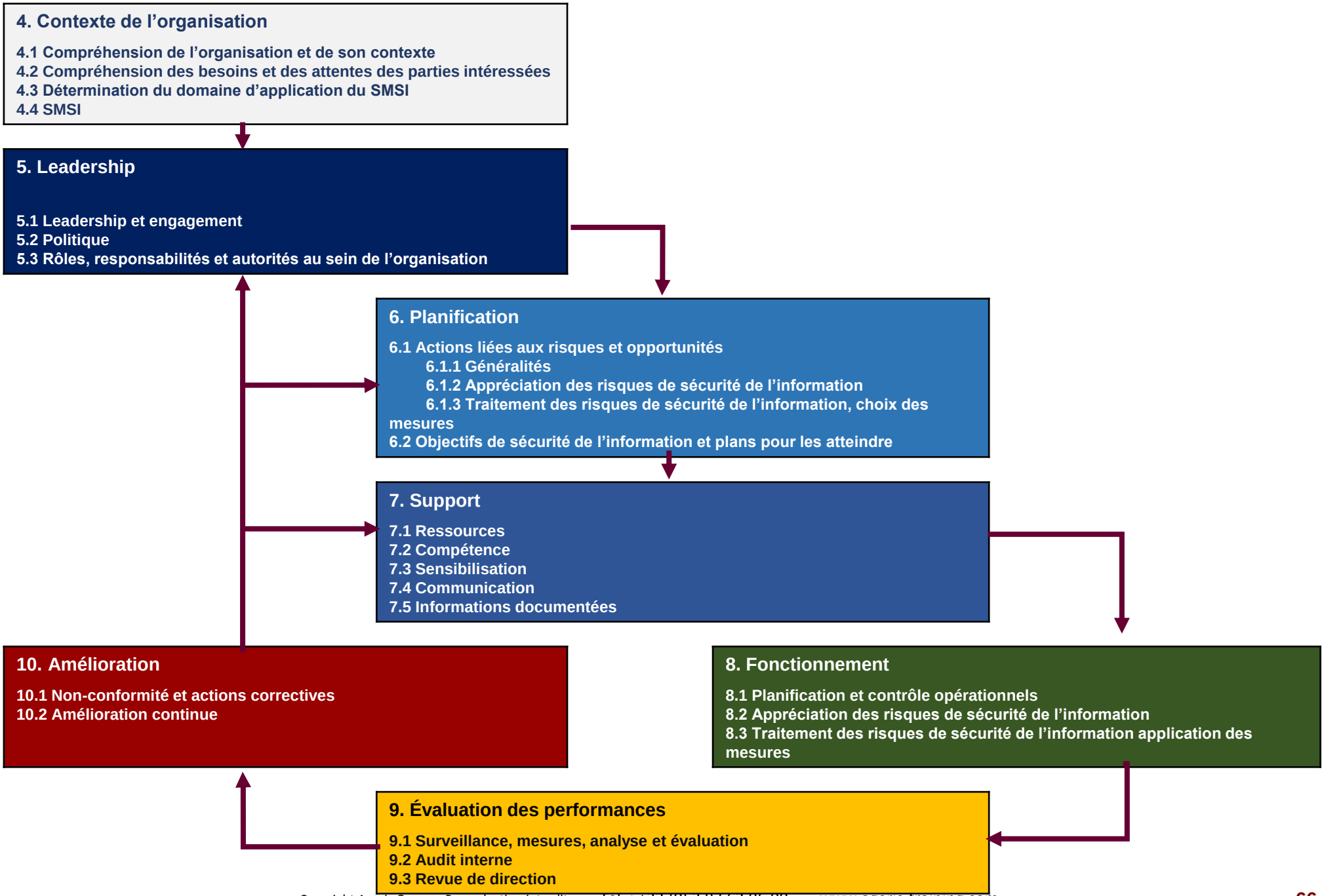
Pour améliorer les processus et l'organisation interne en matière de protection de DCP

Un SMSI – Système de Management de la Sécurité de l'Information est un ensemble d'éléments interactifs permettant à un organisme d'établir une politique et des objectifs en matière de sécurité de l'information, d'appliquer la politique, d'atteindre ces objectifs et de contrôler l'atteinte de ces objectifs.

Le SMSI est établi, documenté, mis en œuvre et entretenu. Son efficacité est mesurée par rapport aux objectifs de l'entité, et cette mesure permet d'améliorer en permanence le SMSI.

L'existence d'un SMSI dans l'organisme permet de renforcer la confiance dans le mode de gestion de la sécurité de l'information »

Le Plan d'actions : Les mesures organisationnelles et techniques /Amélioration continue



Synthèse : Les actions de mise en conformité

Désigner un chef de projet de mise en conformité
Désigner un Délégué à la Protection des Données (DPO) pour le contrôle de conformité au règlement
Poursuivre les actions de sensibilisation des collaborateurs au regard des nouvelles exigences imposées par le règlement (transparence, informations préalables, …)
Déclarer tous les traitements auprès du DPO afin qu'il puisse finaliser la mise à jour du registre des traitements (note interne à destination des services).
Engager une démarche relative à la gouvernance (MOA, MOE, RSSI, DPO, …)
Renforcer les procédures d'alertes internes et la notification des violations au DPO
Formaliser une charte/code éthique « vie privée » pour renforcer la transparence dans l'usage des données pour l'interne et pour l'externe
Définir et formaliser des politiques de protection des données Ex. : Politique de protection de la vie privée et des DCP , Politique de Protection des SI (PSSI)
Prévoir des procédures d'informations des usagers / AC en cas de violation de leur données.
Adapter les procédures de traitements des demandes pour respecter le délai de 1 mois.
Revoir les formulaires pour faire apparaitre clairement la partie / mention relative au consentement.
Réviser les clauses dans les marchés et les conventions.
Inclure la sécurité des données dans tous les nouveaux projets (la démarche projet doit inclure ces aspects dans les phases amonts d'expression des besoins)
Mettre en œuvre une démarche d'évaluation d'impact sur la vie privée (EIVP) pour tous les traitements de données (soumis à autorisation de l'AC)
Prévoir des audits de sécurité des données et appliquer les plans d'actions correctifs proposés.
Appliquer les codes de conduites (et du futur comité européen à la protection des données) (veille régulière à réaliser)
Conserver tous les justificatifs prouvant l'application du règlement (traçabilité des actions engagées et des décisions)

Organisation

- Règlement
- Formations
- Méthodes
- Directives et Procédures
- Contrôles et Preuves
- Sanctions
- Technologies

Relativité Sensibilité des DCP et T et Enjeux organismes

- Potentialités
- Impacts Vie Privée / Organisme
- Relativité des règles corrélées aux besoins et aux risques métiers

Engagement de responsabilité :

- Personne morale
- Délégataire
- Directions
- Chefs de services
- Administrateurs
- Personnels
- Partenaires
- Sous-traitants