ADSTO
Avocats à la Cour

Le RGPD : les apports d'un régime de compliance : quelles opportunités ? quelles aides à la gestion de crise ?

CNEJITA

Mardi 19 juin 2018

ADSTO
Avocats à la Cour

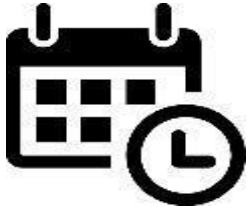
POURQUOI UN PROGRAMME DE COMPLIANCE ?

ADSTO
Avocats à la Cour

QU'EST-CE QUE LE RGPD ET POURQUOI ?

Responsabilisation et meilleure protection des données

Portée
L'ensemble des entreprises dans le monde traitant les données personnelles des citoyens européens



Echéance
Mise en œuvre
depuis le 25 Mai 2018

Charge de la preuve
L'entreprise doit prouver sa **conformité**

Désignation d'un délégué à la protection de données

Temps imparti
Une violation de données doit être signalée dans les 72h, si possible

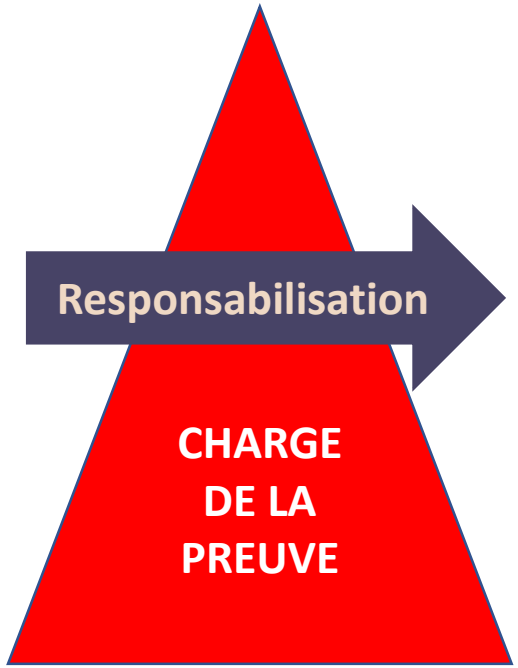
Amendes
S'élèvent à 4% du revenu global des entreprises dans le monde

ADSTO
Avocats à la Cour

DES FORMALITÉS PRÉALABLES À LA LOGIQUE DE RESPONSABILISATION

Loi de 1978

- Déclaration préalable de traitement auprès de la CNIL
- Autorisation de traitement de la CNIL



RGPD

- Registre de traitement
- Autorisation ?

ADSTO
Avocats à la Cour

COMMENT SE TRADUIT LE RGPD ?

> Des consommateurs soucieux de leurs données et des usages qui explosent

- ***78% dérangés par le fait que des informations les concernant soient dans des bases de données***

> Un cadre législatif qui se renforce

- ***Le consommateur en maîtrise de ses données***

> Une position de Marque à protéger

- ***« La confiance se gagne en goutte et se perd en litres » Jean-Paul SARTRE***

Un programme de Data Compliance

Limiter les risques d'atteinte à la réputation.

Accroître la confiance du consommateur.

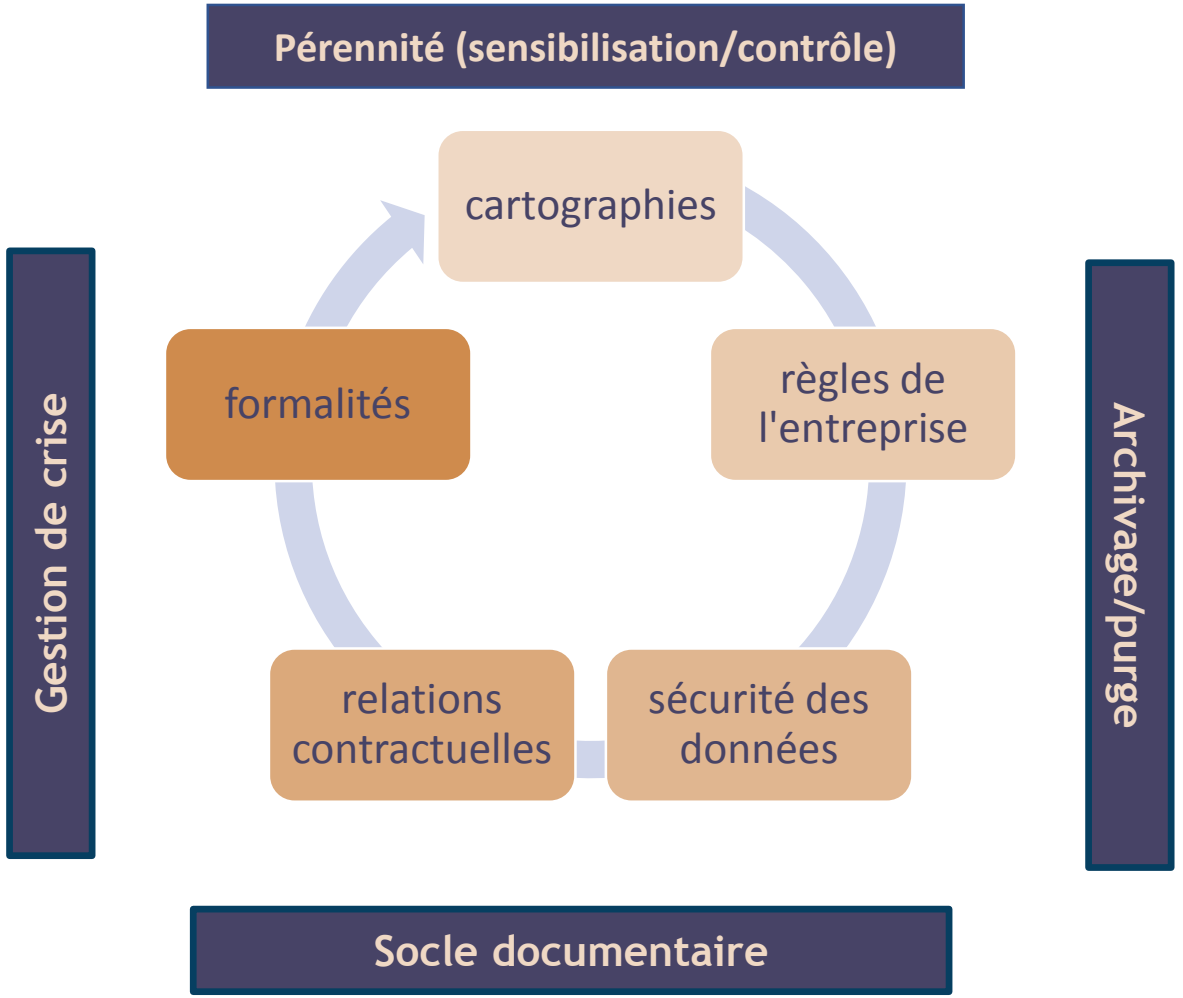
Prouver la conformité dans en cas de contrôle de la CNIL.

Eviter les sanctions financières.

Limiter les risques d'engagement de la responsabilité civile et pénale.

ADSTO
Avocats à la Cour

COMMENT PROCÉDER POUR ÊTRE EN CONFORMITÉ ?



ADSTO
Avocats à la Cour

PILOTAGE DU PROGRAMME DE COMPLIANCE : LE COMITÉ DATA

- **Mettre en oeuvre le programme de compliance**
- **Garantir l'application des Règles Data et leurs évolutions**

Membres du comité	DSI / RSSI	Référent Data Marketing et Communication	Référent Data RH	Référent Data Juridique	Référent Compliance / Éthique	DPO
Rôle	Responsable sécurité informatique	Responsable de l'application des bonnes pratiques de collecte & usage et de la communication interne/externe	Responsable de l'application des bonnes pratiques de collecte & usage	Responsable de la sécurité juridique	Responsable de la vérification du projet compliance et des pratiques éthiques	Responsable des procédures & contrôles Contact de la CNIL et des personnes concernées

ADSTO
Avocats à la Cour

FOCUS : QU'EST-CE QUE LE DPO ?

DPO

QUALITÉS/COMPÉTENCES :

- Indépendance
- Qualification
- Communication
- Proactivité

POINT DE CONTACT :

- Interlocuteur entre l'établissement et l'autorité de contrôle

FONCTION

CONTRÔLE CONFORMITÉ :

- Respect de la règlementation

INFORMATION CONSEIL:

- Faire le lien entre tous les niveaux au sein de l'établissement

ŒUVRER :

- Mise en place des PIA
- Inventaires des données

SUIVI DU TRAITEMENT :

- Tenue du registre

VEILLE D'ACTUALITÉ :

- Circulation de l'information en interne

ADSTO
Avocats à la Cour

QU’EST-CE QU’UNE CRISE ?

ADSTO
Avocats à la Cour

QUELS TYPES DE CRISE ?

FAIT GÉNÉRATEUR NUMÉRIQUE

MALVEILLANCE

Infection du Terminal

Prise de Contrôle à Distance

Exfiltration de Données

ACCIDENT

Erreur humaine

CONTRÔLE

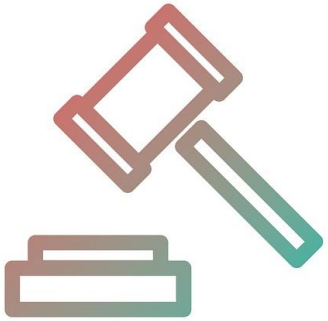
- ❖ Contrôle
- ❖ Enquête
- ❖ Perquisition

Par :

- CNIL
- AMF
- Police
- DGCCRF

ADSTO
Avocats à la Cour

LE RISQUE DE CONTENTIEUX



Action de groupe
(Article 80 du RGPD)

Responsabilité civile
(Article 82 du RGPD)

Responsabilité administrative
(Article 83 du RGPD)

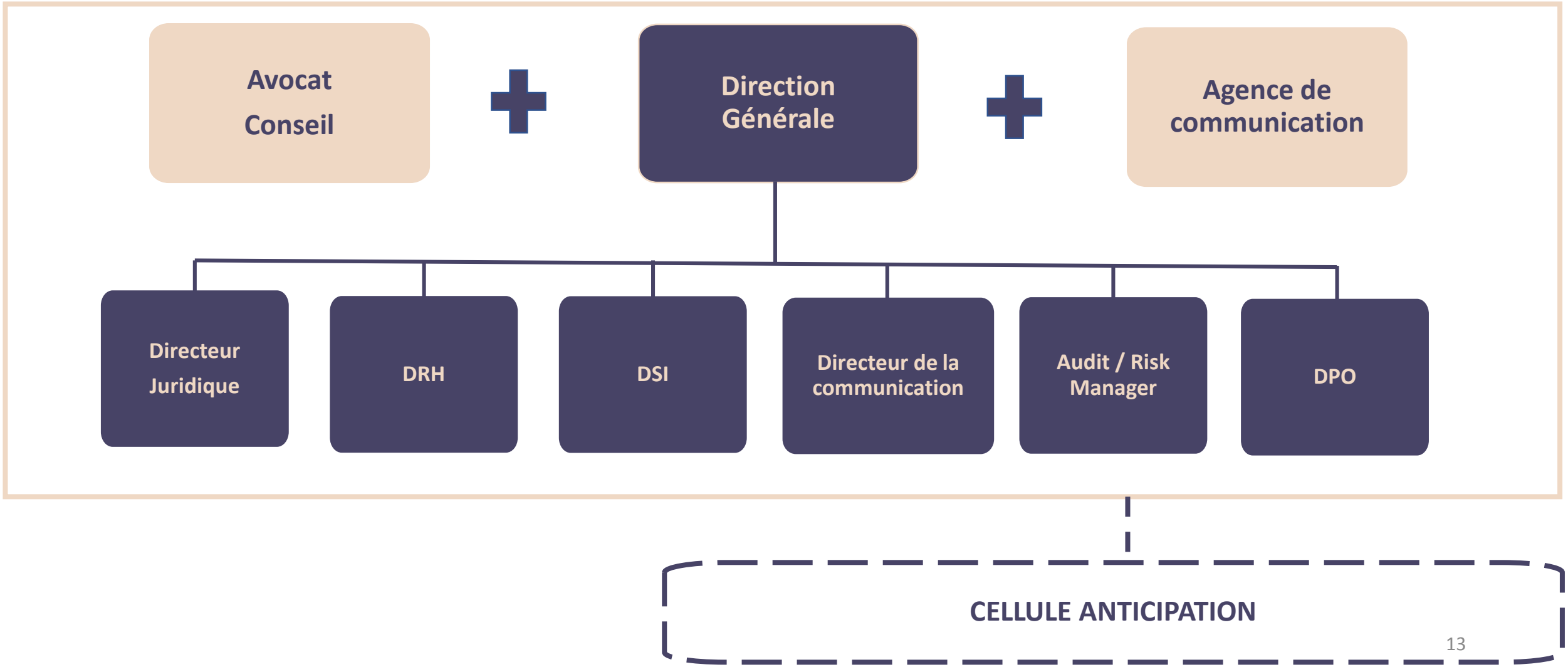
Responsabilité pénale
(Article 84 du RGPD)

ADSTO
Avocats à la Cour

AVANT LA CRISE

ADSTO
Avocats à la Cour

LA MISE EN PLACE DE LA CELLULE DE CRISE



ADSTO
Avocats à la Cour

PENDANT LA CRISE

ADSTO
Avocats à la Cour

LE DÉCLENCHEMENT DE LA CELLULE DE CRISE

FAIT GÉNÉRATEUR NUMÉRIQUE – CONTRÔLE

1. Veiller à ce que l'équipe IT sache qui appeler en 1er
2. Obtenir confirmation de ce qui s'est passé auprès de l'équipe IT
3. Informer les membres de la Cellule de crise
4. Veiller à avoir une liste à jour de téléphones privés des membres de la Cellule de crise à utiliser dans ce cas d'urgence
5. Organisation d'une réunion initiale afin d'accélérer la recherche et la cristallisation des faits
6. Décider s'il faut contacter les autorités judiciaires (police, investigations spéciales, procureur…)
7. Décider s'il faut notifier la violation à la CNIL et s'il faut communiquer au public, aux personnes concernées (et/ou en interne)
8. Organiser des rapports d'évolution de la situation/points d'étape régulièrement (chaque heure / demi journée)
9. Décider s'il faut informer / solliciter les compagnies d'assurance

ADSTO
Avocats à la Cour

MINIMISER LES CONSÉQUENCES D'UNE CRISE

ADSTO
Avocats à la Cour

LE TRANSFERT DU RISQUE VERS L'ASSURANCE

Souscription du contrat

1. **Programme de conformité** *(cartographie des risques notamment sur les données et les SI)*

2. **Sensibilisation à la vulnérabilité** de l'entreprise face aux cyber risques

3. **Analyse des contrats déjà souscrits** *(garanties et clauses d'exclusion)*

4. **Négociation du contrat de cyber assurance** *(garanties, clauses d'exclusion et primes)*

Contrôle / Enquête de la CNIL
Cyber attaque / Erreur humaine
Non respect de la réglementation

1. **Pérennisation de la conformité de l'Entreprise** aux exigences de la réglementation – (*registres de traitements, mesures de sécurité,..)*

2. **Renégociation ponctuelle des contrats d'assurance**, en déclarant les évolutions favorables à la diminution de l'exposition au cyber risque

1. **Gestion immédiate de la crise** (*cristallisation des éléments de preuves en cas d'attaque…)*

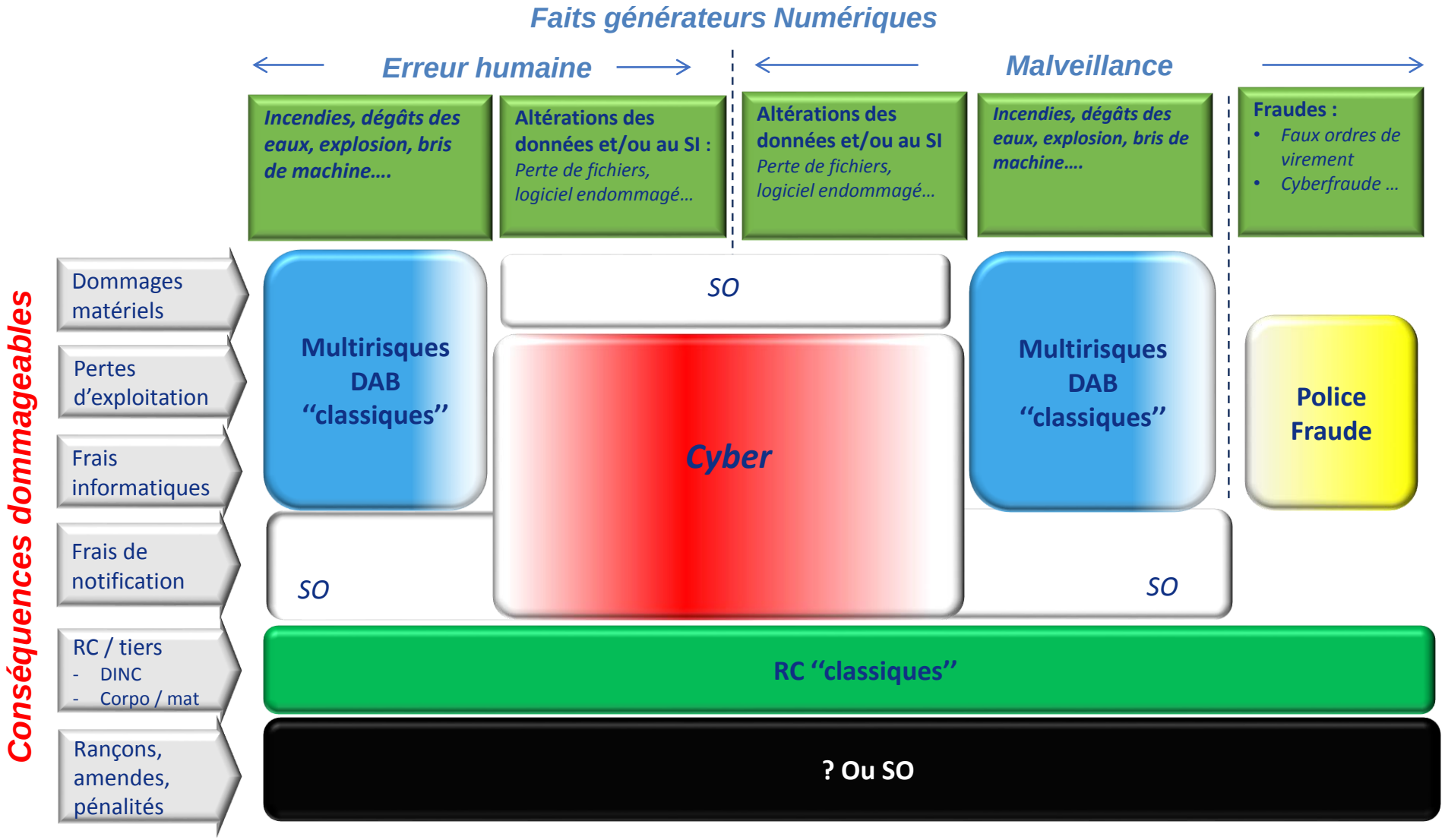
2. **Participation aux actions de la cellule de crise** *(contact avec les assurances, notification à la CNIL, conseils en matière de communication…)*

3. **Gestion juridique de la crise** *(protection des intérêts de l'entreprise vis-à-vis des tiers –CNIL, assureurs, particuliers)*

Les acteurs concernés :
- Organes dirigeants de l'Entreprise
- Risk manager / Compliance Officer
- Courtier
- Assureur

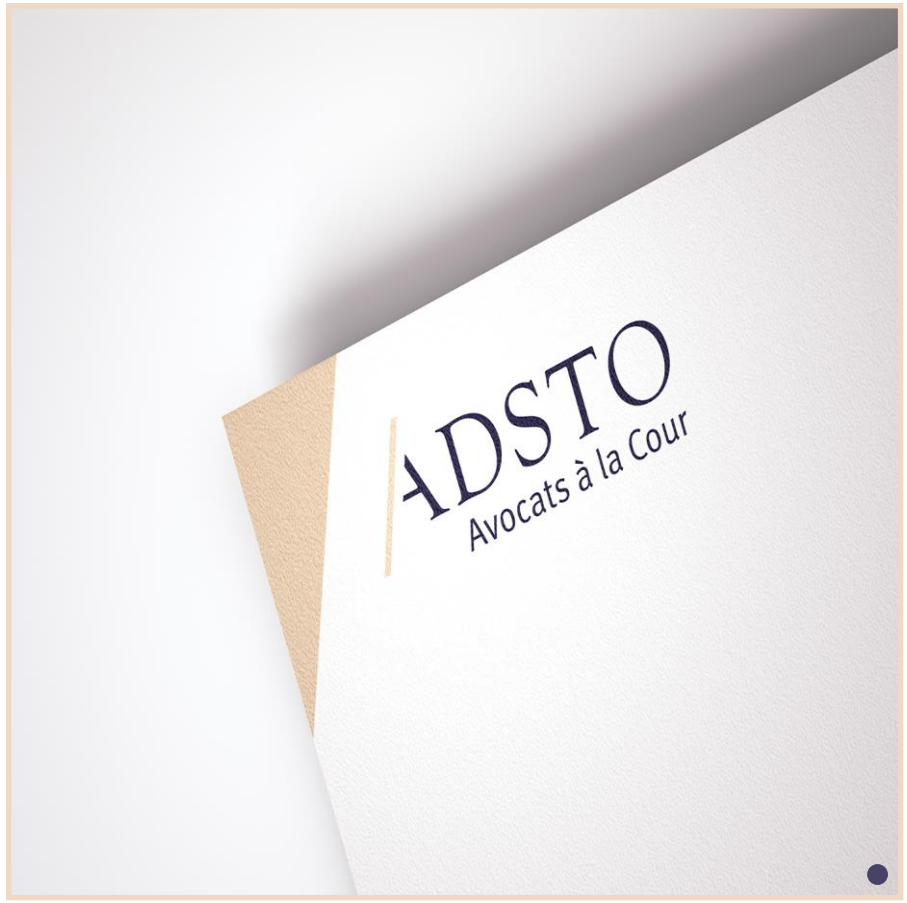
ADSTO
Avocats à la Cour

DÉCLENCHER LA GARANTIE ADAPTÉE



Source : Présentation de la Fédération Française de l'Assurance du 4 avril 2018 au CDSE

ADSTO
Avocats à la Cour



Claire BERNIER ADSTO +33(0)6 73 80 26 37 24 boulevard de Douaumont 75017 clairebernier@adsto.legal