Formation CNEJITA, 20 juin 2017

Le règlement général pour la protection des données – risques et opportunités

Table ronde sur un cas pratique pour une startup

ADSTO Avocats à la Cour

AFDIT

ATM AVOCATS

Expensya

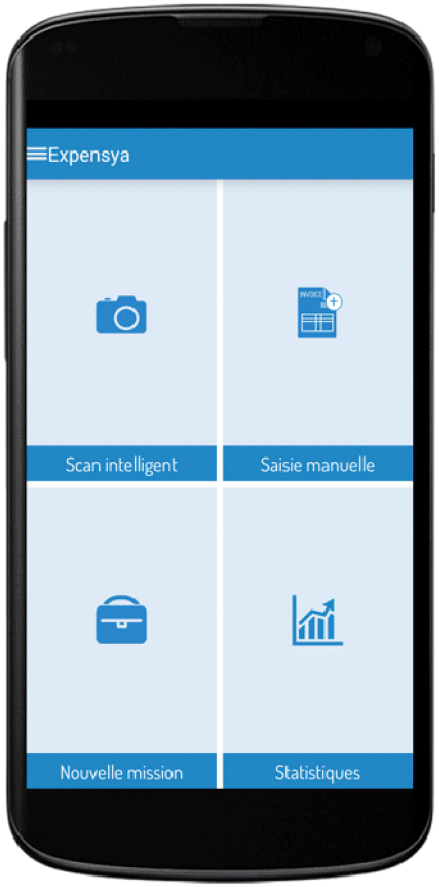
Présentation des intervenants

- **Monsieur Yves Léon**, *expert de justice, Président de la Commission Déontologie de la Cnejita, Président du Hub Digital, HEC Alumni Association*
- **Maître André Meillassoux**, animateur de la table ronde, *Président AFDIT, Avocat spécialisé dans les technologies de l'information, la propriété intellectuelle (IT/IP) et les contrats*
- **Maître Claire Bernier**, *Avocat en droit pénal des affaires et Référent Pénal du Barreau de Paris, Secrétaire général de l'AFDIT*
- **Monsieur Karim Jouini**, *Président de la société Expensya (www.expensya.com)*

Présentation de l'offre

Expensya

- Gestion des notes de frais
- Export de données simplifié
- Intégration du comptable
- Reconnaissance intelligente
- Application Web
- Statistiques intelligentes



Et si on vous facilitait la vie ?

Vous détestez les notes de frais, les frais kilométriques, les procédures de remboursement des frais professionnels ? Expensya a été pensé et conçu pour vous !

Pourquoi Expensya illustre parfaitement la diversité des enjeux du RGPD :

- Une start-up dont la solution numérique voit les **données personnelles au cœur de sa solution.**

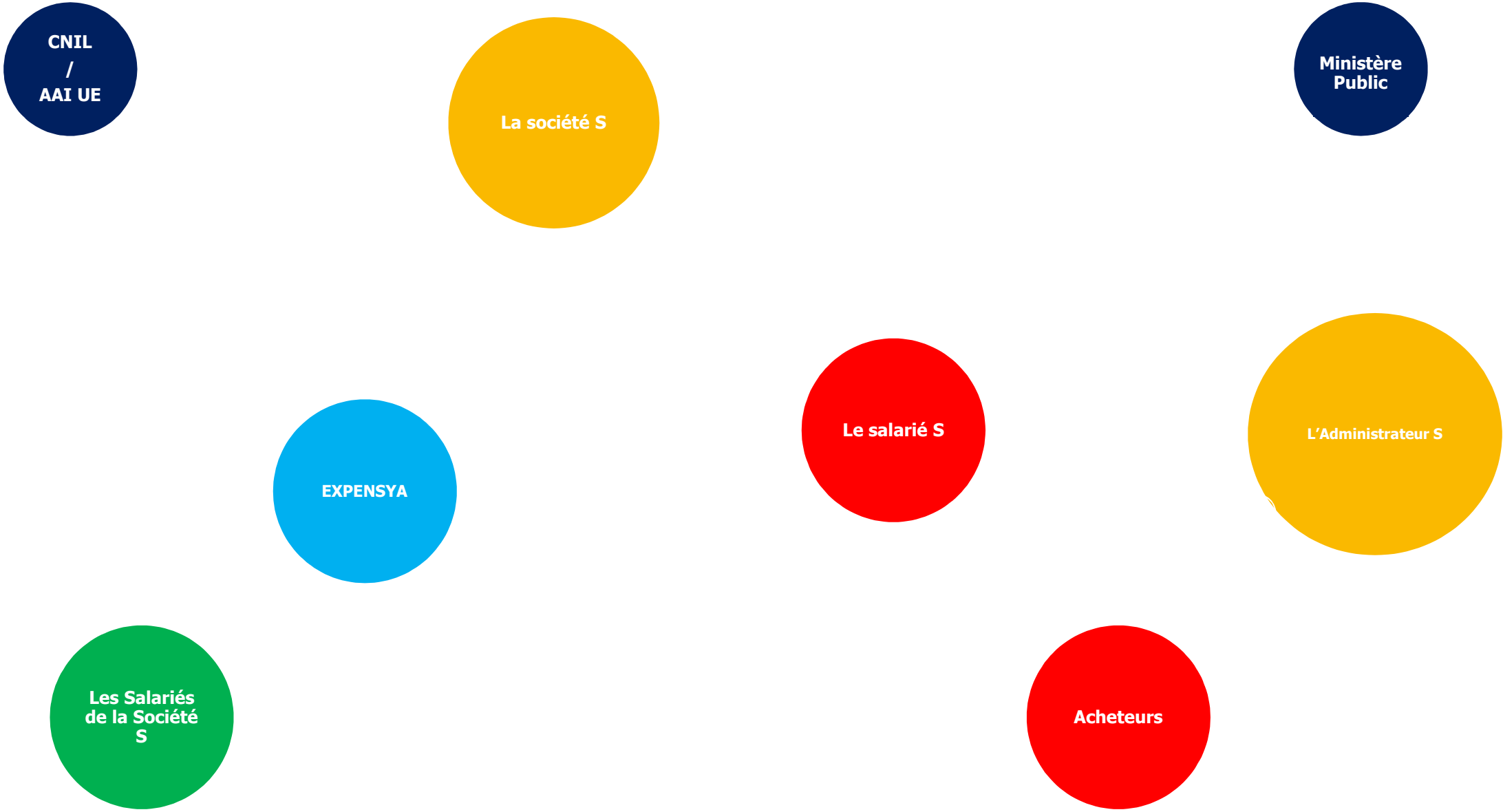
- Des **données hétérogènes** reflétant potentiellement les différentes catégories de données et la diversité des régimes de protection.
- La solution et le business model reposent sur la **qualité de responsable de traitement** d'Expensya, laquelle est en première ligne des nouvelles sanctions.
- Plusieurs **partenariats** qui soulèvent la question de la nouvelle **co-responsabilité entre le responsable de traitements et les divers « sous-traitants » (en réalité, mieux nommés « prestataires »),**
- Nécessité d'une « conformité » selon le récent principe d'**accountability**, à tous égards, y compris crédibilité extérieure, notamment pour des levées de fonds.

Exposé du cas pratique et des différents acteurs

LE CAS PRATIQUE

« La société S, 20 000 salariés, utilise l'outil de gestion de frais de déplacement fourni et géré par la société Expensya.

- *Un **salarié de S a réussi à usurper l'identité de l'administrateur de S du système** Expensya. Il a pénétré le système et a divulgué des informations sur différents clients, notamment des éléments statistiques stockés par le système Expensya. Pourquoi pas le nombre de commandes de Coca-Cola, le CA correspondant, la liste nominative des personnes correspondantes ainsi que le lieu où ont eu lieu ces commandes. »*
- *En réalité, la fraude a un impact qui va bien au-delà des plaignants. Elle impacte directement et interpelle presque tous les acteurs de la chaîne qui ont tous des droits, des obligations et potentiellement un préjudice.*
- *Ce sont :*
- *. les salariés du client S, mais aussi*
- *. EXPENSYA qui est responsable des traitements de son application,*
- *. ses « partenaires » qui sont interfacés sur son système (et son API…par ex)et qui ont accès aussi à ces données personnelles*
- *. ses clients qui, au même titre que les salariés de S, sont potentiellement des victimes.*


CNIL
/
AAI UE
La société S
Ministère
Public
EXPENSYA
Le salarié S
L'Administrateur S
Les Salariés
de la Société
S
Acheteurs

Présentation du cadre juridique général

Les statuts, droits et obligations des différents acteurs

Maître Claire Bernier

ADSTO
Avocats à la Cour

cadre juridique

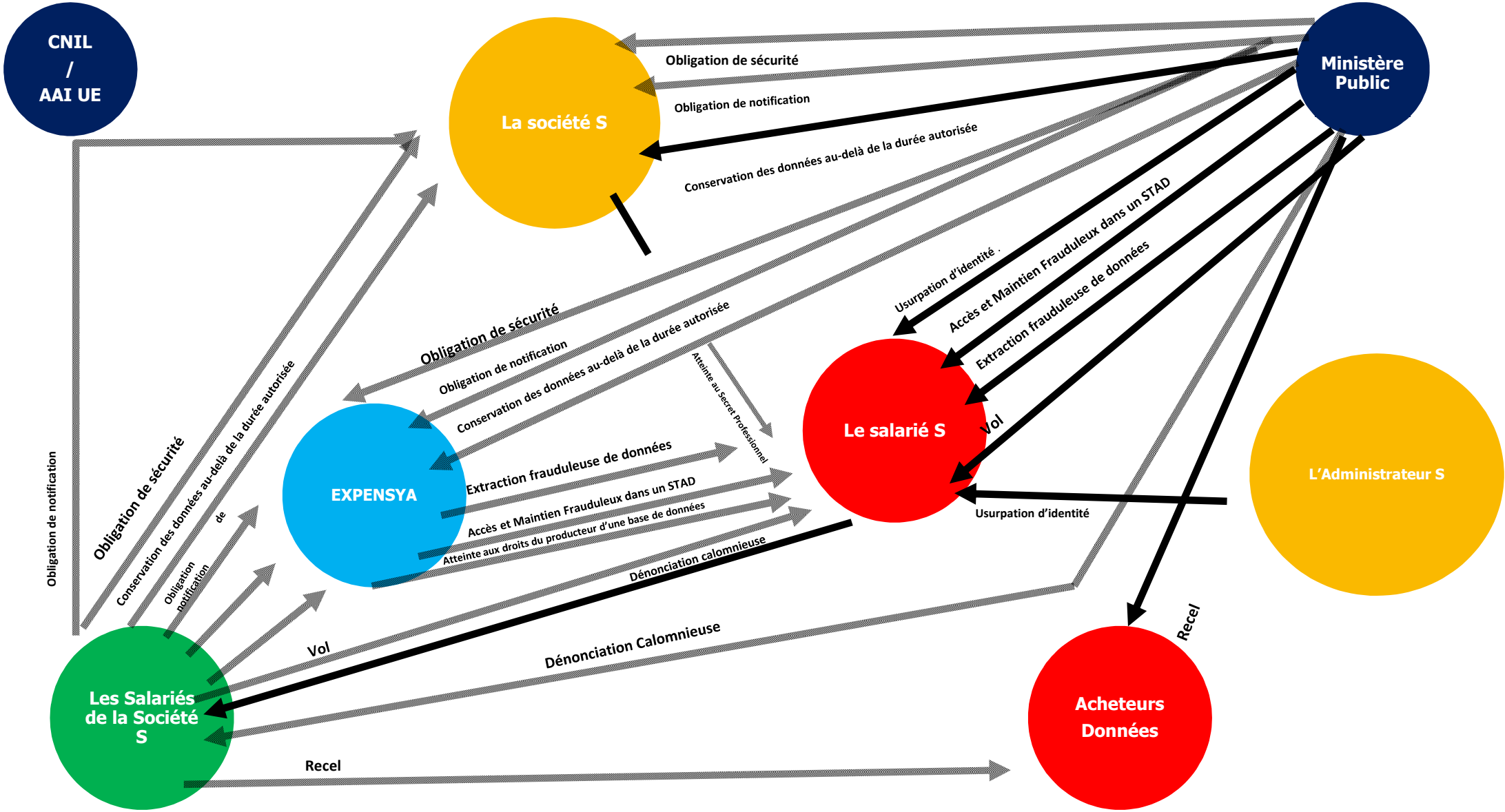
Pourriez-vous sommairement rappeler les différents régimes et réglementations qui gouvernent un tel cas ?

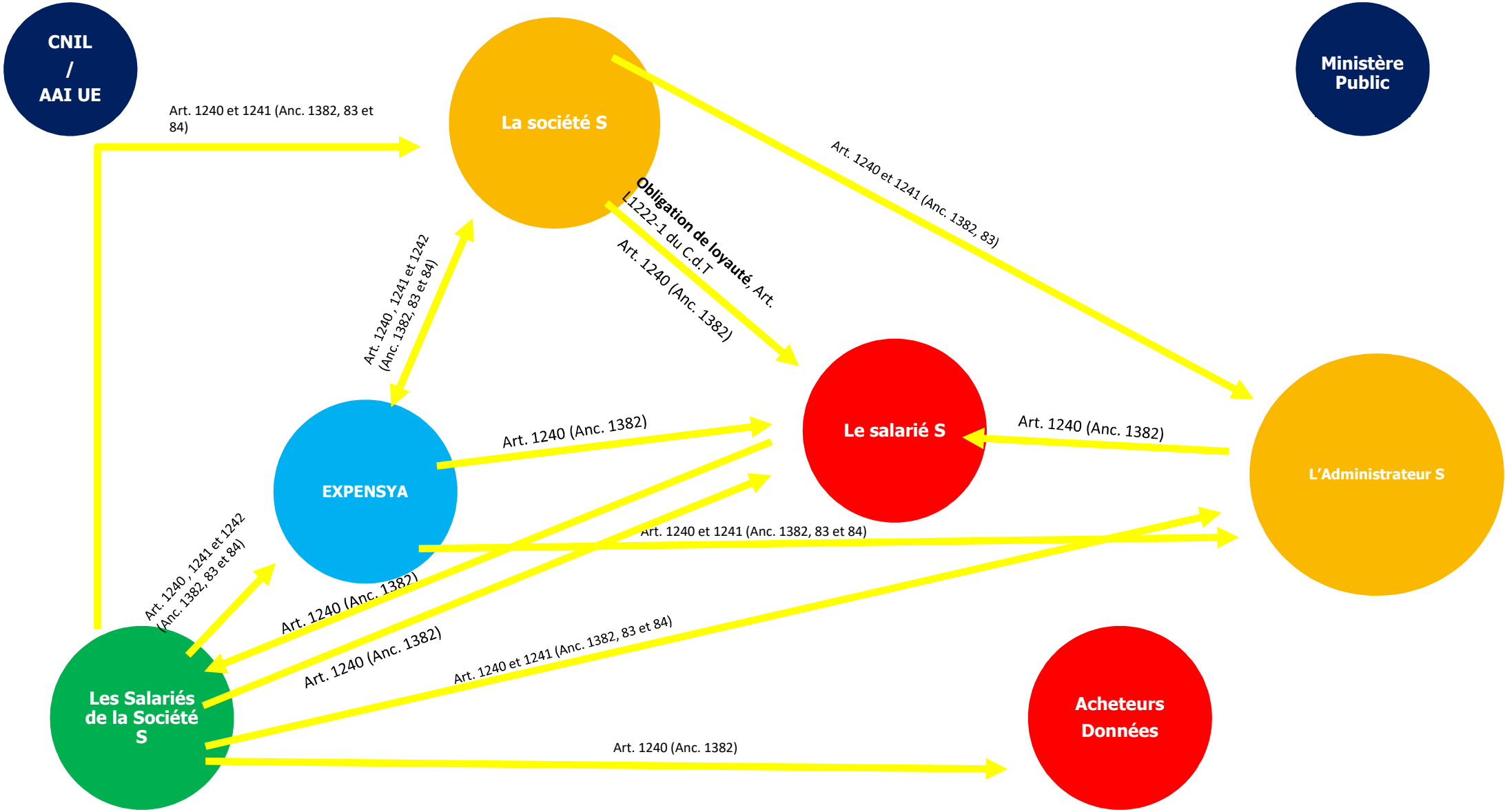
Droit commun, pénal, données personnelles : poser le cadre juridique de la situation, rappeler sommairement voire en faisant un focus, car c'est un peu long, les statuts, les droits et obligations de chacun.

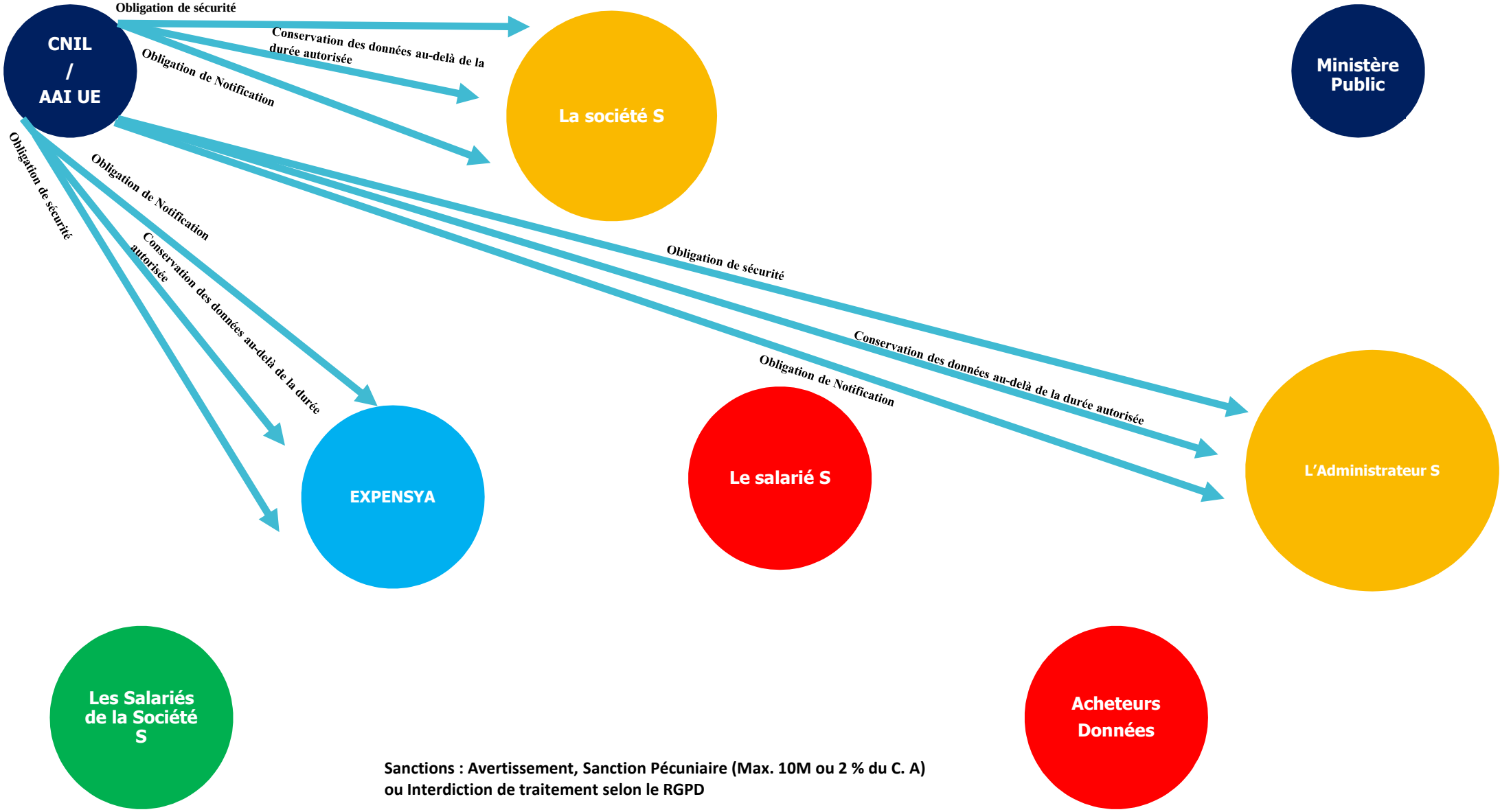
Pourriez vous détailler la situation de chaque acteur, ce qui devrait se faire en 6 blocs pour envisager ces cadres et les actions envisageables

- **Maître Claire Bernier**

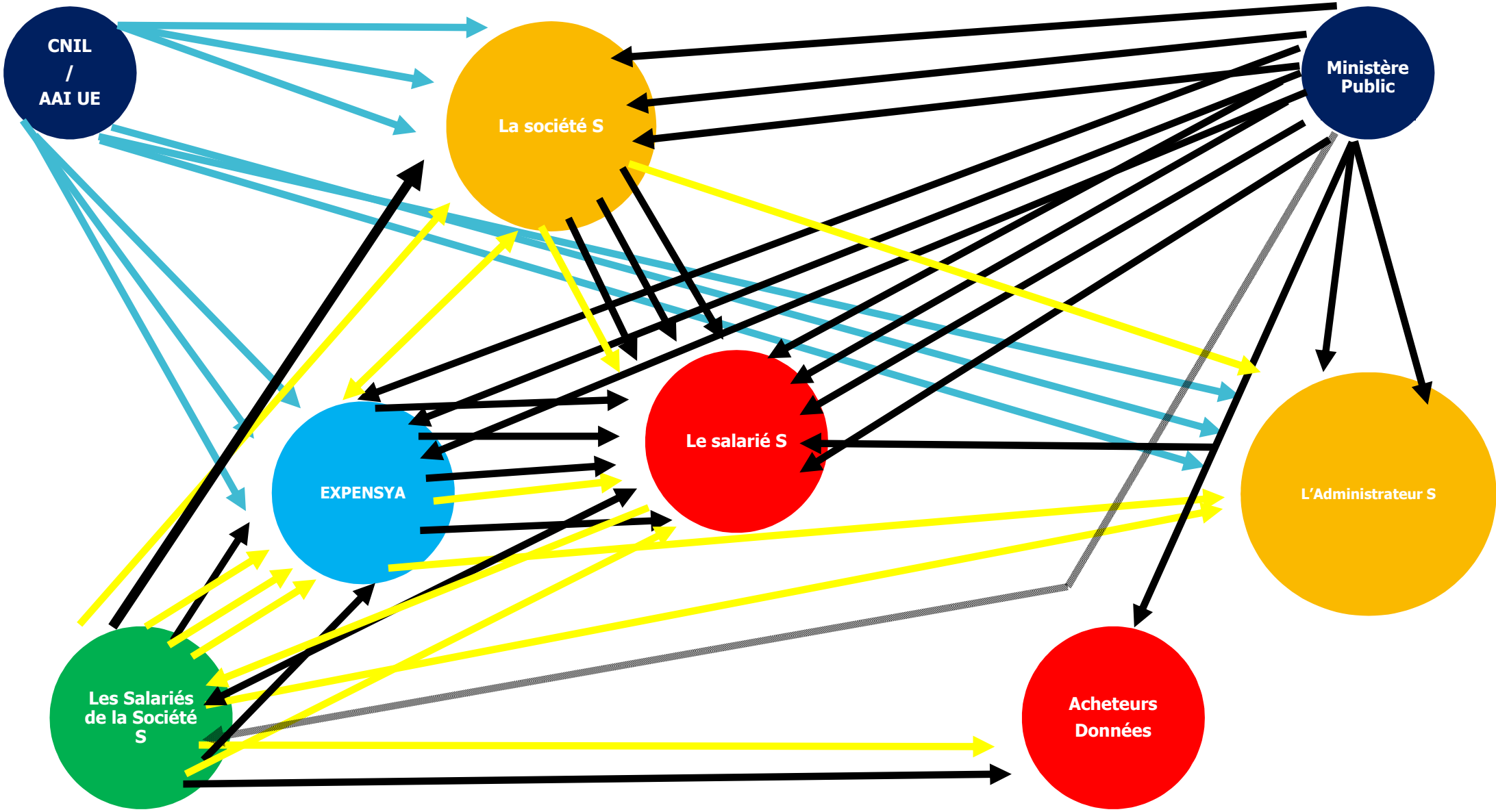
ADSTO
Avocats à la Cour


CNIL / AAI UE
La société S
Ministère Public
Obligation de sécurité
Obligation de notification
Conservation des données au-delà de la durée autorisée
Usurpation d'identité
Accès et Maintien Frauduleux dans un STAD
Extraction frauduleuse de données
Obligation de notification
Obligation de sécurité
Conservation des données au-delà de la durée autorisée
Atteinte au Secret Professionnel
EXPENSYA
Le salarié S
L'Administrateur S
Extraction frauduleuse de données
Accès et Maintien Frauduleux dans un STAD
Atteinte aux droits du producteur d'une base de données
Dénonciation calomnieuse
Vol
Usurpation d'identité
Obligation de notification
Obligation de sécurité
Conservation des données au-delà de la durée autorisée
Obligation de notification
Vol
Dénonciation Calomnieuse
Recel
Les Salariés de la Société S
Acheteurs Données
Recel


CNIL / AAI UE
Art. 1240 et 1241 (Anc. 1382, 83 et 84)
La société S
Ministère Public
Art. 1240 et 1241 (Anc. 1382, 83)
Obligation de loyauté, Art. L1222-1 du C.d.T
Art. 1240 (Anc. 1382)
Art. 1240 , 1241 et 1242 (Anc. 1382, 83 et 84)
EXPENSYA
Art. 1240 (Anc. 1382)
Le salarié S
Art. 1240 (Anc. 1382)
L'Administrateur S
Art. 1240 et 1241 (Anc. 1382, 83 et 84)
Art. 1240 , 1241 et 1242 (Anc. 1382, 83 et 84)
Art. 1240 (Anc. 1382)
Art. 1240 (Anc. 1382)
Art. 1240 et 1241 (Anc. 1382, 83 et 84)
Les Salariés de la Société S
Acheteurs Données
Art. 1240 (Anc. 1382)



Sanctions : Avertissement, Sanction Pécuniaire (Max. 10M ou 2 % du C. A) ou Interdiction de traitement selon le RGPD


CNIL
/
AAI UE
La société S
Ministère Public
EXPENSYA
Le salarié S
L'Administrateur S
Les Salariés de la Société S
Acheteurs Données

Présentation de la vision d'Expensya

Sur la réglementation des données personnelles et les risques encourus

- **M. Karim Jouini**

Expensya

Au regard de ces différentes réglementations, notamment celle ayant trait aux données personnelles, que pensez vous de l'impact qu'elle a sur votre solution?

→ Quels traitements ? Quelles données de l'application.

Quels partenariats vous semblent concernés par ces différentes réglementations ?

→ Avez-vous une politique de partenariat ? Quid des transferts de données mais aussi de la coresponsabilité avec d'autres prestataires.

Quelle serait votre réaction face à ce cas d'école ?

Quelles dispositifs techniques (conformément au GDPR) : notamment confidentialité, *security/privacy by design*…)

- **M. Karim Jouini**

Expensya

Présentation de la vision d'Expert

Sur la place de l'expertise dans la mise en conformité dans le cadre d'un audit ou d'expert de partie

- **M. Yves Léon,**
- Expert près la Cour d'Appel d'Aix-en-Provence
- Président de la Commission Déontologie de la Cnejita
- Membre du Conseil d'Administration de l'Afdit
- Président du Hub Digital, Hec Alumni Association

33 (0) 6 03 81 81 81
yves.leon@expert-de-justice.org

CNEJITA EXPERTS

La vision de l'Expert

Quel apport d'un expert technique spécialisé

Quelles actions recommander, en amont ,dans le cadre d'un audit ou d'une étude d'impact (mapping des gisements de données, évaluation des risques, checks de sécurité, points de faiblesse éventuels ?)

Quels types de mission pourraient être ordonnées dans une situation contentieuse (contrôle CNIL, procédure judiciaires, pénales et/civiles).

- **M. Yves Léon,**
- Expert près la Cour d'Appel d'Aix-en-Provence
- Président de la Commission Déontologie de la Cnejita
- Membre du Conseil d'Administration de l'Afdit
- Président du Hub Digital, Hec Alumni Association

33 (0) 6 03 81 81 81
yves.leon@expert-de-justice.org

CNEJITA EXPERTS

1 – L'expert de justice devra travailler les flux de données

- Les explorer ;
- Les quantifier ;
- Les horodater ;
- Définir leur origine.

2 – Quantification de la charge de travail

- La volumétrie,
- Le nombre d’acteurs,

font craindre une charge significative

3 – L'expert de partie

En amont il devra suggérer les mesures techniques à mettre en œuvre pour :

- Etre conforme au règlement européen,
- Limiter les risques de mise en cause.