# Intervention d'Isabelle FALQUE-PIERROTIN, présidente de la CNIL, au MEDEF

## Sujet : comment vous aider à être prêts en 2018 ?

***jeudi 2 mars 2017***

Bonjour à tous,

Merci de me donner au nom de la CNIL et du G29 l'occasion d'intervenir ce matin devant vous afin de présenter notre vision de cette échéance de 2018 et comment la CNIL et le G29 peut vous aider à s'y préparer.

Nous vivons une période « extraordinaire » à bien des points de vue.

- Un nouveau texte est applicable à compter de 2018 et ce texte change le type de régulation qui va s'appliquer aux données : moins de contrôle a priori par la CNIL, plus de responsabilisation obligations des entreprises, et un niveau de sanction très lourd (4% du CA). **Vous faites donc face à de nouvelles obligations que vous devez comprendre et connaître.**
- Ce texte commun à tous les pays européens remet les entreprises françaises, et européenne, à égalité de concurrence avec les entreprises étrangères même non établies en Europe dès lors qu'elles ciblent un européen. **C'est donc un texte qui vous redonne de la souveraineté !**
- La période post Brexit ouvre de façon inédite la question de la relocalisation sur le continent d'un certain nombre d'acteurs et donc, de l'attractivité de nos modes de régulation
- Enfin, nous sommes dans une année électorale ce qui fait que le texte national (loi CNIL 2) dont nous avons besoin pour « rabouter » notre législation nationale et le GDPR, notamment en matière de sanctions, aura un temps de préparation et d'étude très court, et doit être quasiment prêt pour un dépôt en CM en juin prochain.

Dans un tel contexte, que peut vous apporter la CNIL et comment se positionne le G29.

### Au plan national,

### a) 1er objectif : faire connaître et comprendre le Règlement

Le constat est préoccupant : moins d'un tiers des entreprises se sentent prêtes à se conformer, 97 % n'ont pas de plan d'action, 10 % considèrent qu'elles seront parfaitement prêtes. L'enjeu d'information et d'accompagnement est donc crucial.

**La CNIL a mis en place un plan structuré d'information et de communication sur le sujet à partir de notre site.** la CNIL diffuse sur son site une information large sur le règlement afin de répondre aux questions des professionnels : outre une présentation générale du règlement et une rubrique spécifique pour les délégués à la protection des données, elle publiera prochainement un document pédagogique résumant les 5 (ou 6) étapes pour se préparer au règlement, et sur une cadence mensuelle, des réponses aux questions les plus fréquemment posées (ex : mes anciennes AU resteront-elles valables ?

quelles modalités concrètes de notification de failles ?) sur le règlement européen afin d'assurer une sécurité juridique maximale aux entreprises.
*Concernant les PME/PM*I, qui bénéficient aujourd'hui de NS, mise en place d'une présentation simplifiée et didactique de leurs obligations à partir de la tenue de leur fichier client/prospects.

*De plus, les prestataires sous-traitants*, qui se voient imposer de nouvelles obligations (outre la désignation d'un délégué, la tenue d'un registre des traitements, une obligation de conseil en matière de failles de sécurité, études d'impact, sécurité, destruction des données, contribution aux audits…), feront aussi l'objet d'une rubrique dédiée.

### b) Accompagner le déploiement des nouveaux outils de mise en conformité

Le Règlement, cela a été dit, repose sur une nouvelle logique de régulation et de nouveaux outils : PIA, labels, certification, codes de conduite.

Alors que le montant des sanctions va être considérablement renforcé, l'enjeu pour vous est des lors, de vous familiariser avec les nouveaux outils de conformité, et de disposer d'un cadre de régulation adapté et juridiquement sûr.

Que pouvons-nous vous proposer à cette fin ? Je crois que la CNIL a de solides arguments et atouts car les nouveaux outils s'inscrivent dans la filiation de ceux que nous avons déployés depuis plusieurs années :

- **Sur les PIA** – obligatoires pour tous les traitements de données les plus risqués - : la CNIL a diffusé, dès 2012, une méthodologie pour bâtir les PIA ; actualisée en 2015 (document le plus téléchargé en anglais sur le site).
  Pour vous permettre de vous familiariser avec cette démarche, nous allons mettre en place dès à présent un système de « bac à sable », vous permettant de tester, à blanc, les PIA, pour vous entraîner sur ces nouveaux outils, sans prendre le moindre risque au regard de nos missions de contrôle.
  Nous allons demander au gouvernement de consolider cette faculté de « bac à sable » dans la loi CNIL 2.

- Par ailleurs, nous avons, par souci de simplification, développé depuis plusieurs années des **« cadres » de régulation sectoriels** : autorisations uniques ; packs de conformité, mais aussi une activité de labellisation (plus de 100 labels délivrés à ce jour). Tous ces outils participent d'une même logique : décliner, pour un secteur ou une activité, les obligations IL en construisant des référentiels opposables aux acteurs, mais aussi au régulateur. Car si vous respectez le cadre ainsi défini en amont, celui-ci aura un effet parapluie en cas de contrôle aval.

L'enjeu pour nous est maintenant de convertir ces référentiels, sur lesquels nous avons de l'avance, en référentiels nationaux ou européens.

La loi CNIL 2 va nous offrir une base légale pour les référentiels nationaux.
Concernant les référentiels européens, il s'agira, selon les cas, de recommandations de l'EDPB ; de lignes directrices ; ou de référentiels de certifications dont le respect sera certifié par des tiers homologués.

- **Sur les DPO :** avec près de 18 000 organismes dotés d'un CIL, nous avons l'expérience de l'animation de cette communauté depuis plus de 10 ans. Avec le Règlement, le nombre des DPO va fortement augmenter, concernant peut-être plus de 80 000 organisations, publiques ou privés.

  Le DPO est pour nous est un personnage central de la protection des données au sein de l'entreprise. A ce titre, il continuera à bénéficier d'un accompagnement dédié par la CNIL selon des modalités adaptées : webseminar, extranet en cours de refonte ; permanence juridique dédiée ; information privilégiée. Le DPO, en France, c'est le moyen de participer à la communauté de la *privacy*, d'en connaître les bonnes pratiques et par conséquent, là encore, de réduire l'aléa juridique.

  Nous lançons d'ailleurs une campagne de sensibilisation ce mois-ci sur le DPO. En particulier auprès des grandes têtes de réseaux, associations professionnelles, dont le rôle me parait essentiel pour faire passer les messages auprès de leurs adhérents et offrir le cas échéant la possibilité de délégués à la protection des données mutualisés, largement ouverte par le règlement.

- **Sur l'établissement principal enfin :** enjeu fort pour les entreprises transnationales à déterminer leur établissement principal pour avoir un interlocuteur unique parmi la communauté des régulateurs.

  La CNIL est clairement positionnée pour accompagner ces établissements, à la fois compte tenu de son influence et des moyens qu'elle peut mobiliser pour accompagner ceux-ci.
  Nous en avons d'ailleurs déjà l'expérience à travers notre rôle comme autorité lead dans plus du tiers des 92 BCR adoptés en Europe. Et c'est le sens de la réorganisation de ses services d'il y a trois ans en services sectoriels, qui sont autant de « points d'entrée uniques et professionnels » pour vos entreprises.

**Vous le comprenez : la CNIL se mobilise pour vous aider à utiliser tous ces nouveaux outils en capitalisant sur son expérience passée et dans le but de renforcer la sécurité juridique pour vos activités. Le but est de vous fournir un cadre clair pour limiter, autant que possible, les risques de sanctions. Et elle portera toute sa force technique et institutionnelle au G29 pour faire connaître sa doctrine et faire en en sorte que le nouveau cadre européen soit un atout au service des acteurs français et européens.**

Nous sommes en effet convaincus que la régulation si elle est appuyée sur des outils souples et proches du terrain ne doit pas être vu comme un coût ou un obstacle au développement des entreprises. Elle peut au contraire apporter à celles-ci la sécurité juridique dans un environnement très concurrentiel.

**Au plan européen : Le G29**

**Le G29 a deux objectifs principaux dans la période actuelle : clarifier le règlement et en faire un outil le plus lisible et opérationnel pour les acteurs ; construire la gouvernance européenne. Pour cela, des plans d'action successifs pour 2016, puis 2017 ont été adoptés. Ils visent à consolider la démarche**

**d'harmonisation recherchée par le Règlement sur les sujets clé du texte et à limiter le forum shopping.**

**Concernant les sujets clé d'harmonisation,** en 2016, quatre sujets avaient été identifiés comme prioritaires : le droit à la portabilité, le délégué à la protection des données, les analyses d'impact et la certification.

Les deux premiers thèmes permis au G29 de publier des lignes directrices fin 2016. Le G29 a lancé un appel à commentaires en décembre 2016 destiné à enrichir ces documents et publiera leur version définitive au printemps 2017.
Le sujet PIA devraient être adopté au printemps.
Concernant la certification, un atelier sera organisé en avril à Paris pour que toutes les autorités acquièrent une culture commune en la matière et que par suite, puisse être définie la répartition des responsabilités entre les DPA et les acteurs du marché.

Par ailleurs, de nouvelles lignes directrices sont en cours d'élaboration pour 2017 : le consentement, le profilage et les notifications de failles de sécurité. L'ensemble de ces lignes directrices devrait être publié courant 2017.

Il faut préciser que ces lignes directrices sont élaborées au terme d'une large concertation avec les parties prenantes, au niveau européen et national. C'est ainsi que la CNIL a systématiquement ouvert une consultation publique sur les différents thèmes abordés, afin de recueillir les questions concrètes ou propositions de bonnes pratiques des professionnels. Les premiers thèmes soumis à consultation à l'automne 2016 ont ainsi suscité plus de 500 contributions. Au niveau européen, un Fablab a été organisé à Bruxelles en juillet dernier.

Les 3 nouvelles thématiques inscrites au plan d'action 2017 du G29 pour le premier semestre seront ouvertes à la consultation publique en mars 2017 et un 2ième Fablab sera organisé à Bruxelles début avril.
Vous le voyez, l'objectif du G29 dans ses guidelines est de clarifier un texte qui est parfois un peu complexe et, surtout, de favoriser une interprétation commune de ce texte par les DPA.

**Concernant la gouvernance,** nous travaillons depuis plus d'un an pour mettre en musique les dispositions du Règlement sur les nouveaux modes de coopération entre DPA : assistance mutuelle, contrôle commun, guichet unique, et surtout la nouvelle institution européens qui succède au G29, l'EDPB.
La tâche est lourde mais je dois dire que nos équipes progressent vite dans l'apprentissage de la coopération. Alors que le dossier Google apparaissait comme un cas à part il y a 4 ans en termes de coopération entre autorités, s'est mis en place des échanges réguliers et de plus en plus confiants entre les équipes et une vraie communauté des régulateurs européens est en train d'émerger. L'enjeu est important : être capable de prononcer des sanctions communes et surtout, construire une doctrine européenne commune.

**Je terminerai par l'international en vous disant que face à un environnement numérique mondial, la CNIL souhaite s'inscrire pleinement dans cette dimension, d'une part en travaillant à des outils mondiaux, d'autre part en assurant la promotion des positions françaises ou européennes.**

**A ce titre, l'évènement clé est celui du *Privacy Shield*.**
**Le *Privacy Shield*, accord entre l'Europe et les USA qui a été conclu avant l'été pour remplacer le défunt *Safe harbour*, invalidé par la cour de justice européenne en octobre 2015.**

Cet accord témoigne de l'émergence d'une forme de standard mondial sur les conditions dans lesquelles il est possible, pour des raisons de sécurité nationale, d'avoir accès aux données de citoyens européens. Il est l'expression mondiale d'une approche européenne sur les données.

Il fait entrer dans une négociation commerciale des enjeux de libertés publiques et de droits fondamentaux, ce qui témoigne de l'importance qu'a pris le sujet de la protection des données dans les dernières années et des attentes de nos concitoyens en la matière.

Le G29 a beaucoup travaillé sur le sujet. Il est, je crois, largement à l'origine de l'accord qui a été conclu. Tout en se félicitant des progrès réalisés, il a cependant exprimé des réserves rappelant avec force notre position sur la surveillance de masse et indiscriminée et considérant que celle-ci ne saurait être compatible avec nos principes.

Depuis 1er août 2016, le *Privacy Shield* est entré en vigueur. Le G29, en coopération avec la FTC et le Département du commerce travaille au pilotage opérationnel du *Privacy Shield*. Dans ce contexte, la première revue annuelle, sera un évènement particulièrement important au cours duquel les autorités de protection des données seront particulièrement vigilantes et elles s'assureront que leurs inquiétudes sont belles et bien prises en compte en pratique. Cette première revue sera donc pour nous l'occasion de donner notre appréciation finale sur le niveau d'adéquation du *Privacy Shield* et de rassurer le citoyen européen sur l'accès à ses données par les autorités américaines.

**Conclusion :**

Mesdames, messieurs, voilà ce que je souhaitais partager avec vous ce matin.
Le règlement est un texte majeur, renforçant la souveraineté européenne, individuelle et collective sur les données. Il est destiné à bâtir la régulation des données pour de nombreuses années ce qui justifie pleinement les investissements importants que vous vous apprêtez tous à faire, pour être prêts en mai 2018.
La CNIL est à votre service pour vous accompagner dans ce voyage et faire en sorte que vous puissiez bénéficier d'un cadre juridique stable et robuste.