THE Security Transformation RESEARCH FOUNDATION

# RGPD : à quoi s'attendre jusqu'au 25 Mai et au-delà ?

Face à un contexte général de non-conformité, l'attitude des régulateurs sera déterminante

*Les facteurs clés à considérer en 2018 pour les conseils d'administration et les dirigeants*

Avril 2018

# RGPD : L'Etat des Lieux

Tout au long de l'année 2017, le succès du RGPD a été d'attirer l'attention des conseils d'administration, des cadres et des managers sur des questions – jusqu'à présent trop souvent ignorées - de sécurité et de respect de la vie privée.

De nombreuses entreprises sont actuellement engagées dans d'ambitieux programmes de mise en conformité, et allouent des sommes considérables au RGPD (près de £15M en moyenne pour les organisations du FTSE100 selon une étude récente de SIA Partners*)

Le RGPD a sans aucun doute été un élément catalyseur permettant d'impliquer des couches managériales traditionnellement moins concernées par les questions de sécurité et de protection de la vie privée, et d'assurer l'allocation de budgets conséquents dans des domaines jusqu'à présent trop souvent délaissés.

Tous les secteurs économiques et industriels ont été affectés, bien que les entreprises B2C soient évidemment plus concernées et plus engagées dans le domaine que de plus petits acteurs du B2B, et cela en dépit d'autres obligations réglementaires pour certains secteurs sur 2017 (ex : MiFID II dans l'industrie financière).

Le RGPD est perçu comme faisant partie d'une évolution sociétale sur le long terme vers une utilisation plus responsable et éthique par les organisations (privées comme publiques) des données personnelles qui leur sont confiées.

https://www.sia-partners.co.uk/preparing-gdpr-need-15m-300-450-per-employee-average-implement-gdpr/

# L’accent reste sur la « mise en conformité» … mais le concept est mal défini.

« Ce qu’il faut faire » reste un concept flou pour beaucoup d’entreprises.

La régulation est complexe : 99 articles, des centaines de points de contrôles potentiels, et un langage qui reste ouvert à interprétation dans plusieurs domaines : « Grande échelle », « état de l’art », mesures de protection « appropriées », etc.

La «conformité» n’est pas un concept bien défini et chaque entreprise se retrouve à devoir déterminer pour elle-même «  ce qu’il faut faire » souvent aidée par des tiers (et les marchands de solutions toutes-faites prolifèrent).

Face à un problème fondamentalement transverse, chaque département tend à mettre l’accent sur les enjeux de mise en conformité qu’il comprend le mieux et dont il est le plus proche.

Les problèmes sont généralement formulés autour de la question des données plutôt que de la nature, légitimité, ou sensibilité de leurs traitements.

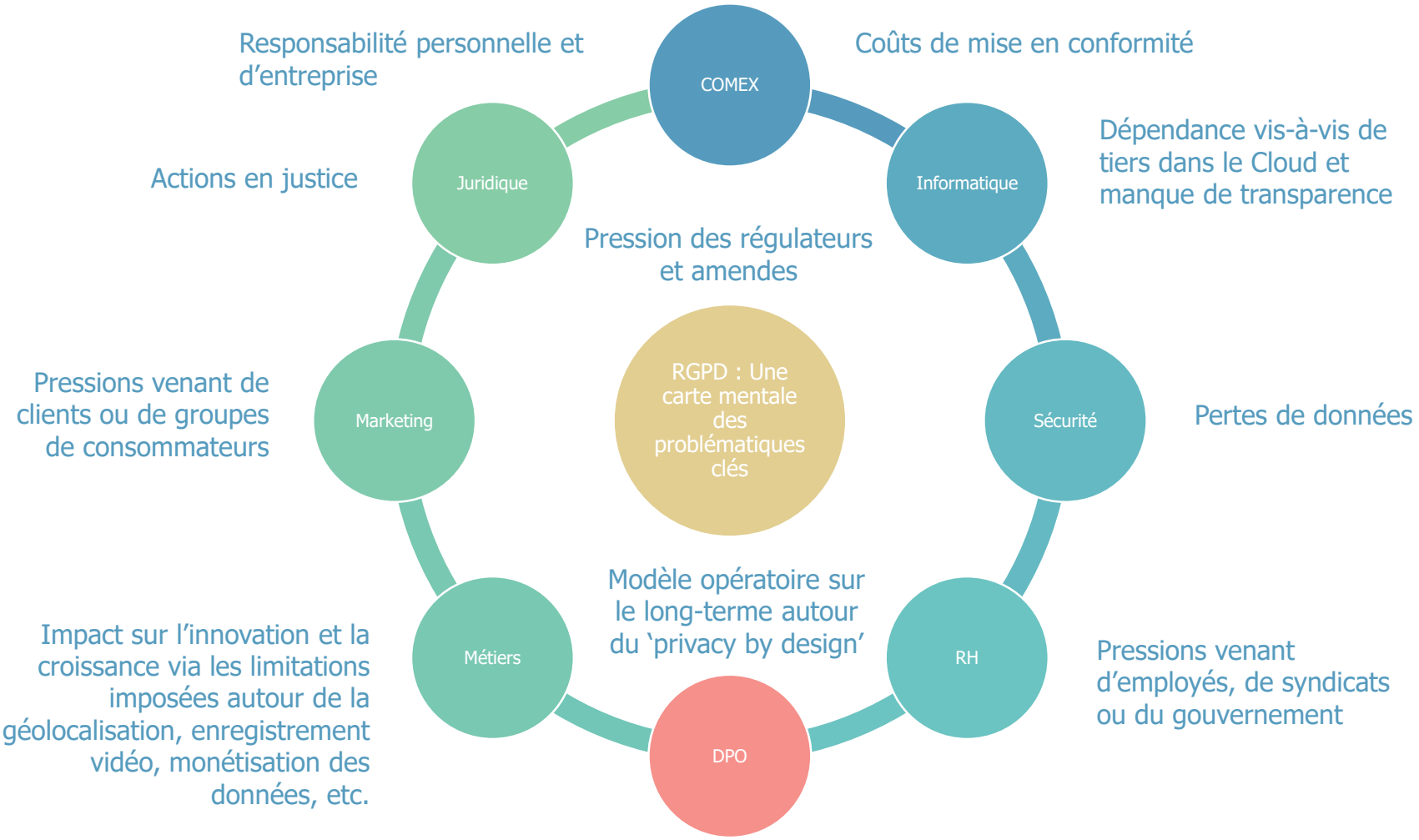
Le rôle du DPO est en train de s’affirmer, mais sa nécessaire indépendance le rend difficile à positionner et à opérer pour beaucoup d’organisations.

De nombreuses voix — surtout dans le B2B— commencent à s’élever autour de la nécessité réelle d’embaucher un DPO plutôt qu’un poste de type ‘Chief Privacy Officer’ — qui serait plus dans la pratique et soumis à moins de contraintes.

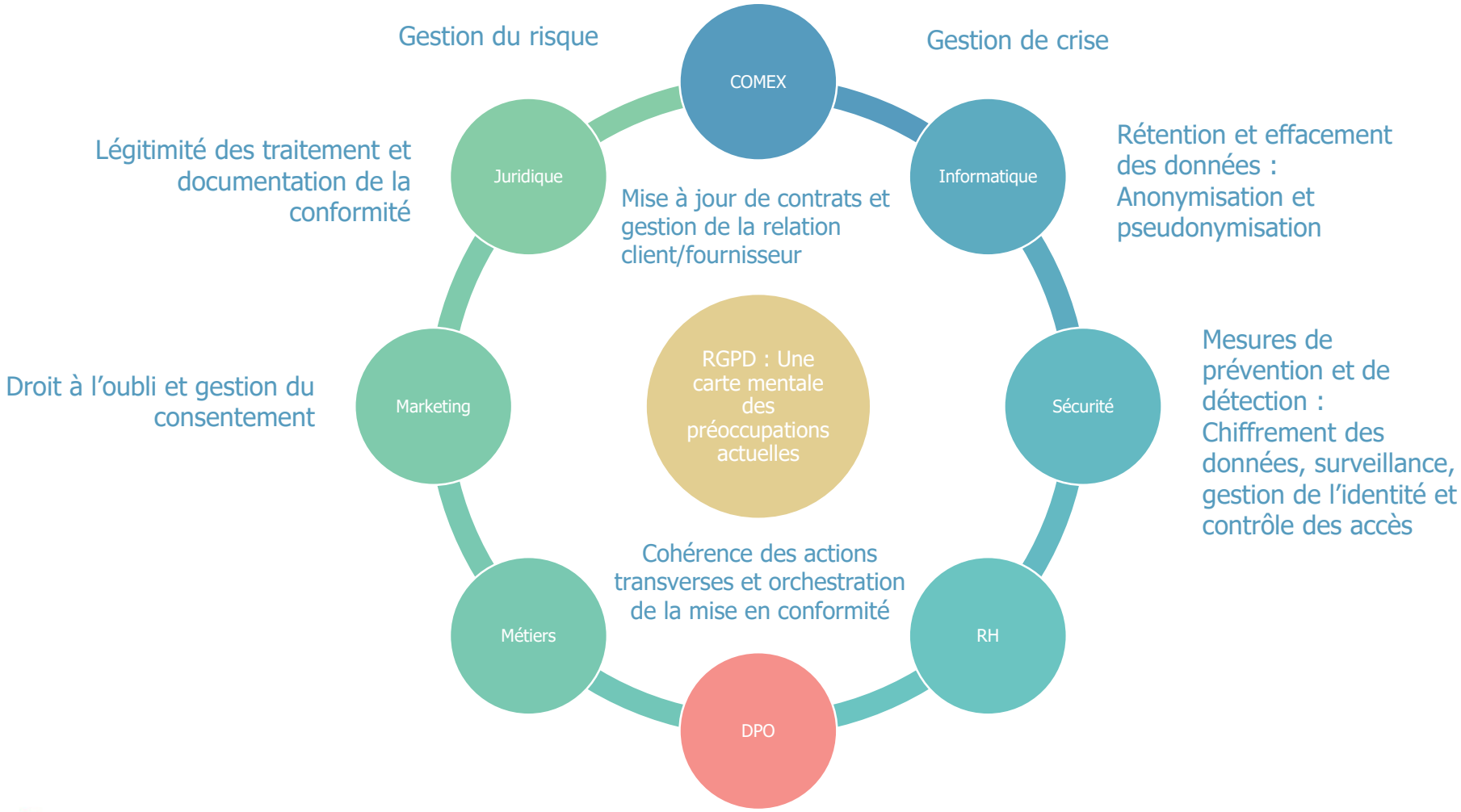
La vision à long terme des régulateurs est incertaine, et les indications officielles n’ont pour l’instant pas donné d’éclaircissements pratiques à ce sujet.

Des programmes de certifications en conformité RGDP vont certainement émerger mais ils devront se bâtir une crédibilité et feront face, au début, aux mêmes problèmes de définition.

# RGPD : Une carte mentale des problématiques clés



# RGPD : Une carte mentale des préoccupations actuelles



# RGPD : les « known unknowns », les “inconnues connues”

Personne ne veut devenir le premier cas traité dans le cadre du RGPD, mais quelqu’un le sera inévitablement.

Quel pays, quel régulateur, agira le premier ? Est-il envisageable que certains régulateurs commencent à « sonner aux portes » dès le 28 mai ?

Les multinationales doivent-elles s’inquiéter d’un risque de contagion (une enquête dans un pays conduisant d’autres régulateurs à ouvrir eux aussi une enquête) ?

Est-il concevable que certains régulateurs soient beaucoup plus — ou moins — durs que d’autres sur certains aspects, faisant ainsi jurisprudence à travers l’Europe ?

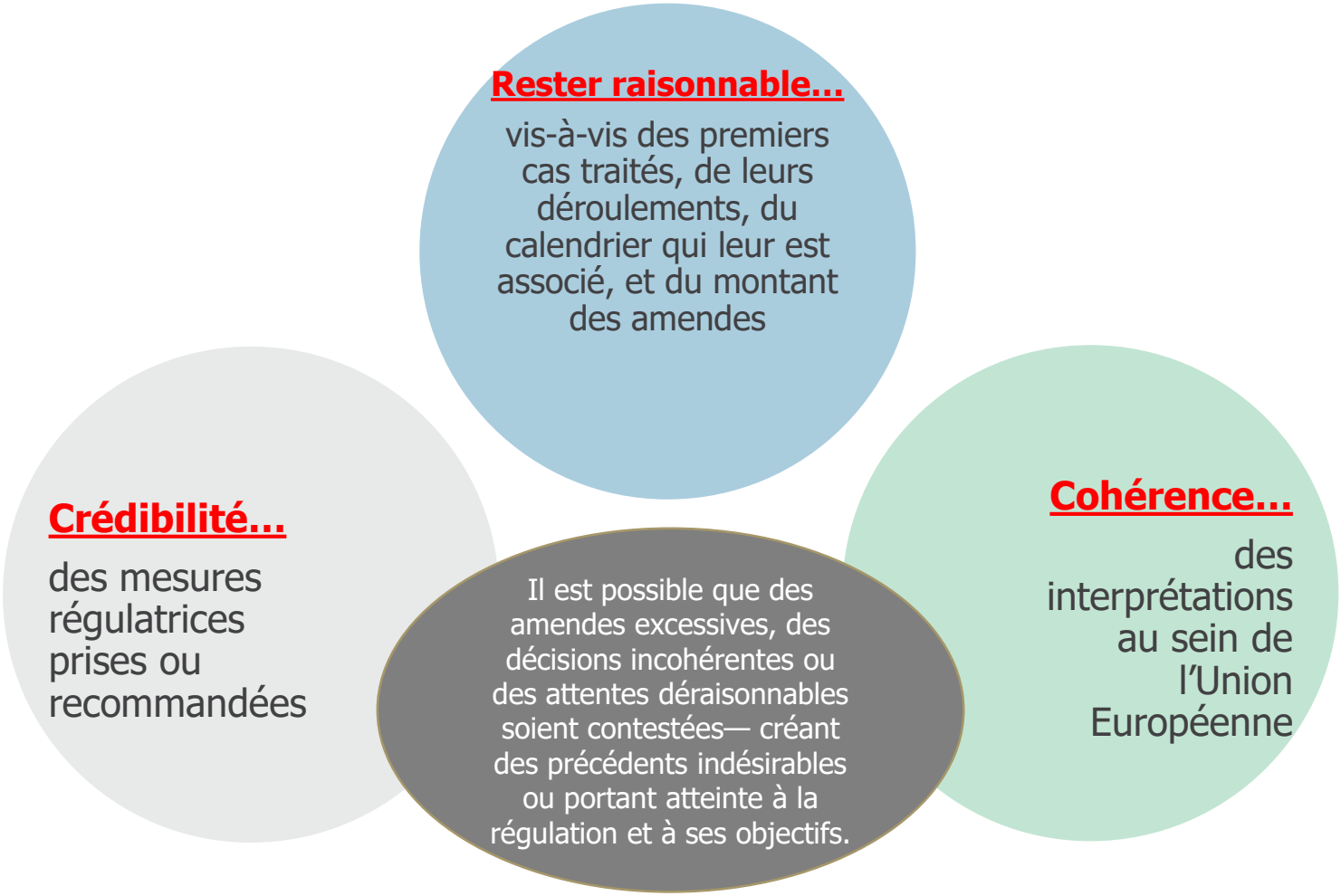
Quels seront les profils des premier cas traités ? Quel sera l’ordre de grandeur des premières amendes ? Seront-elles contestées, et devant quelle cour ? Sur quelles bases légales ? Ces appels aboutiront-ils ?

Devons-nous nous attendre à des conflits avec d’autres régulations (par exemple ePrivacy) ou avec des législations domestiques ?

Quelle-sera la vraie capacité d’investigation des régulateurs et seront-ils capables de se concentrer sur autre chose que les cas les plus importants ou les plus médiatisés ? Est-il possible que rien ne se passe réellement pour la majorité des entreprises européennes ?

Est-il concevable que le RGPD ne soit qu’un outil massif spécifiquement conçu pour s’attaquer aux géants américains de la tech (Google, Facebook, Uber, etc.) ou aux intérêts russes ou chinois ? Quel sera le véritable degré d’indépendance des régulateurs vis-à-vis des acteurs politico-économiques européens ?

# Les régulateurs ont un équilibre très fin à trouver (collectivement)



# L'attitude des régulateurs est désormais le facteur clé

L'attitude des régulateurs dans la mise en œuvre du RGPD à compter du 25 mai devient le facteur clé pour l'année à venir, mais ne peut pas être anticipée.

- 80% des entreprises ne seront pas « conformes » (quoi que cela signifie)
- Le choix sera délibéré pour 50% d'entre elles après une analyse coût-risque

*(Source: Forrester – Predictions 2018 "A Year of Reckoning")*

Les régulateurs à travers l'UE demandent de plus larges prérogatives depuis plus de dix ans. Il faut s'attendre à ce qu'ils cherchent à les exercer au delà du 25 mai avec l'entrée en vigueur du RGDP.

Mais chaque régulateur domestique a ses propres habitudes historiques, préoccupations, contraintes, ressources et priorités. Ces facteurs ne s'effaceront pas du jour au lendemain et continueront à influencer la manière dont le RGPD est mis en place.

Au delà du 25 mai, la prochaine date importante devient le moment, aujourd'hui inconnu, de la publication de la première décision règlementaire relative au RGPD.

# Le rôle du DPO va devenir central dans les plus grandes entreprises, mais il ne peut pas fonctionner seul

C'est l'une des pierres angulaires du nouveau réglement mais, au dela de son indépendence imposée, il doit s' établir en tant que véritable fonction au sein de l'entreprise

C'est en pratique une véritable industrie nouvelle qui émerge en Europe avec près de 28000 postes qui devraient être créés (source : IAPP). Cela prendra cependant plusieurs années avant que les programmes d'éducation et de certification pertinents soient mis en place dans chaque pays.

Le poste doit être indépendant du traitement des données, mais beaucoup d'acteurs dans l'entreprise attendent des conseils pratiques du DPO sur la manière d'interpréter la régulation et de s'y conformer. Le rôle de DPO ne doit pas devenir un rôle inutile, enfermé dans une tour d'ivoire.

L'orchestration de la mise en conformité au travers des différentes divisions des grandes entreprises fera de ce poste un rôle senior exigeant un leadership transversal — qui doit attirer un cadre avec une profonde connaissance du fonctionnement interne de l'entreprise.

Au-delà du rôle lui-même, des compétences très diverses sont associées à la fonction (juridiques, techniques, etc.) qui pourraient être distribuées au sein d'une équipe — en interne ou non.

https://iapp.org/news/a/study-at-least-28000-dpos-needed-to-meet-gdpr-requirements/

# Au-delà des principes arbitraires d'indépendance, comment faire fonctionner le rôle du DPO en pratique ?

Un mode opératoire clair est essentiel pour définir tous les rôles et les responsabilités autour du poste de DPO.


Les équipes opérationnelles demandent, avec raison, de la clarté et de la cohérence concernant le RGPD pré- et post- 25 mai.

La «conformité » — une fois définie — ne doit pas être comprise comme un concept statique ; le règlement évoluera post 25 mai quand les décisions et les jurisprudences émergeront et la « conformité » avec lui.

Qui sera responsable de l'interprétation de la régulation et de ses futures évolutions, et de donner des conseils pratiques aux équipes opérationnelles autour du maintien en conformité ?

Si cela ne peut pas être le/la DPO pour des raisons d'indépendance, positionner et structurer cette compétence de manière claire et pratique au sein de l'organisation est essentiel.

# La marche à suivre

## Si vous avez déjà un programme de mise en conformité en cours

Ne soyez pas obsédés par la date du 25 mai: Gérez sans complaisance obstacles et priorités et continuez à progresser

Il ne s'agit pas simplement de cocher des cases, et rien ne s'arrête le 25 mai. Continuez dans votre lancée et focalisez les attentes sur un calendrier réaliste et réalisable.

Des preuves tangibles de soutien de la part des hautes couches managériales et une approche traçable sur le long-terme visant à mettre en place les principes de 'privacy by design' (qui sont au cœur du RGPD) joueront toujours en votre faveur vis-à-vis des régulateurs, quelles que soient les difficultés de mise en conformité ou de mise en œuvre que vous rencontrerez.

L'objectif principal doit être le maintien en conformité une fois que le programme de travail actuel a rempli ses objectifs.

Attendez-vous à ce que les attentes et les perceptions changent en fonction des acteurs durant la seconde moitié de 2018 quand les régulateurs commenceront à prendre des décisions et que les premiers précédents émergeront.

Le/la DPO aura un rôle clé dans l'orchestration de cette phase dans beaucoup d'entreprises. Si ce rôle n'est pas encore en place, le poste — ou un rôle équivalent — doit être mis en place dès que possible.

Aujourd'hui plus que jamais, une gouvernance transversale forte est cruciale : Commencez à regarder au travers des différentes divisions de l'entreprise et vers un modèle opérationnel efficace à long-terme autour du rôle du DPO pour assurer la mise en œuvre pérenne du 'privacy by design'.

# La marche à suivre

## Si vous démarrez maintenant

Désignez un responsable immédiatement  pour porter le sujet et élaborez un plan en vue du 25 mai et au-delà.

Ne vous précipitez pas dans l'achat d'une solution technologique à un problème que vous ne comprenez pas pleinement.

Concentrez vos efforts pré-25 mai sur l'analyse de votre degré d'exposition et lancez immédiatement une série de tâches pratiques qui forceront les divers acteurs à se confronter au sujet avant le 25 mai.

- Commencez à construire un registre de vos activités de traitement des données personnelles (nature, type, légitimité, sensibilité, échanges transfrontaliers, arrangements avec des tiers, etc.). Evaluez le volume réel de données personnelles que vous possédez.
- Engagez avec les acteurs pertinents autour du rôle long-terme du DPO, déterminez si vous en avez besoin, qui cela pourrait être, et où le poste serait positionné dans votre organisation interne. Considérez si la personne portant le sujet pourrait devenir votre DPO après le 25 mai.
- Relisez les conditions d'utilisation sur votre site internet et les règlements intérieurs ou chartes pour vos employés, vos procédures en cas d'incidents de sécurité, vol de données ou demandes d'accès  aux données personnelles. Si elles n'existent pas, il s'agit de les créer de toute urgence (en impliquant tous les acteurs pertinents), sinon, mettez-les en conformité avec les attentes du RGPD.
- Organisez la simulation d'un incident de perte de données en impliquant toutes les parties prenantes au sein de l'entreprise jusqu'au conseil d'administration (DSI, Juridique, RH, Communications, etc.)
- Notez soigneusement chaque décision prise et la raison pour laquelle elle a été retenue.

En parallèle, identifiez des objectifs réalistes de mise en conformité pour la fin de l'année, définissez un plan, une équipe en charge et un budget.

# Contacts et Remerciements

**Pierre Poinsignon**
Arsia Mons
pierre.poinsignon@arsiamons.fr
+33 (0)6 15 45 85 68
www.arsiamons.fr

**Jean-Christophe Gaillard**
Corix Partners
jcgaillard@corixpartners.com
+44 (0)7733 001 530
www.corixpartners.com

**Richard Preece**
DA Resilience
richard@daresilience.com
+44 (0)7954 694 391
www.daresilience.com

**Frederic Halley**
Next World Capital
frederic@nextworldcap.com
+44 (0)7572 690 509
www.nextworldcap.com

**David Hozé**
Wise Partners
david.hoze@wise-partners.fr
+33 (0)6 09 75 63 36
www.wise-partners.fr

Merci aux membres de notre groupe de travail et à tous les contributeurs.

**Mark Segelov,** Colt Technology Services
**Nick Simms**, Cornwood Risk Management
**Rupert Brown,** The Cyber Consultants
**Ross Jackson / Harvey Seale,** Mimecast
**Andrew Bullivant / Alistair Roberts,** Pension Insurance Corp.
**Karin Lange / Jean-Marie Lapeyre**, PSA Opel Vauxhall
**Steve Lamb**, Rapid 7
**Neil Cordell**, Target Group

**Laure Jallet / Cecile Lagardere**, Care Insight
**Yann-Herve Beulze,** Groupama Asset Management
**Catherine Bouzigues**, Wise Partners

THE
Security
Transformation
RESEARCH FOUNDATION

www.securitytransformation.com

@Transform_Sec

**The Security Transformation Research Foundation is a dedicated think-tank and research body aimed at approaching Security problems differently and producing innovative and challenging research ideas in the Security, Business Protection, Risk and Controls space**



French version – FINAL 1.0