

Le Digital Compliance Officer

03

Avant-propos



La conformité numérique n'a jamais été aussi stratégique, transversale et déterminante pour la confiance, la performance et la valeur des organisations.

Longtemps abordée comme une réponse au RGPD, elle a permis de diffuser une culture de responsabilité et de structurer des pratiques. La fonction de DPO a joué un rôle fondamental. Mais le paysage a profondément évolué.

L'intensification des usages numériques, l'irruption massive de l'intelligence artificielle, la montée des cybermenaces et la responsabilisation accrue des dirigeants ont fait entrer la conformité dans une nouvelle dimension, où les enjeux se croisent, et où les décisions ne peuvent plus être prises en silos.

L'adoption successive du règlement sur l'IA (AI Act), de la directive NIS2, du règlement DORA, du DSA et de la loi SREN a considérablement élargi le périmètre juridique du numérique. **Ces textes créent des obligations distinctes, souvent croisées, qui dépassent le champ de compétence d'une seule fonction.**

La conformité irrigue désormais la stratégie d'innovation, la sécurité et la résilience opérationnelle, la gouvernance des systèmes d'IA, la structuration contractuelle IT, et la valorisation des actifs immatériels.

C'est dans ce contexte qu'émerge le Digital Compliance Officer (DCO). Le DCO n'est pas une remise en cause du DPO. Il en est l'évolution logique — une approche élargie, pro-business, intégrée aux choix stratégiques, pensée dès la conception des projets.

Ce livre blanc formule une proposition précise : confier à une fonction unique, et spécialisée, la coordination de l'ensemble des obligations juridiques attachées aux projets numériques et innovant.

Externalisé, le DCO devient un partenaire de confiance des dirigeants, des directions juridiques, des DSI et des RSSI. Il ne se contente pas de vérifier la conformité : il l'organise, la priorise et la transforme en levier de sérénité, de crédibilité et de valorisation.

NODAL Avocats

Stéphane Astier & Anne-Charlotte Andrieux

Introduction



La question n'est plus : « Sommes-nous conformes ? » Mais : « Notre conformité est-elle pilotée, intégrée et créatrice de valeur ? » Le Digital Compliance Officer apporte cette réponse.

L'adoption successive du RGPD, de l'AI Act, de NIS2, de DORA, du DSA et de la loi SREN a créé un paysage réglementaire dense, transversal et en mouvement constant. Ces textes créent des obligations distinctes, souvent croisées, qui dépassent le champ de compétence d'une seule fonction.

Cette évolution appelle une approche nouvelle : non une addition de fonctions spécialisées, mais une architecture juridique cohérente, capable d'articuler les différents cadres normatifs et de les traduire en décisions stratégiques.

C'est pour répondre à cette réalité que la fonction de DCO a émergé — non comme une mode managériale, mais comme une nécessité organisationnelle : une conformité intégrée, stratégique, orientée vers la maîtrise globale du risque numérique.

AUTEURS

NODAL Avocats

contact@nodal-avocats.com

Chapitre I

Les errements de la conformité numérique



1. Vers la fin d'une conformité sectorisée

La conformité numérique s'est progressivement imposée comme un élément structurant de la gouvernance des organisations. D'abord centrée sur les données personnelles, la fonction de DPO a permis de diffuser des réflexes essentiels de responsabilité et de traçabilité. Mais cette première étape ne suffit plus.

Le numérique est devenu un socle opérationnel et stratégique. Dans ce contexte, **la conformité ne peut plus être pensée par domaines étanches**. Les enjeux de protection des données interagissent avec les choix d'architecture IT, les dispositifs de cybersécurité, les systèmes d'IA, les obligations applicables aux plateformes et les responsabilités pénales et civiles des dirigeants.

La multiplication des textes européens et nationaux — RGPD, RIA, NIS2, DORA, DSA, loi SREN — illustre cette réalité : **le législateur ne régule plus des objets isolés, mais des écosystèmes numériques complets**.

2. Des attentes nouvelles à prendre en compte

Le RGPD a structuré dans les organisations une approche centrée sur les données personnelles. Cette concentration était cohérente avec l'état du droit en 2018. Elle ne l'est plus.

Les organisations sont désormais assujetties à des obligations de nature technique (NIS2, DORA), sectorielle (AI Act) et comportementale (DSA) qui excèdent — juridiquement et structurellement — le périmètre de la fonction de DPO.



3. La fonction DPO face à un changement d'échelle

Le DPO demeure une fonction indispensable, mais il se trouve aujourd'hui confronté à un changement d'échelle. L'élargissement du champ normatif impose une expertise transversale allant bien au-delà de la seule protection des données personnelles.

Dans la pratique, le DPO est souvent sollicité sur des sujets qui excèdent son rôle légal : conformité des projets d'IA, sécurisation contractuelle des systèmes d'information, préparation à des incidents cyber, gestion de plateformes et de contenus.

Cette situation ne traduit pas une insuffisance de la fonction, mais une inadéquation croissante entre un cadre juridique initial et la réalité contemporaine du numérique.

4. Le risque d'un décalage entre conformité et stratégie

Lorsque la conformité reste cantonnée à une approche technique ou documentaire, un décalage peut s'installer avec la stratégie de l'organisation. Ce décalage se manifeste par des projets innovants conçus sans gouvernance juridique, des arbitrages opérés en dehors du cadre de conformité, et une difficulté à démontrer la maîtrise effective des risques.

À l'inverse, **les organisations qui intègrent la conformité au cœur de leurs choix stratégiques constatent un bénéfice tangible** en termes de confiance, de lisibilité et de crédibilité.

Chapitre II

Du DPO au DCO : l'évolution naturelle de la fonction conformité



1. D'une fonction spécialisée à une fonction transversale

Un même projet peut mobiliser simultanément des données personnelles, des algorithmes d'IA, des infrastructures cloud, des prestataires IT, des obligations de cybersécurité.

Le DCO ne remplace pas les expertises existantes, il les coordonne dans une vision transversale.

2. Du contrôle au pilotage

Le DCO incarne un changement de posture : il ne se positionne pas en bout de chaîne, mais au cœur des processus de décision. Sa mission n'est pas de dire uniquement ce qui est interdit, mais de construire juridiquement ce qui est possible.

3. Une conformité alignée sur les objectifs business

Le DCO adopte une approche résolument pro-business : il hiérarchise les risques, priorise les actions à fort impact, adapte les exigences juridiques aux réalités opérationnelles de chaque organisation.

4. Le DCO comme interface stratégique

Il se situe à l'intersection des directions générales, des directions juridiques, des DSI et RSSI, et des équipes innovation. Il traduit les contraintes juridiques en décisions opérationnelles et les enjeux technologiques en risques juridiquement maîtrisés.

5. Une fonction adaptée à la régulation contemporaine

La multiplication des textes applicables au numérique traduit une volonté du législateur de responsabiliser les organisations dans leur globalité. La conformité doit être pensée comme une fonction de gouvernance à part entière. Le DCO répond à cette exigence : une conformité intégrée, stratégique, orientée vers la maîtrise globale du risque numérique.

Chapitre III

Le périmètre du DCO : une couverture globale du risque numérique



01 Le socle historique : protection des données et gouvernance RGPD

La conformité RGPD demeure le fondement de toute gouvernance numérique. Dans ce cadre, le DCO assume pleinement les missions traditionnelles du DPO : pilotage de la conformité des traitements, accompagnement des projets dès la phase de conception, gestion des droits des personnes, relations avec l'autorité de contrôle, sensibilisation et structuration des processus internes.

Mais cette mission est abordée dans une logique renouvelée : la protection des données n'est pas traitée comme une fin en soi, mais comme un fondement de confiance. La gouvernance RGPD devient ainsi un socle de confiance, sur lequel peuvent s'appuyer les projets stratégiques de l'organisation.

02 Intelligence artificielle : conformité, gouvernance et responsabilité (RIA / AI Act)

L'essor des systèmes d'intelligence artificielle transforme profondément les modèles économiques, mais il s'accompagne d'un cadre réglementaire exigeant.

Le DCO intervient pour :

- qualifier juridiquement les systèmes d'IA,
- identifier les niveaux de risque,
- structurer la gouvernance des modèles et des données,
- organiser la documentation et la traçabilité requises,
- anticiper les responsabilités juridiques et pénales.

L'approche du DCO vise à sécuriser l'innovation, non à la freiner. En intégrant la conformité IA dès la conception des projets, il permet aux organisations de développer des solutions robustes, crédibles et acceptables sur le long terme.

03 Systèmes d'information et contract management IT

La dépendance croissante aux systèmes d'information fait du contract management IT un enjeu central de conformité numérique.

Le DCO accompagne les directions juridiques et les DSI dans :

- la structuration et la négociation des contrats IT (cloud, SaaS, infogérance, cybersécurité),
- l'alignement contractuel avec les exigences réglementaires,
- la répartition maîtrisée des responsabilités,
- l'anticipation des risques opérationnels et contentieux.

Cette intervention permet de transformer les contrats IT en outils de gouvernance, et non en simples documents juridiques déconnectés des usages réels.



04 Cybersécurité, résilience et conformité NIS2 / DORA

Les exigences issues de NIS2 et de DORA marquent un tournant : la cybersécurité devient une obligation de gouvernance, impliquant directement les dirigeants.

Le DCO intervient pour :

- structurer la gouvernance cyber,
- articuler les exigences juridiques et techniques,
- accompagner la mise en conformité organisationnelle,
- préparer les dispositifs de gestion d'incident,
- coordonner les acteurs internes et externes en cas de crise.

Dans cette logique, la cybersécurité n'est plus seulement une affaire technique : elle devient un enjeu juridique, stratégique et réputationnel.

05 Plateformes numériques, contenus et régulation (DSA, loi SREN)

Les obligations applicables aux plateformes et aux contenus imposent une vigilance accrue en matière de gouvernance, de modération et de responsabilité.

Le DCO accompagne :

- l'analyse des statuts et obligations applicables,
- la structuration des processus de modération et de signalement,
- la documentation des diligences,
- la gestion des risques de responsabilité.

L'objectif est de sécuriser les modèles économiques numériques tout en garantissant une conformité proportionnée et opérationnelle.

06 Gestion de crise numérique et cyber

Les crises numériques ne relèvent plus de l'exception.

Incident cyber, fuite de données, défaillance d'un prestataire IT, mise en cause publique : ces situations exigent une réaction rapide, coordonnée et juridiquement maîtrisée.

Le DCO intervient :

- en amont, par la préparation et les scénarios de crise,
- en aval, par le pilotage juridique de la gestion de crise,
- en coordination avec les équipes techniques, la communication et la direction.

Cette capacité d'intervention renforce la résilience globale de l'organisation et limite l'impact juridique, financier et réputationnel des incidents.

Chapitre V

L'approche NODAL : le DCO externalisé comme levier de valeur



Le Digital Compliance Officer ne prend pleinement son sens que s'il s'inscrit dans une méthode.

Chez NODAL Avocats, le DCO n'est pas une addition de prestations de conformité : il est l'expression d'une approche globale, reposant sur trois piliers indissociables : l'externalisation assumée, la méthode LegalOps, et la logique de valorisation.

01	Le choix stratégique de l'externalisation : compétence, indépendance et crédibilité La complexité et l'évolution permanente des cadres applicables au numérique rendent illusoire la concentration de l'ensemble des compétences requises au sein d'une fonction interne unique. Externaliser le DCO permet au contraire : • d'accéder immédiatement à une expertise juridique de haut niveau, • de bénéficier d'une veille normative et jurisprudentielle continue, • de mobiliser une vision transversale couvrant l'ensemble des risques numériques, • d'assurer une indépendance fonctionnelle essentielle à la crédibilité de la conformité.
02	Le DCO NODAL : une fonction intégrée aux centres de décision L'externalisation ne signifie pas éloignement. Le DCO NODAL est conçu pour être au plus près des centres de décision. Il intervient : • aux côtés des dirigeants, • en lien étroit avec les directions juridiques, • en coordination permanente avec les DSI et RSSI, • en amont des projets structurants. Cette proximité permet de faire de la conformité un outil d'aide à la décision, et non un filtre bloquant. Le DCO NODAL ne se contente pas d'identifier les risques : il propose des solutions juridiques opérationnelles, adaptées au modèle économique et aux objectifs stratégiques de l'organisation.
03	La méthode LegalOps : intégrer intelligemment le juridique dans l'organisation La spécificité de l'approche NODAL repose sur une application exigeante du LegalOps à la conformité numérique. Concrètement, cela signifie : • intégrer le juridique dans les processus existants, • adapter les exigences réglementaires aux réalités opérationnelles, • structurer des outils et des workflows utiles, • prioriser les actions à fort impact.



04	La conformité comme actif immatériel et levier de valorisation
05	Une conformité orientée solutions
06	Le DCO NODAL : une fonction centrale de la gouvernance numérique

L'un des apports majeurs de l'approche NODAL réside dans la manière dont la conformité est pensée : non comme un coût, mais comme un actif immatériel. Les évolutions jurisprudentielles et les pratiques de marché démontrent que la conformité numérique joue désormais un rôle déterminant dans la valorisation des entreprises, l'appréciation des risques par les investisseurs, les opérations de croissance externe et les partenariats stratégiques.

Le DCO NODAL contribue directement à cette valorisation en :

- sécurisant les actifs data et IA,
- structurant la gouvernance numérique,
- documentant les diligences de manière pertinente,
- renforçant la crédibilité de l'organisation face aux tiers.

La conformité devient alors un facteur de confiance mesurable, intégré dans l'évaluation globale de l'entreprise.

L'approche NODAL repose sur une conviction forte : la conformité n'est utile que si elle permet d'agir.

Le DCO ne se limite pas à rappeler les interdits. Il construit des solutions juridiques stratégiques, permettant :

- de lancer un projet IA dans un cadre sécurisé,
- de structurer un écosystème IT résilient,
- de gérer une plateforme ou des contenus en conformité,
- de traverser une crise numérique sans perte de contrôle.

C'est cette capacité à transformer le droit en levier opérationnel qui fait du DCO NODAL une fonction clé de la gouvernance contemporaine.

En combinant externalisation, LegalOps et logique de valorisation, le DCO NODAL s'impose comme :

- un point de convergence des enjeux numériques,
- un partenaire stratégique des dirigeants,
- un facteur de confiance durable,
- un levier de performance et de différenciation.

La conformité numérique n'est plus une obligation périphérique. Elle devient une fonction centrale, structurante, créatrice de valeur.

Conclusion

La conformité numérique comme fonction stratégique de gouvernance

La conformité numérique a changé de nature. Elle n'est plus un simple exercice de mise en conformité réglementaire, ni une fonction périphérique reléguée à la gestion des risques. Elle est devenue un **enjeu central de gouvernance**.

Dans un environnement marqué par l'accélération technologique, la densité normative et l'exposition croissante des organisations aux risques numériques, une réponse nouvelle s'imposait. Le DPO a permis de structurer une première réponse. Mais **le changement d'échelle appelle une évolution structurelle**.

Le Digital Compliance Officer incarne cette évolution. Il la pilote. Il éclaire les décisions. Il sécurise les projets et les rend possibles.

Externalisé, le DCO devient un partenaire de confiance des dirigeants, des directions juridiques, des DSI et des RSSI. Chez NODAL Avocats, le DCO n'est pas une prestation isolée, mais une **fonction structurante**, portée par une méthode LegalOps exigeante et une vision globale de la conformité comme levier de valeur.

La conformité numérique, lorsqu'elle est pensée et organisée de manière stratégique, devient : un **facteur de confiance** pour les partenaires et les clients, un **actif immatériel valorisable**, un élément différenciant sur le marché, un outil de sécurisation durable de la croissance.

Le temps de la conformité subie est révolu. Celui de la conformité stratégique est ouvert. Le Digital Compliance Officer n'est pas une option. Il est désormais une fonction clé de la gouvernance numérique.

Merci d'avoir pris le temps de lire ce livre blanc.

Si vous avez des questions sur ce contenu, ou si vous souhaitez échanger sur ce sujet, n'hésitez pas à nous contacter

 20 rue du Cotentin, 75015 PARIS

 contact@nodal-avocats.com

 nodal-avocats.com