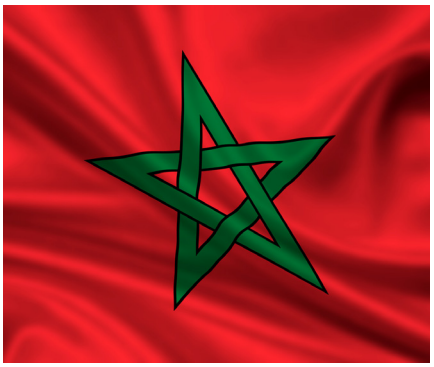
LIVRE BLANC


Données à caractère personnel :

Quels enjeux et comment se préparer à la loi 09-08 ?

AUSIM
Association des Utilisateurs des Systèmes d'Information au Maroc

solucom
management & IT consulting

Le mot de la CNDP

Depuis les recommandations de l'OCDE en 1980 jusqu'aux plus récentes conférences internationales sur le sujet, la protection de la vie privée tend à s'universaliser.

Dans le cadre des relations privilégiées qu'il entretient avec l'Europe, le Maroc a tenu, en adoptant la loi 09-08, à se mettre en conformité avec les standards internationaux de la protection des données à caractère personnel tels qu'ils ont été insérés dans le droit communautaire européen.

La Commission Nationale marocaine pour le contrôle de la Protection des Données à Caractère Personnel (CNDP) est ainsi instituée auprès du Chef du gouvernement. Elle est chargée de mettre en œuvre et de veiller au respect des dispositions de la loi et des textes pris pour son application, de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité de la personne, ni à la vie privée, ni aux libertés et droits fondamentaux de l'homme.

La mise en œuvre de la loi a rencontré un certain nombre de difficultés matérielles, difficultés liées à l'engagement des ressources financières, mais aussi difficultés concernant le recrutement des ressources humaines. Malgré ces handicaps, qui ne sont pas tous surmontés, la CNDP a entamé le traitement de ses premiers dossiers (demandes d'autorisation, traitement de plaintes, et demandes d'avis du gouvernement). Un premier travail de sensibilisation a eu lieu avec les principaux opérateurs téléphoniques et économiques.

L'ensemble des actions déjà menées lui ont d'ores et déjà permis d'obtenir une reconnaissance internationale puisqu'à travers elle, le Maroc est devenu le premier pays africain, arabe et musulman à être accrédité auprès de la Conférence Internationale des Autorités de Contrôle des Données Personnelles.

La CNDP souhaite aujourd'hui développer sa capacité à assurer une protection effective des données personnelles, confortée en cela par l'article 24 de la nouvelle Constitution, qui garantit le droit à la vie privée et le secret des communications.

De ce fait, l'action de la Commission portera sur les quatre grands domaines suivants :

- La sensibilisation des personnes concernées et du public.
- La célérité dans le traitement des plaintes.
- La qualité et l'efficacité des contrôles.
- Le renforcement des relations de confiance entre la CNDP, les responsables de traitements et les personnes concernées.

C'est ce programme que la CNDP est en mesure de rendre effectif à partir du début 2012. Aucun obstacle ne saurait entamer l'inébranlable volonté de la CNDP d'assurer une protection suffisante et satisfaisante des données personnelles au Maroc.

Saïd Ihraï

Président de la CNDP

Le mot de l'AUSIM

La société du savoir se définit comme une continuité de la société de l'information. Elle représente la condition *sine qua non* pour le développement d'une nation. Constituant de véritables leviers de développement économique et humain, les technologies de l'information y jouent un rôle central et déterminant. Dans ce cadre, l'ambition du Maroc est claire : s'élever au rang mondial qui devrait être le sien, en s'appuyant sur les technologies de l'information (TI).

Ainsi, pour les années à venir, l'enjeu est non seulement de pérenniser les avancées déjà réalisées, mais surtout de permettre une intégration amplifiée et largement diffusée des TI au niveau de l'ensemble des acteurs de la société : État, administrations, entreprises et citoyens.

Pour ce faire, l'instauration d'une stratégie de confiance numérique s'avère fondamentale et devrait assurer au mieux la protection de la vie privée des citoyens. L'actualité mondiale récente l'atteste : il s'agit d'une préoccupation croissante à la fois pour le citoyen, qui entend bénéficier pleinement du potentiel des nouvelles technologies tout en en maîtrisant les usages, et pour les investisseurs, aussi bien privés qu'étatiques, qui n'hésitent plus à en faire une condition décisive avant tout engagement de capitaux.

C'est un défi que le Royaume entend aujourd'hui relever, en se dotant de la loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Tous les organismes marocains doivent à présent s'y conformer.

Nous le savons : ces nouvelles exigences suscitent de nombreuses interrogations quant à leur champ d'application, leurs implications concrètes, ou encore la démarche à adopter pour y répondre.

En tant que promoteur de l'usage des technologies de l'information au Maroc et dans le cadre de ses missions d'animation du partage de connaissances entre ses membres, l'AUSIM, l'Association des Utilisateurs des Systèmes d'Information au Maroc, souhaite s'engager fortement aux côtés des organismes marocains sur ce sujet.

Ainsi, l'AUSIM a associé à ses efforts Solucom, cabinet de conseil en management & IT, qui dispose de retours d'expériences riches en matière de mise en conformité, acquis auprès de grandes organisations françaises et internationales soumises à des législations équivalentes.

C'est cette combinaison de l'expérience terrain de Solucom et de l'appréhension par l'AUSIM des préoccupations et des contraintes des organisations marocaines, enrichie d'échanges fructueux avec plus d'une dizaine de ses membres, qui nous permet aujourd'hui de vous présenter ce livre blanc, qui se veut un guide pratique pour la mise en conformité.

Nous espérons que les pistes que nous y développons vous seront précieuses et viendront enrichir et éclairer vos réflexions dans ce sens.

Très bonne lecture à tous.

Mohamed Bennis
Président de l'AUSIM

La loi 09-08, un enjeu clé pour une mise en œuvre complexe

Fruit d'une réflexion qui fait écho à celles déjà menées en Europe, la loi 09-08 permet au législateur marocain de répondre aux préoccupations croissantes du citoyen en encadrant la hausse rapide de l'usage des technologies de l'information tout en encourageant l'afflux de capitaux internationaux.

UN RICHE HÉRITAGE MONDIAL

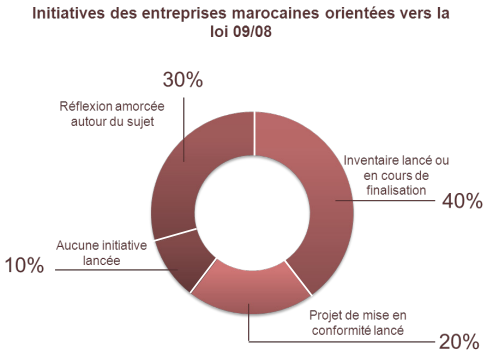
En 1978, et pour la première fois en Europe, la France se dote d'une loi visant à protéger les individus des traitements de données les concernant. Il s'agit alors de répondre aux inquiétudes des citoyens vis-à-vis des fichiers mis en œuvre par l'État.

Petit à petit, les enjeux évoluent, et c'est pour faire face à l'informatisation des entreprises, à la dématérialisation de l'information, aux prémices d'internet et aux soubresauts du télémarketing que l'Europe publie en 1995 une Directive dans le même sens. Celle-ci est aujourd'hui transcrite au sein du droit national de l'ensemble des pays membres de l'Union Européenne.

L'une des premières conséquences en est l'encadrement drastique des flux internationaux de données, à tel point qu'aux États-Unis, l'État fédéral est bientôt forcé de s'adapter en définissant et en mettant en place les mécanismes du *Safe Harbor*. L'objectif de cette certification, qui permet aux entreprises américaines d'attester de leur conformité à la Direction européenne, est de faciliter la collaboration économique avec l'Europe.

En 2008, le législateur marocain se saisit du sujet. Promulguée le 18 février 2009, la loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel vient témoigner d'une réflexion dans la droite lignée de ses prédécesseurs européens.

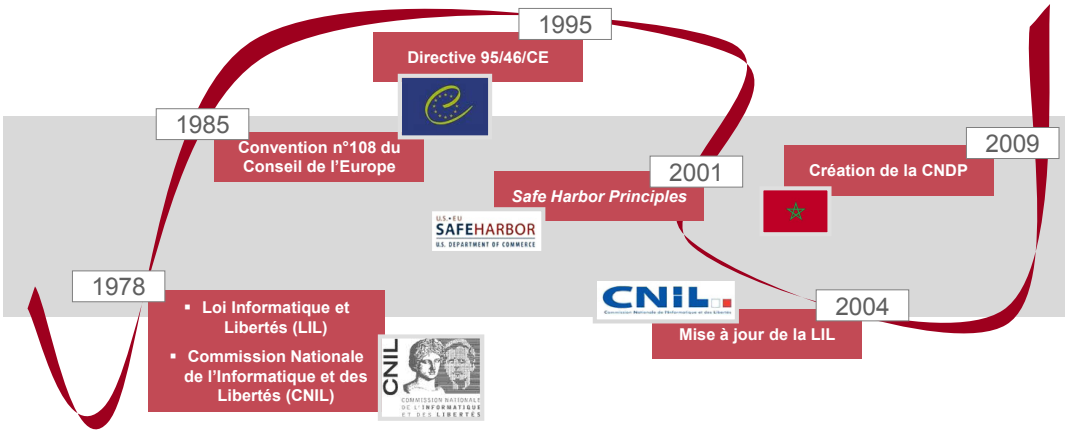
Initiatives des entreprises marocaines orientées vers la loi 09-08



UNE RÉPONSE CLÉ À DES ENJEUX NATIONAUX COMPLEXES

Il s'agit bien, pour le Royaume, de répondre en même temps à l'ensemble de ces mêmes enjeux accentués par *Maroc Numeric 2013*, ambitieux programme de développement des technologies de l'information.

Chronologie de la naissance de la loi



L'objectif est ainsi à la fois :

- De protéger le citoyen face à des pratiques, pour certaines déjà existantes (télémarketing, etc.) et qui risquent de se développer en même temps que l'usage de ces TI.
- D'augmenter le niveau de confiance des partenaires internationaux, en particulier européens, afin de faciliter l'afflux d'investissements étrangers et le transfert de services sur le territoire marocain.

Quels délais de mise en oeuvre ?

La mise en conformité à la loi 09-08 nécessite de prendre en compte l'ensemble du cycle de vie des données à caractère personnel et de l'analyser selon des axes variés. C'est donc un processus long et complexe, qu'il ne faut pas sous-estimer, puisqu'il peut nécessiter de 2 à 3 ans d'effort pour les plus grands comptes.

Pour autant, il existe aujourd'hui chez de nombreux organismes de véritables poches d'excellence : modélisation des processus, culture conformité, centralisation et urbanisation du SI, pratiques de sécurité à l'état de l'art, certifications ISO, gestion proactive de la relation client, etc. Celles-ci permettent a minima d'accélérer le processus, si ce n'est de s'en dispenser en grande partie.

UNE MISE EN CONFORMITÉ DES ENTREPRISES COMPLEXE MAIS INÉVITABLE

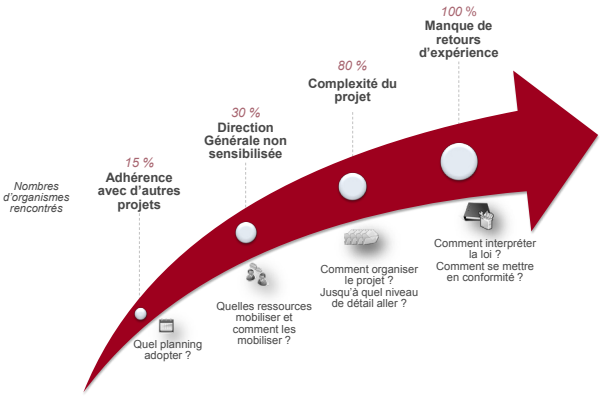
Depuis sa promulgation, la loi 09-08 est applicable.

Ainsi, tout nouveau traitement doit être conforme dès sa mise en œuvre. Les organismes marocains disposent en revanche d'un délai de deux ans pour mettre en conformité l'ensemble des traitements mis en place avant 2009.

Les difficultés pratiques soulevées par ce constat sont néanmoins nombreuses. Les principales sont dues à des différences de lecture de ce délai par les experts qui en fixent l'échéance entre mars et novembre 2012.

Quoiqu'il en soit, et malgré les nombreuses interrogations qui demeurent au sujet de ce texte, faute de retours d'expérience marocains, le mouvement vers la conformité est aujourd'hui réellement enclenché et ne pourra que s'accélérer d'ici fin 2012.

Les freins classiques à la mise en conformité



Les membres de l'AUSIM ont pu faire part de leurs principales difficultés concernant la mise en conformité à la loi 09-08.

Parmi celles-ci, on retrouve les freins classiques à un projet d'une telle ampleur : la complexité intrinsèque du projet ou celle de l'organisme, une impulsion insuffisante de la part de la Direction générale, ou encore des dépendances fortes avec d'autres projets en cours rendant difficile la prise de décision à court terme (refonte ou urbanisation du SI, programme « 0 papier », réorganisation, réflexion sur la relation client, etc.).

Toutes les difficultés se cristallisent cependant sur le manque de retours d'expérience concrets sur la mise en application de cette loi.

Le travail effectué par différentes associations et groupements professionnels encourageant le partage de bonnes pratiques et la mise en commun d'éléments de réflexion, tout comme les nombreux exemples européens, et notamment français, sont riches d'enseignements. Les entreprises regrettent néanmoins une communication qu'elles jugent aujourd'hui insuffisante au regard des enjeux que porte pour elles un tel projet.

Que dit la loi ?

La loi 09-08 encadre la mise en œuvre de traitements des données à caractère personnel. Si les exigences qu'elle introduit apparaissent en première lecture aussi précises que fortes, ces deux notions cœur que sont les données et les traitements appellent une explication de texte, tant leur périmètre d'application peut sembler large.

UN PÉRIMÈTRE D'APPLICATION LARGE...

L'une des premières sources de complexité de la loi 09-08 découle directement de l'étendue de son champ d'application.

Tout d'abord, la notion de données à caractère personnel recouvre un volume considérable d'informations. Le législateur la définit comme « toute information, de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image, concernant une personne physique identifiée ou identifiable, [c'est-à-dire] une personne qui peut être identifiée, directement ou indirectement ».

Autrement dit, et à titre d'exemple, un nom qui apparaît sur un fichier, un numéro de téléphone ou d'immatriculation sont des informations à caractère personnel. Bien plus, un regroupement d'informations, tel que l'association d'une date de naissance à une commune, ou même une information qui, seule, ne permettrait pas d'identifier une personne (une liste de centres d'intérêts, la participation ou non à un groupement professionnel) sont également considérés par la loi comme des données à caractère personnel.

Par conséquent, il est clair que la grande majorité des informations manipulées par une entreprise sont bien des données à caractère personnel. Cette notion de donnée à caractère personnel s'éclaire lorsqu'on la met en regard de celle de *traitement*, dont la définition recouvre également une large variété de situations.

C'est bien ce *traitement* qui est au cœur de la loi, soit toute manipulation de données, quels que soient sa nature et son mode de réalisation (manuel, partiellement ou totalement informatisé) : inscription sur un registre papier, stockage, comparaison visuelle, utilisation par une ou plusieurs applications informatiques, etc. La loi ne s'applique toutefois pas à certains traitements relatifs à la défense nationale, la sûreté intérieure et extérieure de l'État et à la justice.

Par exemple, un registre des visiteurs, une application informatique, un ensemble d'applications ou de modules traitant des données à caractère personnel, les mécanismes de contrôle d'accès SI ou aux bâtiments, un dispositif de vidéosurveillance ou de traçabilité peuvent, au sens de la loi 09-08, constituer un traitement de données à caractère personnel.

A contrario, les données concernant des personnes morales, à condition toutefois de ne pas être associées à des contacts physiques, ne sont pas concernées.

Par ailleurs, il convient de ne pas faire de confusion entre cette notion de données à caractère personnel et celles :

- D'informations *privées*, par opposition à *professionnelles*, que les collaborateurs d'une entreprise peuvent être amenés à manipuler via leur outil de travail.
- De données *individuelles*, par opposition aux informations *collectives*, partagées entre plusieurs collaborateurs d'une même entreprise.

Des données et traitements particulièrement sensibles

Au sein de l'ensemble extrêmement large des données et traitements de données à caractère personnel, la loi en distingue de particulièrement sensibles, relatives :

- Aux origines raciales ou ethniques.
- Aux opinions politiques, convictions religieuses ou philosophiques, ou l'appartenance syndicale.
- À la santé et aux caractéristiques génétiques.

Les traitements sensibles sont quant à eux :

- Ceux manipulant des données collectées à d'autres fins que le traitement lui-même.
- Ceux s'appuyant sur le numéro de la carte d'identité nationale.
- Ceux portant sur les infractions, condamnations ou mesures de sûreté.
- Ceux consistant en une interconnexion ou le croisement, technique ou manuel, de fichiers aux finalités différentes.

…SUR LEQUEL S'IMPOSENT DES EXIGENCES FORTES ET PRÉCISES…

La loi 09-08 encadre ces *traitements de données à caractère personnel*, en posant trois principes clés que sont la finalité, la proportionnalité et la loyauté. De ces principes découlent des exigences précises.

Tout d'abord, un traitement doit avoir une finalité clairement définie et une durée de mise en œuvre limitée, fonction de cette finalité. De la même façon, les données manipulées doivent être proportionnelles à cette finalité. Cette

dernière conditionne également les mesures de sécurité qu'il convient de mettre en place afin d'assurer la confidentialité et l'exactitude (intégrité) des données manipulées. Ces différents éléments doivent faire l'objet de formalités déclaratives auprès de l'organisme approprié.

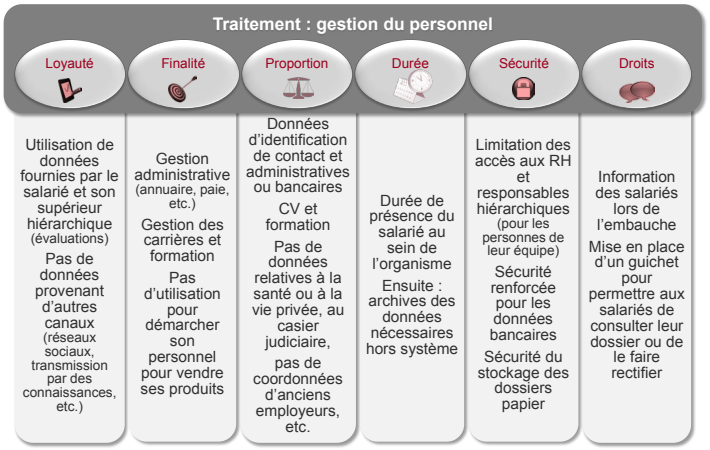
Un *responsable de traitement*, garant de la conformité, est d'ailleurs désigné pour chaque traitement.

Celui-ci devra s'assurer que les données soient collectées loyalement, c'est-à-dire que les personnes soient bien informées de la mise en œuvre d'un traitement concernant leurs données et que leurs droits soient respectés : le *droit d'accès*, c'est-à-dire le droit de se faire communiquer, à tout moment, les données dont dispose un organisme à leur sujet, le droit de s'opposer à ce que leurs données soient utilisées, et le droit de rectification et de suppression de ces données.

Première implication marquante : ces différentes dispositions interdisent dorénavant explicitement la prospection directe par tout autre moyen que le courrier électronique, dont l'usage est lui-même strictement encadré.

Afin de garantir la transcription concrète de l'ensemble de ces dispositions dans les pratiques des entreprises, la loi institue une Commission Nationale de contrôle de la protection des Données à caractère Personnel (CNDP – voir encadré ci-dessous) qui veille à la protection des données personnelles sur le territoire marocain.

Exemple : les exigences de la loi 09-08 appliquées à la gestion du personnel



La Commission Nationale de contrôle de la protection des Données à caractère Personnel (CNDP)

Afin d'assurer le respect de la loi 09-08, le Maroc s'est doté d'une Commission Nationale de contrôle de la protection des Données à caractère Personnel (CNDP).

Véritable régulateur des données à caractère personnel, la CNDP remplit des missions multiples :

- L'information et la communication auprès des entreprises et du grand public.
- L'organisation des modalités de déclaration des traitements et le recensement de l'ensemble des traitements.
- La proposition de projets réglementaires au gouvernement ou au parlement ou le conseil sur tout traitement mis en œuvre par le gouvernement.
- Le contrôle du bon respect de la loi.

La CNDP peut ainsi contrôler les organismes marocains et enquêter sur des plaintes qui peuvent lui être adressées directement par le citoyen. Elle peut alors ordonner des modifications de traitements ou la destruction de données ou encore saisir le Procureur du Roi.

La CNDP est composée de sept membres nommés par le Roi, qui s'appuient dans l'exercice de leurs fonctions sur des fonctionnaires, agents et techniciens spécialisés.

À titre de comparaison, son homologue français, la CNIL, comprend 17 membres et environ 170 agents.

Contact : 6 boulevard An-Nakhil, immeuble Les patios
Hay Ryad, 10 000 Rabat
Tél : +212 (0) 537 571 124 Fax : +212 (0) 537 572 141
Mail : contact@cndp.ma Site internet : www.cndp.ma

Pourquoi et comment se mettre en conformité ?

Si la loi prévoit des sanctions lourdes, ces dernières ne doivent pas être l'unique moteur pour la mise en conformité. Bien au contraire, dans bien des cas, d'autres enjeux liés à la conformité peuvent être prédominants.

UN LARGE ÉVENTAIL DE SANCTIONS

Le législateur a prévu un éventail large de sanctions en cas de non-respect de la loi : 15 articles du texte de loi y sont même consacrés.

Dans un premier temps, la CNDP peut elle-même interdire la mise en œuvre ou le maintien d'un traitement, sa modification ou la suppression des données manipulées.

La voie pénale ensuite, par l'intermédiaire du Procureur du Roi que la CNDP peut saisir, permet de prononcer des sanctions allant jusqu'à une amende de 300 000 DH et une peine de 2 ans d'emprisonnement. Ces condamnations peuvent être doublées en cas de récidive. À ceci peuvent enfin s'ajouter des dommages et intérêts en cas de plainte des personnes concernées.

DES ENJEUX ANNEXES

Avec la sanction pénale ou la poursuite civile vient l'impact d'image.

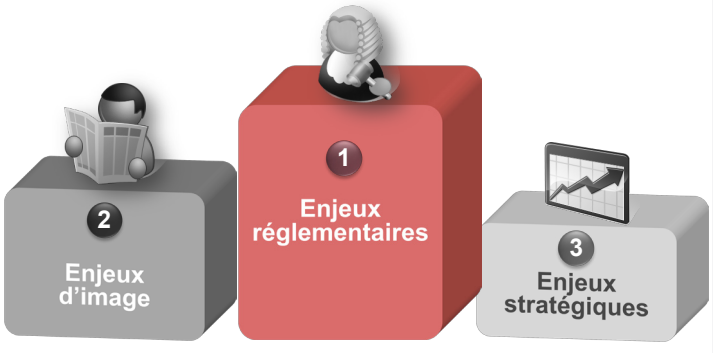
Si aujourd'hui le niveau de maturité du citoyen en matière de protection des données à caractère personnel est assez disparate en fonction du profil de clientèle de chaque entreprise, l'expérience internationale montre que les attentes croissent exponentiellement à mesure que les organismes se mettent en conformité.

D'ores et déjà, l'exemplarité en la matière s'impose à un certain nombre d'acteurs, pour qui l'enjeu d'image, vis-à-vis de l'externe comme de l'interne, est double. Il s'agit à la fois d'éviter toute atteinte critique à la réputation en cas de non-conformité, mais également de transformer, avant la concurrence, la conformité en un véritable levier de gestion de l'image.

Parmi les autres enjeux possibles, citons également les enjeux stratégiques, particulièrement prégnants pour les organismes dont la manipulation de données à caractère personnel est le cœur de métier : télémarketing, centres d'appel, tierce maintenance applicative, sous-traitance métier, etc.

Enfin, rappelons l'un des objectifs affichés de la loi : il est fort à parier qu'être conforme à la loi 09-08, et être à même de le démontrer, constituera bientôt une condition indispensable pour toute entreprise souhaitant accéder aux données d'une entreprise européenne, que ce soit dans le cadre d'un accord commercial ou d'une sous-traitance.

Principaux enjeux relatifs à la mise en conformité selon les entreprises marocaines sondées



LES CINQ PILIERS DE LA CONFORMITÉ

L'expérience permet de mettre en évidence les cinq écueils classiques de la mise en conformité à une telle législation. À ceux-ci correspondent les cinq piliers suivants, sur lesquels il conviendra de bâtir une démarche pragmatique et adaptée à l'organisme.

Pilier n°1 : « La notion de traitement est la clé de voûte de la conformité »

Le premier obstacle est la méthodologie elle-même. Si l'inventaire exhaustif des données peut s'avérer un outil précieux pour la mise en œuvre de mesures de sécurité, il s'agit bien souvent d'une fausse piste pour la mise en conformité.

Ainsi, après avoir mobilisé une équipe pendant une durée non négligeable, bien des entreprises se trouvent dans l'incapacité d'utiliser cet inventaire pour lancer les travaux de mise en conformité : catalyseur indéniable, l'inventaire des données pris trop tôt ne fait souvent que retarder la véritable mise en conformité.

Les plans d'actions pratiques s'imposent en revanche généralement d'eux-mêmes lorsqu'une approche *top-down*, du traitement à la donnée, est mise en place.

Exemple de démarche de mise en conformité intégrant les cinq piliers

Pilier n°2 : « Viser une conformité totale immédiate est contre-productif »

L'ambition d'inventorier toutes les données est bien souvent le symptôme du travers qui consiste à considérer la conformité comme un bloc uniforme d'exigences.

Les entreprises parcourant le plus facilement et le plus rapidement leur chemin vers la conformité sont ainsi celles qui ont su hiérarchiser les traitements et les exigences, et de ce fait initier un véritable cercle vertueux de la conformité.

Au contraire, les organismes visant une conformité totale immédiate gaspillent généralement un temps précieux et aboutissent souvent à une démobilisation irrémédiable des ressources sur le sujet.

Pilier n°3 : « Il ne s'agit pas d'un projet informatico-informatique »

Une approche *top-down* et clairement priorisée ne permet toutefois d'atteindre la conformité qu'à la condition que les bons interlocuteurs soient mobilisés.

Il convient en effet de conserver constamment à l'esprit les idées clés suivantes : un traitement de données à caractère personnel n'est pas un traitement au sens informatique du terme. Les métiers sont les seuls à même de connaître précisément les pratiques mises en œuvre, les besoins et les contraintes terrain sous-jacentes. La mise en conformité nécessite ainsi la mobilisation d'expertises métiers, mais également SI, sécurité et juridique. *In fine*, c'est l'entreprise dans son ensemble, en tant que personne morale, qui est légalement responsable de la conformité.

Pilier n°4 : « La déclaration à la CNDP n'est jamais que la partie émergée de l'iceberg »

L'analyse des sanctions prononcées dans les pays disposant de législations comparables permet de compléter ce panorama par deux erreurs fréquentes.

La première consiste à limiter la mise en conformité à ces formalités déclaratives. Bien au contraire, l'essentiel des efforts doit être porté sur les autres exigences de la loi, principalement l'information et le respect des droits des personnes, l'application du principe de proportionnalité et la sécurité des données.

Le relâchement des efforts une fois un premier niveau de conformité atteint constitue la seconde erreur.

Pilier n°5 : « La conformité doit être une manière de travailler »

Les efforts doivent en effet être maintenus dans le temps, afin d'éviter la dérive naturelle du niveau de conformité, due aux évolutions des activités, des pratiques ou des systèmes d'information.

Pour cette raison, un *projet* de mise en conformité ne peut être considéré comme un projet comme un autre, pour lequel l'attention peut être totalement relâchée une fois la cible atteinte. De nombreux organismes l'ayant oublié n'ont pu éviter une sanction qu'au prix d'efforts démesurés de remise en conformité.

« Il conviendra de bâtir une démarche pragmatique et adaptée à l'organisme. »

Pilier n°1 - Adopter une démarche centrée sur le traitement

L'intitulé de la loi 09-08 est explicite : il met en évidence sa vocation à poser un cadre pour les traitements de données à caractère personnel. C'est d'ailleurs bien la notion de « finalité » d'un traitement qui est mise en avant par le législateur et qui conditionne l'ensemble des mesures à mettre en place. Le concept de « traitement » est ainsi bien à placer au cœur de la réflexion.

OUBLIER LA DONNÉE DERRIÈRE LE TRAITEMENT

La grande majorité des données manipulées au sein d'une entreprise sont des données à caractère personnel. Une même donnée peut d'ailleurs être utilisée au sein de traitements différents. C'est le cas par exemple des données sur les collaborateurs qui peuvent être utilisées à la fois pour gérer la paie, les accès aux outils informatiques, les avantages offerts aux salariés sur les produits de l'entreprise ou encore les activités organisées par le comité d'entreprise.

De plus, une même donnée peut être ou ne pas être une donnée à caractère personnel, en fonction du traitement pour lequel elle est utilisée, et ceci selon qu'elle désigne ou non une personne physique. À titre d'exemple, la référence d'un produit devient une donnée à caractère personnel dès lors qu'il s'agit d'analyser les achats d'un client à des fins marketing.

Ainsi, au sens de la loi 09-08, les données ne sont considérées comme étant à caractère personnel que par rapport à un traitement. Leur niveau de sensibilité découle par conséquent de la finalité de ce dernier.

Leur manipulation pourra ainsi être licite ou illicite selon le contexte et la finalité du traitement associé.

Ainsi, l'utilisation des données relatives aux handicaps des collaborateurs par les services de ressources humaines est considérée comme licite et légitime s'il s'agit d'aménager le temps de travail ou les positions de travail. Il n'en sera bien entendu pas de même dans le cas de l'utilisation de ces mêmes données à des fins discriminatoires.

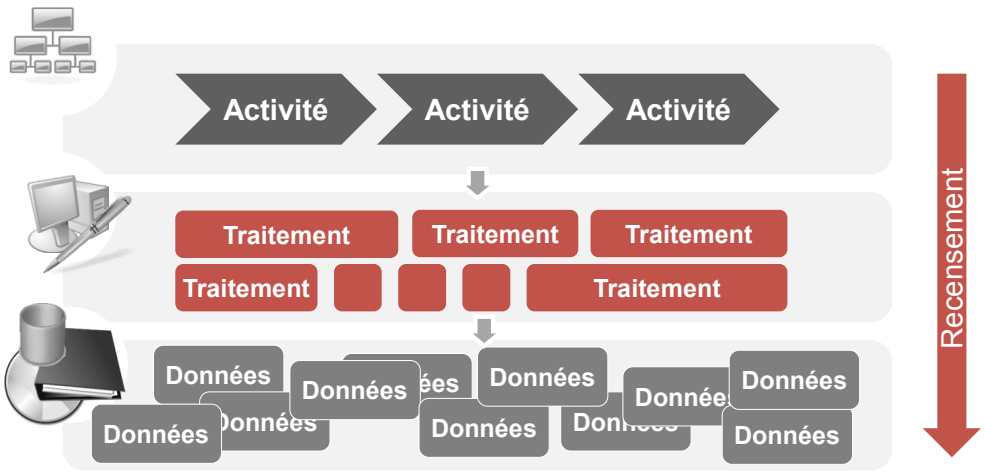
Ainsi, outre sa conformité à l'esprit de la loi, une démarche orientée « traitement » et non « données » permet de faciliter les différentes étapes du processus de mise conformité :

- Le recensement des traitements et données est facilité : sauf à disposer d'une cartographie précise et à jour de l'intégralité du SI et des traitements manuels, une approche *top-down*, prenant les activités métiers comme point de départ, permet très naturellement d'identifier les traitements et données concernées, avec un risque d'oubli minimal.

- La sécurisation des données est rendue possible de bout en bout grâce à l'identification des pratiques, des flux fonctionnels, des différents canaux et outils et des contraintes métiers associées.

- La gestion du changement, enfin, s'effectue naturellement : les différents acteurs étant responsabilisés quant à manipulation de données dans le cadre de leurs propres activités quotidiennes.

Une démarche centrée sur le traitement



Exemple d'inventaire

Traitement	Responsable	Finalités	Resp. mise en œuvre	Applications	Déclaration (existante)	Responsable du droit d'accès
Gestion des ressources humaines	DRH	Gestion de la paie	DSI Groupe	XXX	Déclaration / autorisation N° de déclaration Date du récépissé	XXX
		Suivi des formations	RH filiale	N/A		XXX
		Suivi du recrutement (sourcing, CV, etc.)	Prestataires	XXX		XXX
		Gestion des carrières	RH filiale	XXX		XXX
		Gestion administrative	DSI Groupe	XXX		XXX

Domaine	Exemples de traitement de données à caractère personnel
Activités métier	Gestion des fichiers clients, produits, gestion commerciale
RH	Gestion du personnel, organisation du travail, rémunération, annuaires papier
	Recrutement, suivi des accidents de travail
Achats	Gestion des achats et de la relation avec les fournisseurs
Services généraux	Contrôle de l'accès physique aux locaux et vidéosurveillance, liste des visiteurs
Outils du Système d'Information	Outils de travail bureautiques (postes de travail, messagerie, etc.) et téléphonie
	Supervision et gestion des traces
	Enregistrement des communications en centre d'appel
Administration et finance	Finance, contrôle de gestion, comptabilité générale
Communication	Communication interne et externe (site Internet, newsletters, etc.)

INVENTORIER LES TRAITEMENTS : UNE ÉTAPE LONGUE ET INDISPENSABLE

La démarche de mise en conformité débute par l'inventaire des traitements de données à caractère personnel : il s'agit alors d'identifier aussi bien les traitements purement métiers que les traitements mis en œuvre par les fonctions support tels que les traitements SI, gestion RH, etc.

Cette étape d'inventaire ne doit pas être sous-estimée : certes longue, elle est absolument clé pour la suite du projet. Son succès conditionne le bon déroulement de la suite des travaux.

Il est donc indispensable de définir et de mettre en œuvre une méthodologie pragmatique et applicable, adaptée à l'organisme.

Cela se traduit généralement par la mise en place d'une démarche et d'un outillage simple qui s'appuient autant que possible sur l'existant, en termes d'organisation, d'outils de *workflow*, de culture d'entreprise ou de documentation (processus décrits, référentiels d'urbanisation du SI, etc.).

Par ailleurs, la réalisation de l'inventaire est l'occasion d'examiner chaque traitement. Au-delà de l'élaboration d'une simple liste, il convient donc de profiter de cette étape pour anticiper et préparer la mise en conformité, en consignant de manière claire et exploitable l'ensemble des informations qui seront par la suite indispensables à la mise en conformité.

L'inventaire ainsi constitué peut alors contenir, pour chaque traitement, sa ou ses finalité(s), sa maîtrise d'ouvrage et sa maîtrise d'œuvre, ses modalités de mise en œuvre (traitement manuel ou application(s) informatique(s)), les données manipulées, les modalités d'exercice des droits des personnes etc.

L'organisme dispose alors d'un outil précieux pour assurer son maintien en conformité dans le temps : en le complétant et le maintenant à jour, il se met en position non seulement de piloter le projet de mise en conformité initiale mais également et surtout de maîtriser à chaque instant et sur le long terme son niveau de conformité.

« Les données ne sont *à caractère personnel* que par rapport à un traitement. »

Pilier n°2 - Prioriser en fonction du risque juridique

Bien des organismes se heurtent à la difficulté de concilier de manière abordable la volumétrie écrasante des traitements et le nombre important d'exigences de la loi. On l'a vu, les bonnes pratiques consistent à mettre en œuvre une démarche pragmatique, consistant à traiter en priorité les risques majeurs de non-conformité et à initier ainsi un cercle vertueux permettant de s'améliorer de façon continue.

PRIORISER POUR ÉLEVER PROGRESSIVEMENT LE NIVEAU DE CONFORMITÉ

Il peut être tentant de cibler une conformité totale et immédiate. Or, particulièrement dans un contexte où tout n'est pas maîtrisable (comment gérer les fichiers constitués par les collaborateurs sur leur poste de travail ? comment contrôler l'ensemble des projets ?) et où il appartient aux entreprises de se familiariser avec les concepts d'une loi pour laquelle il n'existe ni retours d'expérience ni jurisprudence, un tel objectif s'avère inutilement ambitieux voire contre-productif.

Il s'agit alors de prioriser les travaux : les efforts doivent être organisés de façon à être proportionnels aux enjeux.

Les risques majeurs de non-conformité sont ainsi traités en priorité, le niveau de risque acceptable étant par la suite progressivement abaissé. La faisabilité des actions doit également être prise en compte, ce qui peut nécessiter de faire des arbitrages.

Il revient ainsi à chaque organisme de s'interroger sur ses propres enjeux, ses moyens disponibles et son niveau de tolérance aux non-conformités. C'est en effet à chacun de fixer ses critères de priorisation en fonction de son domaine d'activité, de son climat social, de sa culture, de ses pratiques, etc.

À titre d'illustration, il peut être intéressant de prioriser en fonction du risque d'atteinte à la vie privée des personnes ou du risque de plainte. Le premier de ces risques se traite en considérant les traitements manipulant des données *sensibles* au sens de la loi. Le second considère les traitements fortement exposés. Ainsi, une entreprise traitant directement avec le grand public sera attentive à sa relation client, tandis qu'une entreprise soucieuse de préserver son climat social se penchera en priorité sur ses traitements liés à la gestion du personnel et de l'outil informatique.

Cette notion de priorisation doit ensuite être mise en application à chaque étape de la démarche.

Dès l'étape d'inventaire, elle doit permettre de fixer le cadre dans lequel les travaux s'organisent : il n'est pas réaliste de vouloir tout inventorier, sauf à mettre en œuvre un projet excessivement consommateur (en temps et en ressources) et continu dans le temps.

Lors de la mise en œuvre du plan d'actions de mise en conformité lui-même, on se concentrera ensuite en premier lieu sur les traitements les plus sensibles (au sens de la loi ou sur des enjeux spécifiques de l'organisme) voire les plus exposés.

Enfin, dans la phase de maintien de la conformité, l'attention sera portée en priorité sur les périmètres (entité organisationnelle, de taille de projet...) les plus porteurs d'enjeux.

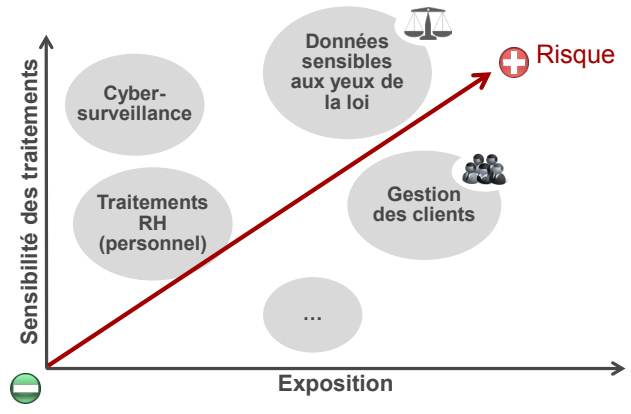
LANCER SANS ATTENDRE LES PREMIERS CHANTIERS

La réflexion sur la priorisation, ainsi que la démarche d'inventaire décrite précédemment, ne doivent en aucun cas retarder la mise en œuvre des premières actions.

Les délais sont courts et il y a fort à parier que pour de nombreux organismes, la mise en conformité ne pourra se faire qu'au prix de chantiers, généralement transverses, bien souvent identifiables dès les balbutiements du projet lui-même. Ceux-ci doivent être lancés rapidement.

Il s'agit tout d'abord d'instaurer ou de consolider un niveau acceptable de sécurité de l'information, matérialisé par une politique de sécurité formalisée. Il apparaît en particulier indispensable que l'organisme se soit doté des moyens nécessaires à une lutte antivirale efficace, à une bonne protection de son réseau et de ses postes de

Priorisation des traitements selon leur sensibilité et leur exposition



travail, mais aussi à un contrôle effectif des accès aux ressources informatiques et à l'ensemble des bâtiments où de l'information est manipulée.

La conduite d'une analyse des risques de sécurité permet ensuite d'identifier les axes de travail prioritaires. Les normes internationales en matière de protection de l'information, notamment l'ISO 27001 et 27002, sans être indispensables, fournissent néanmoins pour cela une aide précieuse, dès lors qu'elles sont utilisées avec pragmatisme.

En parallèle, il est bien souvent incontournable de s'interroger sur ces pratiques en matière de gestion des sous-traitants et fournisseurs. La responsabilité pénale ne peut en effet se déléguer et la loi 09-08 elle-même insiste sur ce point. Elle requiert ainsi explicitement que toute sous-traitance soit encadrée par un acte juridique formel, incluant des exigences relatives à la protection des données à caractère personnel (en particulier le respect des finalités du traitement sous-traité) mais aussi la sécurité des données. Au-delà de la gestion purement contractuelle, un dispositif doit être mis en place pour s'assurer du respect de ces contrats dans le temps, notamment via des contrôles réguliers.

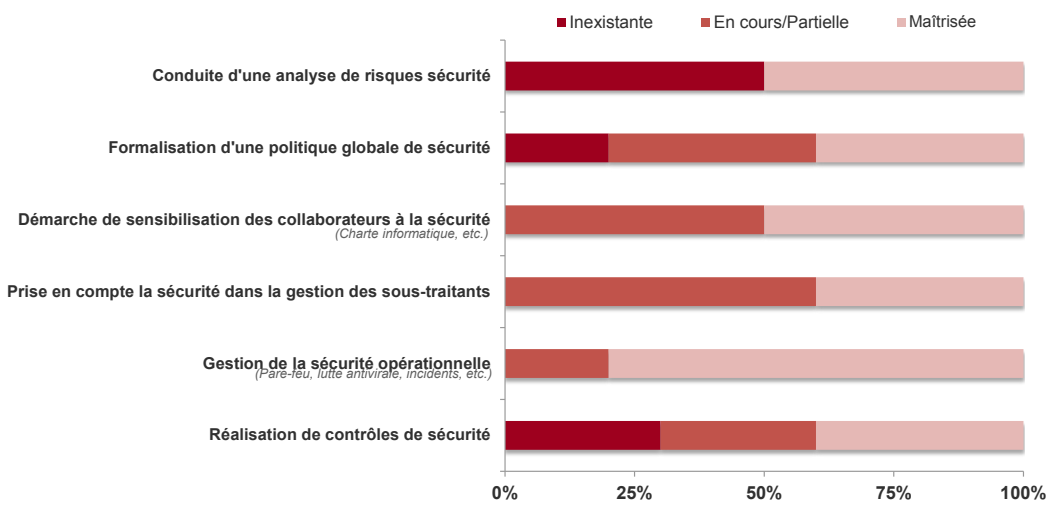
Ces chantiers permettent de poser les bases qui permettront de mettre les traitements en conformité. Plus encore, ils constituent une protection précieuse de l'entreprise, la loi 09-08 ne constituant alors qu'une opportunité d'élever, si nécessaire, le niveau global de sécurité au niveau des standards internationaux.

L'apport d'un lancement rapide de ces premiers chantiers ne se limite pas à l'optimisation des plannings et au lissage dans le temps des ressources. Cela permet également d'assurer l'adhésion de chacun en mettant en place une démarche globale et cohérente, un véritable projet d'entreprise, dont les gains sont appréhensibles par tous.

L'aspect « visibilité » doit ainsi être particulièrement étudié. En ce sens, à titre d'exception au principe de priorisation, il convient d'identifier des actions rapides et peu coûteuses, y compris si elles n'apportent que peu de choses en matière de conformité. Cela facilitera la mobilisation future des différents acteurs de l'entreprise : distribution de clés USB chiffrées, utilisation d'enveloppes scellées pour certaines communications internes, etc.

« Cibler une conformité totale et immédiate s'avère inutilement ambitieux voire contre-productif. »

Niveau de maturité en termes de sécurité au sein des entreprises marocaines sondées



Pilier n°3 - S'appuyer sur les bons acteurs

Parmi les grands chantiers à lancer rapidement, résident la définition et la mise en place d'une organisation adaptée. Cette réflexion, prérequis incontournable, doit être menée dans tous les organismes, quels que soient leur mode de fonctionnement, leur niveau de maturité ou leurs objectifs en matière de conformité.

IMPLIQUER LES BONS ACTEURS, AU BON NIVEAU, POUR CONDUIRE LE PROJET DE MISE EN CONFORMITÉ…

Un balayage rapide des différentes exigences de la loi 09-08 suffit à nous renseigner sur le caractère nécessairement transverse d'un projet de mise en conformité.

Les juristes et les responsables conformité sont tout d'abord très naturellement sollicités et doivent l'être à plus d'un titre : en tant qu'experts légaux d'une part, mais aussi en tant que porteurs opérationnels d'actions de mise en conformité (revue des contrats, etc.). Leur association peut être également utilisée comme levier pour asseoir plus globalement la légitimité de l'ensemble de l'équipe projet.

Les responsables des systèmes d'information et de leur sécurité sont ensuite souvent chargés du pilotage du projet, la grande majorité des traitements étant informatisée.

L'expérience montre par ailleurs qu'une implication des métiers et fonctions support s'avère rapidement indispensable à la conduite des travaux, tant la connaissance des pratiques et contraintes terrain est nécessaire. Par ailleurs, ce sont bien eux qui manipulent quotidiennement les données à protéger et qui en ont, au préalable, défini les traitements.

Tout l'enjeu est donc de définir une organisation permettant d'exploiter au mieux les compétences disponibles.

Se posent alors les questions de la mise en œuvre concrète de cette pluridisciplinarité et du pilotage du projet. S'il existe une multitude de réponses possibles à ces questions, toutes doivent pouvoir se résumer en trois mots : légitimité, transversalité et visibilité.

… ET PERMETTRE LE MAINTIEN DANS LE TEMPS DU NIVEAU ATTEINT

Afin de maintenir le niveau de conformité atteint, les missions associées doivent perdurer également, en prolongement de l'organisation projet.

S'il est possible de ventiler ces missions au sein de l'organisation existante, la nomination d'un interlocuteur unique constitue généralement la solution optimale.

Véritable chef d'orchestre de la conformité, ce *correspondant* aura pour fonction de solliciter et de coordonner les expertises disponibles pour assurer la conformité sur le long terme. Sa présence facilitera de plus le respect des droits des personnes, la gestion de la relation avec la CNDP et plus généralement, la diffusion des bonnes pratiques au sein de l'organisme.

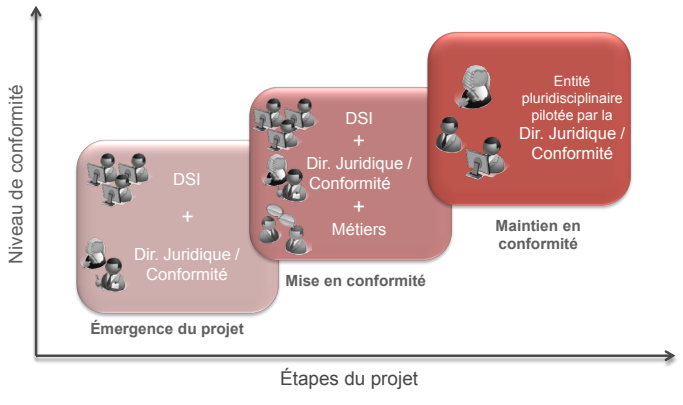
Nécessairement haut placé dans l'organigramme, afin d'avoir la légitimité et le poids suffisants pour lancer des actions transverses, il peut être épaulé par une équipe dimensionnée en fonction de la complexité du contexte et des ambitions en matière de conformité. Ce sont également les enjeux de l'organisme qui conditionneront les profils à mobiliser. Par exemple, on pourra solliciter des profils RH pour une entreprise BtoB, des profils sécurité pour une entreprise manipulant des données susceptibles d'attirer la convoitise (données bancaires notamment), des profils métier pour un groupe multi-métiers, ou encore des profils « conformité » pour une entreprise mettant en œuvre principalement des traitements sensibles, etc.

INSTAURER UNE VÉRITABLE CULTURE DE LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL POUR PROTÉGER L'ENTREPRISE

Les efforts de communication ne doivent pas se limiter aux participants directs du projet de mise en conformité.

Si la nécessité de convaincre la Direction générale et le top management dans son ensemble ne fait généralement pas débat, de nombreux organismes ont vu leurs efforts de conformité perdre considérablement en efficacité du fait d'une communication mal gérée auprès de l'ensemble de leurs collaborateurs.

Organisation pour conformité au sein des organismes sondés (tendance)



« On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre. […] »

Dahir formant code des obligations et des contrats, art. 85

Pour autant, il ne s'agit pas de s'adresser à chacun de manière indifférenciée : c'est un véritable plan de communication qui doit être bâti afin d'apporter le bon message, au bon moment, à la bonne personne, en s'appuyant sur les bons canaux (journal interne, réunions d'équipes, sessions de formation, etc.). En ce sens, les efforts de communication doivent accompagner et prolonger le projet de mise en conformité.

L'objectif, à terme, doit être d'instaurer au sein de l'organisme une véritable culture de la protection des données à caractère personnel, afin d'assurer le respect des règles par tous et de faciliter la remontée de l'information aux acteurs en charge de la conformité.

L'un des leviers incontournables de communication est la charte d'utilisation des SI, qui doit être juridiquement opposable aux collaborateurs.

Une entreprise peut en effet être tenue civilement responsable des actions de ses collaborateurs : elle peut ainsi être condamnée à verser des dommages et intérêts, par exemple en cas de revente de données à caractère personnel par un salarié - sauf à démontrer qu'elle interdit explicitement ce type de pratiques.

C'est bien là tout l'objet de ce document : outre la responsabilisation des collaborateurs, il garantit la protection juridique du responsable de traitement.

Qui est le responsable du traitement ?

La loi 09-08 définit le responsable de traitement comme étant *la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel*.

Deux critères sont ainsi clés pour identifier le responsable de traitement : la finalité et les moyens. Il s'agit donc de la personne ou de l'entité fixant les objectifs du traitement et ses grands principes de fonctionnement (quelles données, quelle durée, etc.). Dans le monde informatique, on parlera de maître d'ouvrage, par opposition au maître d'œuvre qui définit les caractéristiques techniques du traitement, sous la responsabilité du maître d'ouvrage.

La précision *personne* ou *entité* est ici essentielle. En effet, il convient de ne pas perdre de vue que le responsable de traitement est bien plus souvent une entreprise qu'une personne physique. C'est en ce sens que le dirigeant, en tant que représentant légal de l'entreprise, sera par défaut le *responsable de traitement*.

Cette responsabilité peut être déléguée à travers le mécanisme classique de délégation de pouvoir. Ainsi, en application directe de la définition de la loi, le DRH devient responsable de traitement pour les traitements RH, le directeur commercial responsable des traitements liés à la relation client, etc.

Il convient en effet de considérer cette notion de *responsable* non pas vis-à-vis d'un organisme dans son ensemble mais bien par rapport à chaque traitement : la loi ne s'oppose en aucun cas à ce qu'il y ait plusieurs « responsables de traitement » au sein de la même entreprise, chacun n'étant *in fine* qu'un représentant du véritable *responsable de traitement*, c'est-à-dire de l'entreprise elle-même, en tant que personne morale.

Pour autant, cette identification du *responsable de traitement* ne dédouane en aucun cas les autres acteurs du respect de la loi, pas plus qu'elle n'incrimine de manière automatique le représentant identifié en cas de non-respect.

Ainsi, les sanctions prises par les autorités en charge de la protection des données à caractère personnel en Europe le sont toujours contre un organisme, bien que physiquement adressées à l'un de ses représentants légaux : ce n'est pas lui, en tant qu'individu, mais bien l'organisme qui est mis en cause.

En revanche, la responsabilité pénale peut porter aussi bien sur le *responsable du traitement* que sur n'importe quelle personne impliquée, morale ou physique. Ainsi, dans le cas de la revente de la base client par un salarié, c'est le salarié qui a été reconnu coupable de violation de protection des données à caractère personnel et condamné en son nom propre.

Bien qu'essentielle, la notion de *responsable de traitement* doit donc, dans la majorité des cas, être dédramatisée : l'identification d'un responsable plutôt qu'un autre au sein d'une entreprise n'influera pas sur les mesures à mettre en œuvre. Elle doit au contraire faciliter leur mise en place, en responsabilisant les maîtrises d'ouvrage.

En revanche, elle devient bien entendu cruciale dans des cas de sous-traitance ou de mise en œuvre conjointe d'un traitement par différents organismes, la loi ne reconnaissant pas, à ce jour, la *coresponsabilité*.

Pilier n°4 - Traiter la conformité dans sa globalité

Le lancement des grands chantiers transverses aura permis de poser des bases solides, l'inventaire priorisé d'organiser les travaux et la mobilisation des bons acteurs de les conduire. La mise en conformité doit alors à ce stade être abordée à la fois unitairement, traitement par traitement, et dans sa globalité, en prenant en compte l'ensemble des exigences de la loi.

S'APPUYER SUR LES FORMALITÉS DÉCLARATIVES POUR STRUCTURER LA RÉFLEXION

Le premier aspect de cette mise en conformité correspond bien évidemment aux formalités déclaratives. Tout traitement doit être porté à la connaissance de la CNDP.

La loi distingue ainsi deux régimes : l'autorisation, pour les traitements sensibles ou manipulant des données sensibles au sens de la loi, et la déclaration, pour tous les autres cas.

Dans les deux cas, il convient de notifier à la CNDP :

- L'identité du responsable de traitement.
- Les caractéristiques du traitement : ses finalités, le type de données manipulées, leur durée de conservation et les personnes, désignées par leurs rôles ou missions, susceptibles d'y accéder.
- Les modalités d'application des droits des personnes.
- Les dispositifs de sécurisation des traitements, les éventuelles interconnexions, ainsi que les transferts vers des tiers et/ou à l'international.

La déclaration n'est pas une fin en soi : de nombreux organismes, notamment en France où les formalités sont très similaires, se sont vus sanctionner alors qu'ils avaient effectivement déclaré leurs traitements. L'essentiel des efforts doit porter sur les autres exigences de la loi – à tel point que la notion de déclaration tend à disparaître en Europe.

En ce sens, on peut donc s'appuyer sur ces formalités pour structurer la réflexion autour de la mise en conformité de chaque traitement.

GARANTIR LE RESPECT DES DROITS DES PERSONNES

L'intitulé de la loi est explicite : il s'agit de protéger les personnes physiques à l'égard des traitements de données à caractère personnel. Dès lors, le respect de leurs droits se trouve tout naturellement au cœur des préoccupations du législateur.

Les personnes doivent ainsi en tout premier lieu être informées de la mise en œuvre et des caractéristiques de tout traitement de leurs données. Elles doivent être en mesure de pouvoir s'y opposer. Il convient ainsi, pour chaque traitement, d'identifier les canaux de collecte afin d'y faire figurer les mentions d'information adaptées.

Par ailleurs, la loi impose la mise en œuvre de moyens permettant aux personnes de se faire communiquer les données les concernant et, si besoin, de les faire corriger ou supprimer.

Traiter la conformité dans sa globalité

Comment déclarer ?

On s'est interrogé sur le niveau de détail à adopter pour décrire un traitement. Les mêmes questions que l'on se posait alors peuvent également s'appliquer à la déclaration. Doit-on déclarer une application ? Un processus ? Un ensemble ou, a contrario une sous-partie d'application ?

Les principes posés restent alors d'autant plus vrais qu'une déclaration doit être maintenue à jour, chaque modification devant être également portée à la connaissance de la CNDP :

- La déclaration doit s'effectuer d'un point de vue fonctionnel : les évolutions techniques n'entraîneront pas de nouvelles notifications à la CNDP.
- La déclaration doit être effectuée à un niveau de détail élevé, des précisions étant apportées en fonction du niveau de sensibilité du traitement : une légère évolution du processus ou des fonctionnalités n'entraîneront pas de non-conformité. Par ailleurs, si le texte de la loi spécifie que chaque traitement doit faire l'objet d'une déclaration, il n'en est pas moins possible de réaliser une déclaration unique pour un ensemble de traitements.
- Le périmètre de déclaration doit permettre d'anticiper sur les évolutions futures : si plusieurs modules d'applications concourant à des finalités proches évoluent à des rythmes très différents, il est préférable de faire plusieurs déclarations.

Les formulaires de déclaration sont disponibles sur le site de la CNDP.

Ces moyens doivent inclure un pan procédural et organisationnel et un pan outillage. Outre la mise à disposition de courrier type ou la création de listes de diffusion internes dédiées, il peut être nécessaire de modifier les applications afin de rendre possible cet accès ou cette modification des données.

L'expérience montre qu'il s'agit peut-être ici de l'aspect le plus complexe de la loi : comment propager sur le SI la modification des données d'une personne ? Comment permettre la restitution de ces données ? Comment informer les personnes si les données n'ont pas été collectées directement auprès d'elles ? Comment conserver une trace de l'opposition d'une personne à ce que l'on manipule ses données ?

De nombreuses questions peuvent se poser. Seul un examen minutieux, au cas par cas, permet d'y apporter une réponse.

PROTÉGER LES DONNÉES, EN FONCTION DE LEUR SENSIBILITÉ, DURANT TOUT LEUR CYCLE DE VIE

Les données doivent être protégées contre tout risque de divulgation, de perte ou de déformation. Les mesures à mettre en œuvre doivent être proportionnées aux risques encourus : les formalités déclaratives fournissent alors l'occasion d'évaluer ces risques pour chaque traitement et ainsi d'identifier les éventuelles mesures spécifiques à déployer pour renforcer localement la sécurité (chiffrement, renforcement du contrôle d'accès, conduite d'audits supplémentaires réguliers, etc.).

Ces mesures doivent se propager aux éventuels sous-traitants susceptibles d'intervenir sur le traitement : ceux-ci doivent donc être inventoriés et le dispositif contractuel mis en place doit être adapté.

De la même façon, le responsable de traitement doit assurer la sécurité de données, y compris si celles-ci sont amenées à être transférées vers des pays étrangers. Ainsi, des mesures spécifiques doivent être mises en place dès lors que les données deviennent accessibles depuis un pays n'offrant pas une protection juridique équivalente à la protection à présent garantie sur le territoire marocain par la loi 09-08.

AU-DELÀ DE LA LOI, METTRE L'ESPRIT DE LA LOI AU SERVICE DE LA PROTECTION DE L'ENTREPRISE

La réflexion décrite précédemment permet de se conformer aux exigences explicites du texte. Celles-ci découlent, on l'a dit, des trois principes clés que sont la loyauté, la finalité et la proportionnalité.

Et c'est bien à l'aune de ces principes qu'au final, chaque traitement doit être examiné : quelles sont réellement les raisons ayant amené à la mise en œuvre du traitement ? Les finalités que je poursuis sont-elles légitimes ? Nécessitent-elles raisonnablement l'ensemble des données qui sont manipulées ? Ai-je collecté ces données de manière loyale ? Etc.

Ce questionnement permettra d'augmenter le niveau de conformité de l'entreprise bien plus que la mise en place de mesures de sécurité complexes et coûteuses. Il permettra de plus, à terme, d'identifier les traitements superflus ou inutilement complexes et ainsi de mettre en évidence des axes clairs de rationalisation ou de simplification des pratiques et du système d'information.

Pilier n°5 - Maintenir et améliorer le niveau de conformité

La conformité n'est pas un projet. C'est un mode de fonctionnement qui doit s'ancrer au sein de l'ensemble des processus de l'organisme. Tout l'enjeu est alors de mettre en évidence ces points d'ancrage et de maintenir le niveau minimal d'efforts pour faire durablement évoluer les pratiques.

MAÎTRISER LES ÉVOLUTIONS DES TRAITEMENTS

De nouveaux traitements sont régulièrement mis en place. En parallèle, les anciens traitements évoluent en permanence : des fonctionnalités sont ajoutées, des nouvelles technologies sont introduites, des données jusqu'alors non manipulées sont enregistrées, de nouveaux canaux de collecte émergent, etc.

Ainsi, un organisme totalement conforme à un instant donné le sera de moins en moins si les actions nécessaires ne sont pas menées, parce que les traitements ne correspondent plus à ce qui a été déclaré, parce que les nouveaux canaux de collecte ne garantissent pas le droit d'information des personnes, parce que les nouvelles technologies ne sont pas suffisamment sécurisées, etc.

Les écarts entre le niveau cible de conformité et le niveau réel se creusant, l'entreprise devra alors se lancer dans un nouveau projet de mise en conformité, avec inventaire, analyse d'écart et plan d'actions complets.

La rationalisation des efforts de maintien en conformité passe alors par la mise en place, très en amont, des dispositifs permettant de maîtriser ces divergences sur le long terme.

Il s'agit donc d'analyser les pratiques en place en matière de gestion de projet pour y intégrer la conformité et la sécurité. Ce mode de fonctionnement, le *privacy by design* anglo-saxon, permet de maintenir un niveau acceptable de conformité avec un effort minimal : dès leur mise en place, les traitements ou évolutions de traitement sont conformes et aucun *rattrapage* coûteux n'est nécessaire. On l'a dit, l'atteinte d'un tel objectif nécessite un bon niveau de sensibilisation de l'ensemble des acteurs impliqués dans les projets. En particulier, afin d'être à même d'accompagner ces évolutions de traitement dès leur émergence et ce, y compris lorsque la direction des systèmes d'information n'intervient pas, les métiers doivent être suffisamment informés des enjeux pour avoir le réflexe de solliciter les bons experts. On retrouve ici l'impératif de visibilité de l'interlocuteur en charge de la conformité.

Par ailleurs, la mise en place d'un cadre garantissant la bonne gestion des sous-traitants doit venir renforcer ce dispositif. L'objectif est alors de s'assurer que toute externalisation d'activité, qu'elle soit métier ou technique, fait bien l'objet d'un contrat prenant en compte les exigences adéquates de sécurité et de conformité et que le respect de ces exigences est suivi et contrôlé dans le temps.

ALIMENTER LE CERCLE VERTUEUX DE LA CONFORMITÉ

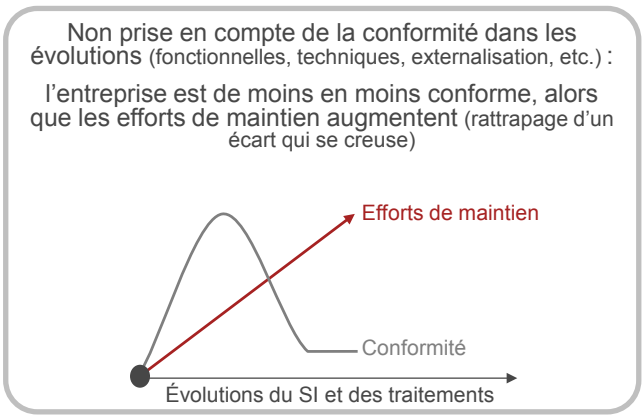
L'intégration de la conformité dans les projets et la gestion des sous-traitants permet donc de pérenniser les efforts déjà menés pour la mise en conformité.

Au-delà de cette préoccupation, la mise en conformité initiale ayant reposé sur la priorisation et l'arbitrage, il peut être souhaitable d'augmenter progressivement le niveau initialement atteint.

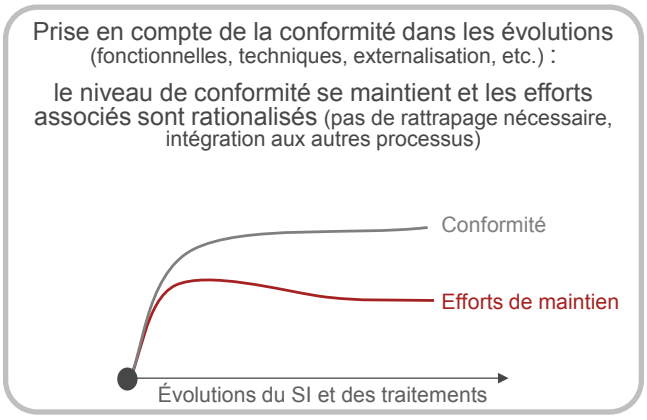
Par ailleurs, si les traitements évoluent, l'exposition au risque de non-conformité augmente elle aussi : la sensibilité du grand public va croître, en parallèle des attentes des partenaires commerciaux. La comparaison à la concurrence risque également de devenir de moins en moins favorable pour les organismes n'offrant pas les garanties suffisantes en matière de protection de la vie privée. La doctrine de la CNDP va s'enrichir, et des sanctions seront prononcées. La loi elle-même peut être amenée à évoluer.

Il convient donc de se doter d'un dispositif permettant de rester aligné sur les éventuels futurs changements législatifs et de répondre à une pression externe qui va croître.

Intégrer la conformité aux processus existants...



... pour pérenniser les efforts



Un tel dispositif peut prendre la forme d'un véritable système de management de la conformité, c'est-à-dire d'un processus continu permettant d'améliorer progressivement son niveau de conformité, aligné sur une cible ajustée en permanence en fonction d'éléments externes comme internes.

La première étape de ce processus correspond ainsi à la construction de cette cible et l'analyse de l'écart à cette cible. Cette analyse permet d'élaborer un plan d'actions mis en œuvre dans une deuxième étape.

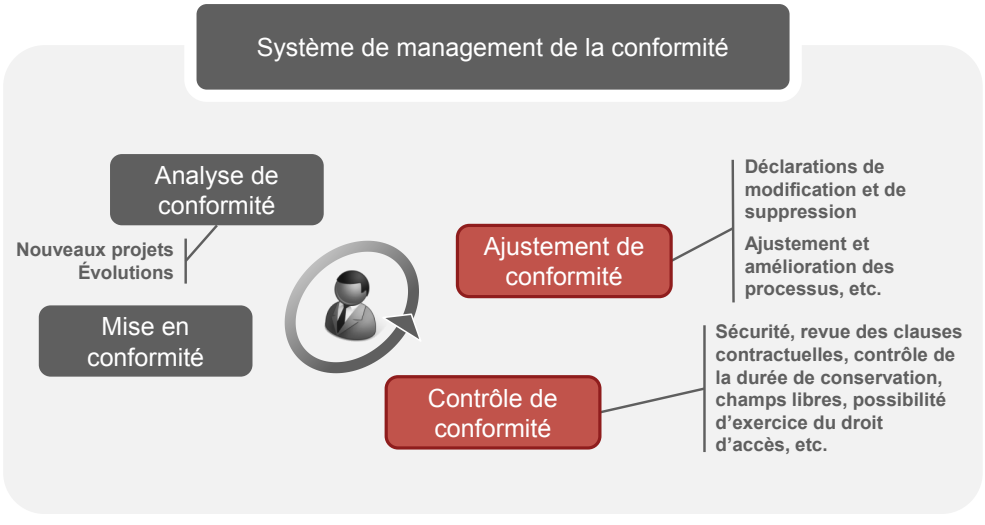
La troisième étape consiste ensuite à contrôler aussi bien l'efficience que l'efficacité des actions menées : a-t-on bien mis en oeuvre les mesures de sécurité nécessaires ? Les canaux en place permettent-ils d'assurer les droits d'accès et de rectification de façon rationalisée ? Les contrats contiennent-ils les clauses de sécurité adaptées ? Les ressources mobilisées pour la conformité sont-elles correctement exploitées ? Etc.

Les éléments de sortie de ce contrôle permettent ainsi de corriger les éventuels écarts résiduels, dans une quatrième étape, ou d'ajuster la cible pour un nouveau cycle.

Une fois encore, chacune des briques nécessaires à ce système de management sont à mettre en œuvre en fonction des enjeux et du niveau de maturité déjà atteint par l'organisme. À titre d'illustration, les étapes de contrôle et d'ajustement sont généralement initiées relativement tardivement.

Quoi qu'il en soit, l'ensemble du processus est bien à anticiper dès les étapes de cadrage, qui doivent notamment prévoir la montée en charge de la structure de pilotage de la conformité et la définition d'indicateurs.

Mettre en place un véritable système de management de la conformité



« Bien plus que de se mettre en conformité à une nouvelle loi, il s'agit de se familiariser dès aujourd'hui, à son rythme, avec ce qui permettra demain de répondre à des impératifs bien plus grands et bien plus pressants »

En conclusion

La loi 09-08 accompagne et structure l'ensemble des volets du plan *Maroc Numeric 2013*.

Son entrée totale en application, fin 2012, va progressivement faire évoluer la relation qu'entretient le citoyen avec les technologies de l'information. Dès lors, il s'agit pour les organismes marocains de se mettre en ordre de marche pour accompagner, voire anticiper ce mouvement.

Pour autant, et même si des chantiers transverses peuvent dès à présent être lancés, il est indispensable de prendre le temps de la réflexion et de procéder par étapes, en fonction de ses enjeux et priorités propres. Progressivement, c'est l'ensemble des acteurs de l'entreprise qu'il conviendra de mobiliser afin de mettre en place les dispositifs transverses permettant d'assurer la conformité sur le long terme.

D'ores et déjà, la réflexion est plus qu'amorcée au sein de nombreux organismes. Sous la pression d'un grand public de plus en plus averti et d'un paysage concurrentiel de plus en plus mature, le niveau s'exigence en matière de conformité ne fera que croître.

À ce jour, l'absence logique d'une doctrine claire sur le sujet est perçue comme un handicap majeur. Les interprétations des lois équivalentes votées en Europe commencent néanmoins à converger ; un riche retour d'expérience existe donc et est à disposition de qui saura méditer sur les bonnes pratiques internationales en la matière.

Bien plus, ce vide tout relatif constitue une opportunité unique de participer à l'élaboration de cette doctrine au lieu de la subir. Il offre ainsi un droit précieux à l'erreur pour les organismes qui, même tâtonnant, auront joué le jeu de la mise en conformité.

Enfin, au fur et à mesure que la pédagogie laissera place à la sanction, il y a fort à parier que les exigences de la loi iront en se durcissant, à l'image de ce que l'on observe aujourd'hui sur la scène internationale. En Europe comme aux États-Unis, on parle en effet notamment de plus en plus de rendre obligatoire la notification publique de toute violation à la protection des données à caractère personnel.

Nous espérons que ce livre blanc vous aura fourni les clés nécessaires pour aborder sereinement ce défi.

Remerciements

L'AUSIM et Solucom remercient vivement l'ensemble des membres de l'association, et en particulier leurs dirigeants et collaborateurs qui ont consacré un temps précieux pour apporter leur contribution à l'élaboration de ce livre blanc : 2M, Bank Al Maghrib, Banque Centrale Populaire, Centrale Laitière, Crédit Immobilier et Hôtelier, Lydec, Méditel, ONE, Barid Al Maghreb, Régime Collectif d'Allocation de Retraite, Toyota Maroc.

L'AUSIM tient à remercier particulièrement les représentants de ses membres qui ont pris part au cadrage et à l'accompagnement des travaux d'élaboration de ce livre blanc à travers l'équipe ad hoc.

Association des Utilisateurs des Systèmes d'Information au Maroc

L'Association des Utilisateurs des Systèmes d'Information au Maroc – AUSIM – est une association à but non lucratif créée en 1993. Elle compte parmi ses adhérents de nombreuses structures (Offices, Banques, Assurances, Entreprises Industrielles, …) qui jouent un rôle de leadership sur le plan organisationnel et managérial au Maroc. L'AUSIM a pris les devants pour démontrer sa volonté de contribuer à la promotion des systèmes d'information au Maroc tout en s'associant aux autres acteurs du secteur, et s'est donné pour objectifs :

- La promotion de l'usage des systèmes dinformation au profit de la création de valeur.
- La contribution à la protection des intérêts de ses adhérents.
- Le renforcement des liens qui l'unissent aux associations similaires au Maroc et à l'étranger.
- La diffusion entre les membres des connaissances et des informations relatives aux systèmes d'information.
- La participation aux grandes réflexions et réformes nationales sur le sujet.

L'AUSIM constitue un carrefour privilégié d'échange et de débat autour des problématiques du secteur des technologies de l'information. Ainsi, l'association organise les « RDV de l'AUSIM » sous forme de rencontres périodiques réunissant les membres de l'AUSIM et des experts du secteur autours de problématiques communes à l'ensemble de la communauté. Les « Assises de l'AUSIM », qui se veulent un rendez-vous incontournable des SI au Maroc et un vecteur de propositions concrètes dans tous les domaines relatifs aux TIC, constituent une excellente tribune permettant aux participants et intervenants de débattre de la manière de faire des systèmes d'information un levier de croissance pour l'économie nationale, et un outil de performance et de compétitivité pour les entreprises.

Véritable porte-parole des DSI qui la constituent, l'AUSIM a pour mission principale d'influencer l'écosystème des SI au Maroc, par la coordination avec les divers partenaires et parties-prenantes et par le développement des projets, aussi bien pour les membres que pour la communauté.

S'inscrivant dans une démarche de sensibilisation de ses membres, l'AUSIM produit régulièrement des livrables thématiques (bulletins de veille SI périodiques, enquêtes…) visant à les informer régulièrement des dernières actualités, au Maroc et ailleurs, liées aux technologies et aux systèmes d'information ainsi que leur macro environnement. L'AUSIM réalise également des travaux à forte valeur ajoutée au profit de la communauté : des rapports d'études, des enquêtes… et des livres blancs qui constituent une synthèse de bonnes pratiques dans le domaine des SI.

Par ailleurs, l'AUSIM soutient la vulgarisation de l'usage des technologies de l'information, par le biais d'actions d'accompagnement associatif. Des partenariats ont été signés avec des associations et des établissements d'enseignement dans ce sens. Dans cette optique, l'AUSIM s'engage à sensibiliser ses membres et supporter toutes les initiatives visant l'économie d'énergie et le développement durable des technologies de l'information. L'association œuvre également pour le renforcement du partenariat Ecoles-Entreprises à travers l'organisation de rencontres et de concours (Innov'IT) encourageant l'innovation et la créativité dans le domaine des technologies de l'information.

Les DSI marocains sont ainsi invités à prendre part, en tant que représentants de leurs entreprises et administrations, aux différents chantiers de l'association afin de contribuer à l'expansion de l'usage des systèmes d'information au sein des organisations marocaines, à influencer intelligemment l'environnement TIC dans notre pays et à faire gagner des points pour le Maroc Numérique.

« …La vision de l'AUSIM est de jouer le rôle de locomotive pour accélérer la diffusion de l'usage des systèmes d'information au Maroc. »

solucom
management & IT consulting

NOTRE AMBITION 2015 : DEVENIR LE PREMIER CABINET DE CONSEIL INDÉPENDANT EN FRANCE

Solucom est un cabinet de conseil en management et système d'information.

Ses clients comptent parmi les plus grandes entreprises et institutions : Solucom intervient auprès des directions métiers et des directions des systèmes d'information, dans le cadre de leurs réflexions stratégiques, démarches d'innovation et projets de transformation.

Solucom s'est constitué sur une idée simple : réunir au sein d'un même cabinet les meilleures expertises du marché sur chacun des domaines clés du conseil en management et système d'information, et conjuguer sans couture l'ensemble de ces compétences afin d'apporter, au titre de chacune de ses missions, une valeur ajoutée sans égale.

L'étendue de ses savoir-faire, et sa connaissance approfondie des enjeux de chaque grand secteur économique, ont permis à Solucom de devenir un acteur de premier plan, partenaire naturel des réflexions stratégiques et des grands programmes de transformation.

Cette stratégie, ce choix d'indépendance, ainsi que la focalisation sur le métier du conseil, sont les fondements du modèle de Solucom. Un modèle porté par près de 1 000 collaborateurs et validé par le marché. Un modèle sur lequel Solucom veut capitaliser pour devenir, à horizon 2015, le champion de la transformation des entreprises.

UNE PRÉSENCE INTERNATIONALE

Afin de mieux accompagner ses clients dans leur développement international, Solucom a noué des partenariats : Hidra Partners, cabinet de conseil espagnol spécialisé dans les nouvelles technologies de l'information et de la communication, et DMW group, cabinet britannique indépendant de conseil IT. Il a également tissé des relations privilégiées avec des acteurs de référence du Maroc et de la Belgique.

DES PRISES DE POSITION FORTES

Solucom a toujours eu pour ambition de partager ses convictions et visions du marché librement à travers des articles de presse et des publications (accessible sur www.solucom.fr, rubrique publications).

En mars 2011, Solucom a lancé son magazine en ligne (SolucomINSIGHT), qui propose des éclairages et des points de vue sur l'actualité des organisations et du SI au travers de rubriques thématiques et sectorielles. SolucomINSIGHT est également disponible en version iphone depuis juillet 2011.

Venez découvrir SolucomINSIGHT : www.solucominsight.fr

Livre blanc écrit par **Marianne Benichou** et **Ons Ben Abdelkarim**, respectivement consultante senior et consultante au sein du cabinet Solucom.

Association des Utilisateurs des Systèmes d'Information au Maroc

42 rue Omar Slaoui, 1er étage
20 140 Casablanca, Maroc.
Tél : +212 522 48 75 96 Fax : +212 522 48 75 96
ausim@ausimaroc.com
www.ausimaroc.com

solucom
management & IT consulting

Tour Franklin, 100-101 Terrasse Boieldieu, La Défense 8
92042 Paris La Défense Cedex, France
Tél. : 01 49 03 25 00 Fax. : 01 49 03 25 01
www.solucom.fr