L'Europe se penche sur la protection des données

Dès 2018, une nouvelle règlementation européenne sur la protection des données privées contraindra les entreprises à des adaptations. Laurent Deheyer et Michael Raison, respectivement cybersecurity consulting director et principal consultant de la société Approach, nous en dressent une esquisse.

Laurent Deheyer
Cybersecurity consulting director chez Approach

Le GDPR est abordée soit sous l'aspect juridique soit sous l'aspect informatique, mais pour bien la gérer, il faut nécessairement impliquer des profils différents.

Michaël Raison
Principal consultant chez Approach

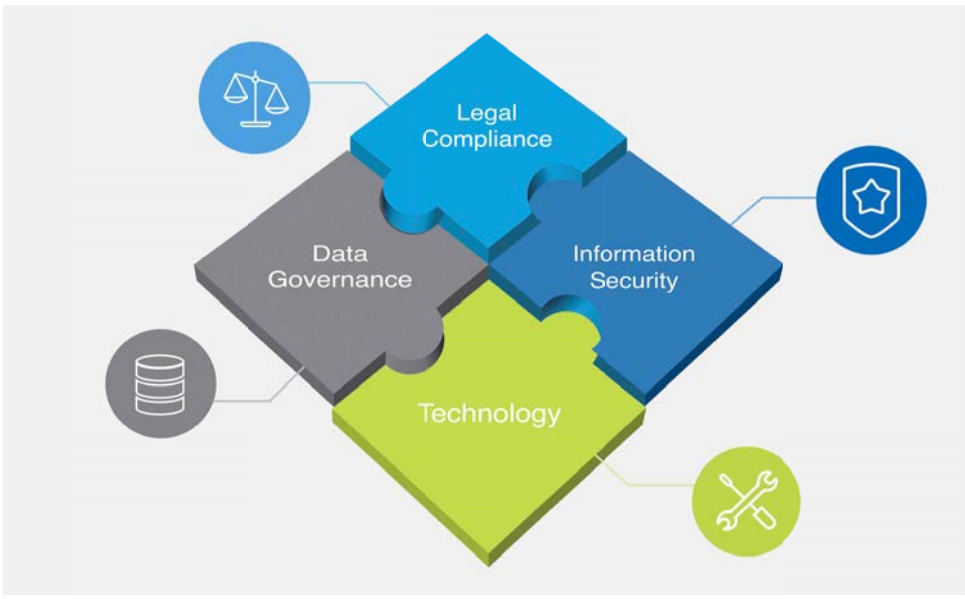
Dans certains cas, le GDPR impose la désignation d'un Data Protection Officer (DPO). Cette fonction peut être interne ou externalisée.

Quels changements la nouvelle règlementation entraînera-t-elle ?
Michaël Raison : « Le General Data Protection Regulation – en abrégé, RGPD en français et GDPR en anglais - entrera en vigueur en mai 2018. La nouvelle règlementation considère les données sur tout leur cycle de vie, de l'acquisition à la suppression, et fournit des détails imprécisés auparavant. Lors de l'acquisition, elle insiste beaucoup plus sur le consentement explicite d'un utilisateur. Exemple : plus de case cochée par défaut ! L'entreprise devra détailler toutes les finalités de l'utilisation des données et préciser celles des tierces parties qui y auront accès, comme des sous-traitants. Les contraintes augmenteront. Toutefois, dans le cadre de la libre circulation des données et du marché unique, cela ouvre aussi des portes. »

Quel est l'objectif de cette règlementation ?
Laurent Deheyer : « Il est entre autres d'harmoniser et renforcer les lois actuelles et de faciliter les échanges. Jusqu'ici, chaque État de l'UE pouvait traduire les directives européennes existantes. En outre, les contraintes du GDPR seront assorties de sanctions beaucoup plus lourdes. »

Les entreprises y sont-elles suffisamment sensibilisées et préparées ?
L. D. : « Au niveau des dirigeants et des comités de direction, nous avons aujourd'hui atteint un degré de sensibilisation qu'on aurait souhaité avoir il y a un an, à la publication du règlement. Au niveau des employés, cela varie d'un secteur d'activité à un autre, voire d'un département à un autre. Certains collaborateurs sont sensibilisés, d'autres le sont moins ou le voient comme une contrainte, par exemple au sein des départements marketing. Nous observons aussi qu'au sein d'une même entreprise, chaque département avance à son propre rythme : le département juridique peut déjà être avancé sur la question, tandis que le département informatique ne l'est pas du tout... ou vice-versa ! »

Quelles connaissances le GDPR implique-t-elle de maîtriser ?
L. D. : « En général, le GDPR est abordée soit sous l'aspect juridique soit sous l'aspect informatique, mais pour bien la gérer, il faut nécessairement impliquer des profils différents : des juristes, des spécialistes en gouvernance et gestion de flux des données, des experts en cybersécurité, des spécialistes du domaine technologique tel que le cloud ou le big data... »



Framework GDPR : la General Data Protection Regulation entrera en vigueur en mai 2018.

M. R. : « Nous agissons de manière structurelle sur quatre axes : juridique, gouvernance des données, technologie de l'information et sécurité des données. Nous travaillons avec une approche transversale et un large spectre couvrant tous les départements de l'organisation. Des données liées à la vie privée circulent dans toute l'entreprise : sont-elles sensibles ? Par où passent-elles ? À qui les transmet-on ? »

L. D. : « Il faut d'abord avoir une bonne connaissance de son entreprise et de ses relations avec l'extérieur - sous-traitants, partenaires, clients. Il faut cartographier le traitement des données et ses flux. Ensuite, il faut se demander si ce traitement respecte la réglementation et quels sont les risques. Enfin, il s'agit de mettre en place une équipe, des responsabilités et de définir le planning des opérations à effectuer. »

Qui doit se charger de ces tâches ?
M. R. : « Il faut définir un comité de gestion sur cette problématique au sein de l'entreprise, avec les acteurs principaux. Dans certains cas, le GDPR impose la désignation d'un Data Protection Officer (DPO). Cette fonction peut être interne ou externalisée. Afin qu'il ait un jugement objectif du traitement des données, ce DPO ne peut pas être impliqué dans l'opérationnel. »

Vous organisez également sous peu des événements sur ces questions...
L. D. : « Oui, nous partons du constat que de nombreuses entreprises se sentent désorientées ou ne savent par où commencer. Avec, de surcroît, une pression sur le timing imposé par une mise en vigueur en mai prochain. Pour les aider, nous organisons notamment une série de tables rondes avec des décideurs de diverses entreprises de tout secteur. Nous contribuons aussi régulièrement à des conférences et forums professionnels sur la cybersécurité. Par ailleurs, en collaboration avec un partenaire, nous organisons aussi des formations certifiantes pour les DPO (Data Privacy Officer). Il est possible de s'inscrire à nos tables rondes, nos formations ou tout simplement demander plus d'informations sur notre site. Précisons que notre société est spécialisée en cybersécurité et notamment en conformité des systèmes informatiques. À ce titre, nous disposons de plus de 60 experts qui réunissent toutes les compétences pour accompagner nos clients dans leur conformité avec le GDPR. »

APPROACH

WWW.APPROACH.BE/NEEDS/GDPR

Philippe Van Lil
redaction.be@mediaplanet.com