Les clés de l'IT - Sécurité : Toutes les définitions à connaître Téléchargement Gratuit

ARTENAUTA - FOTOLIA

GDPR : quels outils faut-il commencer à mettre en place pour atteindre la conformité ?

par
Cyrille Chausson
Rédacteur en Chef

Pour y voir plus clair dans le nouveau règlement européen sur la protection des données privées, l'avocat spécialisé François-Pierre LANI explique les points clefs à comprendre et à mettre en œuvre. Cette deuxième partie revient sur l'outillage que l'on peut d'ores et déjà déployer.

François-Pierre LANI est avocat associé au sein du cabinet Derriennic Associés. Il est spécialiste en droit de l'informatique et des technologies nouvelles.

Cet article est le troisième d'une série de cinq. Le premier a abordé les trois piliers du RGPD que sont l'« Accountability », la coresponsabilité et le « Privacy by Design ». Le troisième se penchera sur les outils que l'on peut d'ores et déjà commencer à mettre en place pour atteindre la conformité. Le quatrième précisera les différentes étapes d'un projet de mise en conformité pour la DSI. Enfin, la cinquième partie de cet entretien reviendra sur les opportunités et les menaces que le GDPR représente pour les acteurs français.

Comment atteindre la conformité et – en attendant que tout soit bien précisé par la CNIL - comment démontrer que l'on a bien tenté de l'atteindre ?

Un acteur économique peut utiliser de nouveaux outils qui lui permettront de démontrer son niveau de conformité.

On a par exemple le « registre des traitements » , la mise en place et l'adhésion à codes de conduite. Il pourra également faire certifier certains traitements et/ou processus.

Il faut bien comprendre que l'entreprise va être jugée sur ses processus internes. Et sur la responsabilisation de chaque intervenant dans le processus allant de la fabrication à la commercialisation du produit ou du service.

Justement, une nouveauté concrète est le « Privacy by Design » que vous avez abordé dans la première partie de cet entretien. Comment, concrètement, mettre cette notion en place?

Privacy by Design » signifie littéralement que la protection des données personnelles doit être prise en compte dès la conception du produit ou du service.

C'est ce que j'explique à mes clients éditeurs de logiciels, notamment dans les RH et la paye... Et ils tombent de leur armoire !

L'idée est de dire qu'ils s'attachent déjà, dès la R&D, au modèle conceptuel des données, aux algorithmes, à la maintenabilité du produit, à son évolutivité, à sa conformité par rapport à la loi (les payes, les déclarations annuelles, etc.). Et bien désormais, ils vont aussi devoir s'attacher à la protection des données personnelles.

Concrètement cela signifie que dans la conception même de mon produit, je dois préciser les outils techniques de protection et les garanties que je vais mettre en place dans mes produits logiciels ou dans mes plateformes Web ou Intranet pour que les principes de protection des données (ex : la minimisation des données) soient respectés. Quels sont les outils ? Quelles sont les recommandations que je fais ? Et comment je vais tracer tout cela dans mon document de conception de mon produit ?

C'est un point fondamental. Dès que je pose mon produit sur le papier, je dois à présent mettre une case « protection des données personnelles ».

La conséquence directe de cela c'est **l'analyse d'impact**. C'est une description systématique des opérations de traitements. Elle comprend une évaluation de la nécessité et de la proportionnalité des opérations au regard des finalités – c'est-à-dire que je vais justifier pourquoi, au sein de mon entreprise, j'effectue chaque traitement et quelle est sa nécessité. En clair, on pose la question « est-ce véritablement nécessaire de faire ce traitement ? »

Dans cette analyse d'impact il y a également **l'évaluation des risques pour les droits et les libertés**. Il doit aussi y figurer, et c'est peut-être le point le plus important, les **mesures pour faire face aux risques identifiées**. Et ce sont ces mesures que je vais ensuite mettre en place.

Y'a-t-il d'autres points majeurs de ce règlement ?

Oui, il y a la notification des failles de sécurité (violation de données).

Une fois que j'ai mon analyse d'impact, je dois aussi - et surtout – imaginer un processus technique qui me permet de déceler des failles et d'y apporter les mesures correctives de première urgence.

Ce processus technique doit me permettre de notifier cette faille à l'autorité contrôle mais aussi, dans certains cas, à toutes les personnes concernées. En France, il faudra par exemple prévenir la CNIL dans les 72 heures.

Ces exigences en matière de sécurité commencent déjà à apparaitre dans les appels d'offres. Des listes commencent à être établies. C'est purement et simplement un cahier des charges en matière de sécurité. Si en tant que prestataire vous répondez par oui, tout est parfait. Si c'est « oui, peut-être », c'est à analyser. Et si vous répondez « non », vous ne serez très certainement pas choisi.

De ce que vous dites, cela risque d'avoir quelques conséquences économiques ?

Oui parce que ces nouvelles exigences en sécurité vont partir de la base. Les entreprises commencent à dire « à partir du moment où je te confie un outil susceptible de produire de la donnée personnelle, voici les éléments de sécurisation que je souhaite ».

Les exigences vont être de plus en plus élevées et sélectives, et le marché va épurer les fournisseurs qui ne prennent pas en compte le « Privacy by Design ».

C'est pourquoi les **audits de conformité** que nous faisons se doublent déjà d'un **audit technique** qui permet de déterminer si l'entreprise dispose des bons outils de protection. Déceler la failler, alerter, notifier. Les éditeurs de sécurité travaillent sur ces sujets.

Y'a-t-il des listes de produits « certifiés conformes » ou des checklists officielles pour qu'un DSI s'assure qu'il a fait tout fait correctement pour la sécurité des données aux yeux de la loi ?

Pas encore. Pour l'instant, chacun s'inspire de tout le monde.

On voit des listes très différentes dans les appels d'offres. Certaines confinent à l'excès. D'autres sont d'une simplicité inquiétante. Mais certaines sont très abouties.

Pour le « sceau de conformité », c'est un sujet qui n'est pas bien défini. Les autorités nationales auront la possibilité de contrôler et d'allouer ces sceaux. Certains prestataires pourraient également le donner. Mais ce n'est pas du tout défini aujourd'hui. En tout cas c'est l'esprit de la loi.