Focus #4 – Application du RGPD : « démêler le vrai du faux »

Août 2017

*Notre livre blanc « **Le RGPD en 10 leçons – L'essentiel du RGPD dans un guide pratique** » avait pour objectif de synthétiser et de rendre accessibles les dispositions issues du règlement européen sur la protection des données (RGPD) afin de vous:*

- permettre de cerner les implications en résultant pour les entreprises ;
- proposer des astuces et bonnes pratiques visant à traduire ces dispositions règlementaires en actions concrètes de mise en conformité à envisager.

*Nous vous proposons désormais, sous l'intitulé **« Le RGPD en focus »**, une série de focus sectoriels et/ou métiers afin de vous permettre d'approfondir les évolutions induites par le RGPD et plus généralement de soulever certains points d'alertes spécifiques. En effet, les principes et obligations résultant du RGPD ne constituant pas que des nouveautés, cette nouvelle règlementation est aussi l'occasion d'une mise en conformité plus globale et de rappels génériques en matière des bonnes pratiques.*

Ces focus n'ont pas pour objet de reprendre l'intégralité des principes et obligations applicables en matière de traitements de données (sur ce point, vous pouvez consulter le livre blanc) mais de s'attacher aux pratiques spécifiques des secteurs et/ou métiers visés.

Nous restons à votre écoute pour toute thématique que vous souhaiteriez voir aborder dans ce cadre, n'hésitez pas à nous en faire part.

L'application désormais imminente du RGPD est à l'origine de tous les fantasmes. Entre craintes et espoirs, doutes et certitudes, il résulte surtout qu'un certain nombre d'interrogations demeurent en suspens et que nombre d'idées reçues se répandent. Or, compte tenu de l'impact de ces nouvelles dispositions, il est structurant de ne pas en mésestimer les conséquences tout en ayant une lecture claire et pragmatique de leurs incidences.

C'est pourquoi nous vous proposons dans ce 4ème numéro du « RGPD en focus » de revenir sur « le vrai du faux » de certaines affirmations entendues ici et là s'agissant de l'application de cette nouvelle règlementation.

*
* *

1. **<u>Le RGPD abroge la loi Informatique et libertés française</u>**

FAUX

Le RGPD abroge la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données avec effet au 25 mai 2018[1]. En revanche, il n'abroge pas la loi Informatique et libertés française (loi 78-17 du 6-1-1978 relative à l'informatique, aux fichiers et aux libertés).

En effet, le RGPD est un règlement européen, et donc d'application directe dans les Etats membres de l'Union européenne (c'est-à-dire que son application dans chacun de ces Etats ne nécessite pas de transposition par une loi nationale). Il lui est par ailleurs conféré une supériorité dans la hiérarchie des normes par rapport au droit national. Toutefois, le RGPD n'a pas le pouvoir d'abroger la loi française : il a uniquement pour conséquence de rendre inapplicables les dispositions légales et réglementaires nationales qui seraient incompatibles avec les dispositions qu'il contient.

En pratique, cela signifie qu'en cas d'incompatibilité entre les dispositions du RGPD et celles de la loi Informatique et libertés française, alors le RGPD prévaudra et la loi française sera écartée. En revanche, en l'absence d'incompatibilité, la loi française aura vocation à s'appliquer également.

Pour éviter toute discussion autour de cette notion d'incompatibilité, mais également parce que le RGPD comporte de très nombreux renvois au droit national des Etats membres, une réforme ou révision de la loi Informatique et libertés française est nécessaire, ce que la Cnil appelle d'ailleurs de ses vœux. C'est à cette loi que reviendra la tâche d'abroger les dispositions de droit français qui seront incompatibles (voire redondantes) avec le RGPD, et de parachever l'environnement normatif initié par le RGPD en matière de protection des données à caractère personnel.

2. **<u>Le RGPD ne sera pas applicable tant que les Etats membres n'auront pas pris les mesures législatives ou règlementaires appropriées en droit interne</u>**

FAUX, en partie

Comme précité, le RGPD est un règlement européen, et donc d'application directe au sein de chaque Etat membre[2]. Toutefois, il comporte de nombreux renvois au droit national desdits Etats membres, ce droit national ayant vocation à venir compléter le cadre normatif posé par le RGPD.

Aussi, il est vrai qu'une réforme de la loi Informatique et libertés française est nécessaire pour ne pas rendre inapplicable un certain nombre de dispositions du RGPD.

Toutefois, il n'en demeure pas moins que :

- les dispositions du RGPD qui ne font aucune référence au droit national seront applicables immédiatement au 25 mai 2018 de manière effective ;

- certaines dispositions, qui renvoient à une possible intervention des Etats membres par le biais de leur droit national, pourront tout à fait être applicables, même en l'absence de texte local ;

[1] RGPD, art.94.
[2] RGPD, art.99.

- il reste encore près de dix mois aux autorités pour prendre les mesures qui s'imposent en vue de l'élaboration et de la discussion de ce que certains surnomment déjà la « Loi Cnil 2 ».

La date d'entrée en application effective du RGPD ne doit donc pas être vue comme purement théorique mais bien comme une date butoir à avoir en ligne de mire en vue d'une mise en conformité la plus complète possible.

Il convient en tout état de cause de rester particulièrement vigilant sur les évolutions législatives et réglementaires imminentes en droit français en matière de protection des données à caractère personnel pour en identifier sans délai les impacts et déterminer les moyens de s'y conformer.

3. **Le RGPD laisse aux responsables de traitement une période complémentaire à horizon 2020 pour mettre en conformité les traitements préexistants**

FAUX

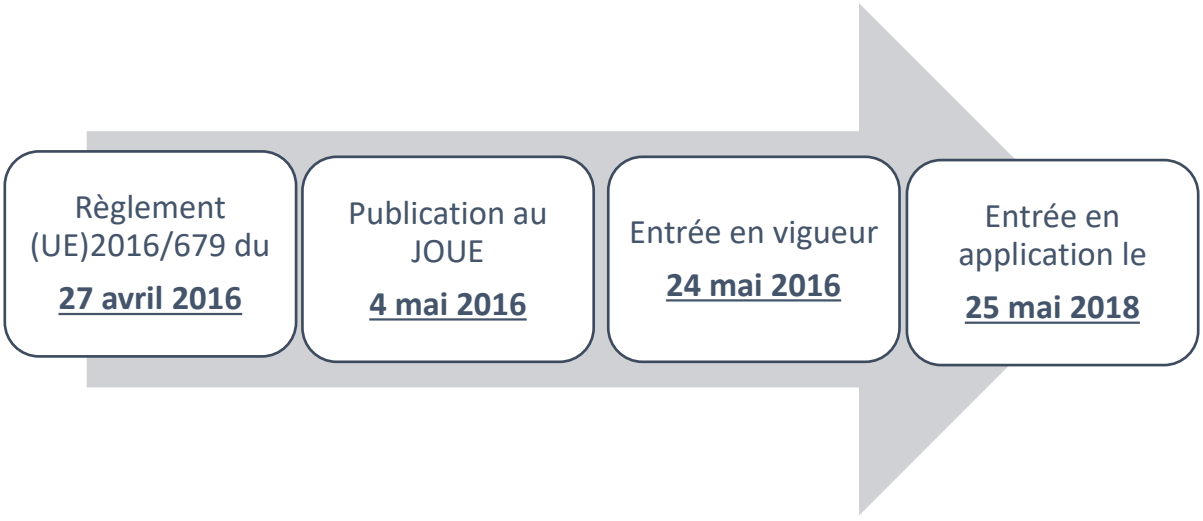
Cette confusion provient du fait que :

- la date d'entrée en vigueur du RGPD et sa date d'application effective sont différenciées ;

- le RGPD ne prévoit pas de régime transitoire, mais comporte en son considérant 171 une précision selon laquelle « *Les traitements déjà en cours à la date d'application du présent règlement devraient être mis en conformité avec celui-ci dans un délai de deux ans après son entrée en vigueur* ».

C'est sur le fondement de ce considérant que certains seraient tentés de penser que deux ans supplémentaires sont octroyés aux responsables de traitements et aux sous-traitants pour mettre en conformité leurs traitements d'ores et déjà mis en œuvre.

Mais qu'on se le dise : ***le RGPD est déjà « entré en vigueur »***, et ce depuis le vingtième jour suivant sa publication au Journal officiel de l'Union européenne[3], à savoir le 24 mai 2016. C'est uniquement son application qui est reportée au 25 mai 2018, soit deux ans après son entrée en vigueur.



[3] RGPD, art.99.

Aussi, une lecture attentive et une reformulation du considérant précité permettent d'éviter tout contre-sens :

- tous les traitements déjà en cours avant la date d'application du RGPD, c'est-à-dire avant le 25 mai 2018 ;

- devront être mis en conformité dans les deux ans suivant l'entrée en vigueur du RGPD, c'est-à-dire le 24 mai 2018 (la veille de la date d'application de ce texte).

Pour conclure, il résulte de ce qui précède que les traitements déjà mis en œuvre avant le 25 mai 2018 devront d'ici cette date être mis en conformité avec les dispositions du RGPD, les responsables de traitements et sous-traitants ne bénéficiant d'aucun délai complémentaire.

4. Le sous-traitant devient « coresponsable » de traitements

FAUX

Certes, le droit de la protection des données à caractère personnel, qui dans sa version applicable jusqu'à présent concernait essentiellement les « responsables de traitements », est significativement modifié pour étendre aux sous-traitants une large partie des obligations imposées aux responsables de traitements (assurer la sécurité des données, tenir un registre des traitements, désigner dans certaines hypothèses un délégué à la protection des données,…).

Certes, le sous-traitant peut désormais se voir imposer des mesures correctrices ou infliger des sanctions administratives par la Cnil, et ce à hauteur des sanctions pouvant être prononcées à l'égard des responsables de traitements pour des manquements équivalents. De même, à l'instar du responsable de traitements, le sous-traitant peut être poursuivi en justice par les personnes concernées.

Toutefois, le sous-traitant demeure responsable des manquements à ses propres obligations en qualité de sous-traitant et non des manquements aux obligations qui s'imposent au responsable de traitements (même si certaines obligations sont communes).

La confusion peut naître des dispositions selon lesquelles :

- les personnes concernées ont droit à un recours effectif contre un responsable du traitement ou un sous-traitant si elles considèrent que les droits que leur confère le RGPD ont été violés du fait d'un traitement de leurs données à caractère personnel effectué en violation du règlement[4] ;

- toute personne ayant subi un dommage matériel ou moral du fait d'une violation du RGPD a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi, chacun des responsables de traitements ou des sous-traitants participant au même traitement pouvant être tenu responsable du dommage dans sa totalité afin de garantir à la personne concernée une réparation effective.

[4] RGPD, art.79.

Il n'en demeure pas moins que :

- le sous-traitant n'est tenu pour responsable d'un dommage causé par un traitement que s'il n'a pas respecté les obligations prévues par le RGPD qui incombent spécifiquement aux sous-traitants ou qu'il a agi en-dehors des instructions licites du responsable de traitements (ou contrairement à celles-ci) ;

- lorsqu'un sous-traitant a, conformément aux dispositions précitées, réparé totalement le dommage subi, il est en droit de réclamer auprès des autres responsables du traitement ou sous-traitants ayant participé au même traitement la part de la réparation correspondant à leur part de responsabilité dans le dommage.

Il en résulte que si les sous-traitants se voient imposer des obligations et responsabilités complémentaires renforcées aux termes du RGPD, ils ne deviennent pas pour autant « co-responsables » des traitements dans le cadre desquels ils interviennent pour le compte et sur instructions d'un responsable de traitements.

Outre la répartition des obligations et le partage des responsabilités résultant du texte même du RGPD à l'égard des responsables de traitements et des sous-traitants, il conviendra de porter une attention particulière aux documents contractuels à conclure entre ces acteurs : en effet, si les clauses contractuelles à prévoir dans une telle hypothèse sont en grande partie dictées par le RGPD[5], des aménagements spécifiques à chaque situation devront être envisagés.

5. Le RGPD signe la fin des formalités pour la mise en œuvre de traitements de données à caractère personnel

FAUX

Il est certain qu'il résulte du RGPD un allègement des obligations en matière de formalités préalables.

Toutefois, si les déclarations préalables à réaliser sous l'empire de la loi actuelle auprès de la Cnil disparaissent du paysage règlementaire, il convient toutefois d'être conscient que les nouvelles dispositions applicables à compter du 25 mai prochain imposent :

- une consultation de la Cnil pour les traitements soumis à une analyse d'impact dont il résulte qu'ils présenteraient un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer ce risque ;

- une autorisation de la Cnil dans certaines hypothèses (certes limitées), telles que par exemple en cas de transfert des données vers des Etats non membres de l'Union européenne qui serait fondé sur des clauses contractuelles ad hoc.

Enfin, tout responsable de traitement et tout sous-traitant se verra imposer la tenue d'un registre des activités de traitement[6]. Or, ce registre doit comporter un certain nombre d'informations qui étaient jusqu'à présent, pour l'essentiel, formalisées dans les déclarations préalables à effectuer après de la Cnil. Ce registre devra par ailleurs être mis à disposition de l'autorité de contrôle sur demande.

[5] RGPD, art.28.

[6] RGPD, art.30. S'il existe des exceptions à cette obligation de tenue d'un registre, elles sont résiduelles et doivent être interprétées restrictivement. Sur ce point, voir la leçon 4 du « RGPD en 10 leçons ».

Si les hypothèses de consultation ou de demande d'autorisation auprès de la Cnil ont vocation à être plutôt limitées, il convient toutefois d'en tenir compte mais également de ne pas sous-estimer le travail à fournir dans le cadre de l'élaboration et de la mise à jour régulière du registre des activités de traitement[7], qui implique un recensement permanent (à intégrer dans les politiques et processus internes) et une analyse des traitements mis ou ayant vocation à être mis en œuvre, plus qu'un simple « remplissage » des champs obligatoires.

*
* *

Laure Landes-Gronowski
Agil'IT
Avocate Associée
Pôle IT & Data protection

[7] Sur le registre des traitements :
voir les guidelines de la Cnil https://www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles ou encore les récentes recommandations de la « Cnil Belge » (Commission de la protection de la vie privée ou CPVP) https://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_06_2017_0.pdf.