Dalloz Avocats

Exercer et entreprendre

n° 3 – Mars 2018

Dossier

RGPD

entre risque et opportunité

9 782993 718032

Version numérique incluse*

DALLOZ

Comment piloter la mise en conformité RGPD ? Quelques lignes directrices

Par

Géraldine Péronne
Avocat, Cabinet Vigo, membre du réseau GESICA

et

Emmanuel Daoud
Avocat associé, Cabinet Vigo, membre du réseau, Docteur en droit GESICA

Seul celui qui aurait vécu dans une tour d'ivoire pendant plusieurs mois pourrait avoir échappé à l'agitation entourant l'entrée en application du Règlement général sur la protection des données[1], dit « RGPD », tant les messages incitant à la mise en conformité se sont multipliés.

Jamais la conformité n'a été aussi encensée et les promesses d'accompagnement des entreprises aussi nombreuses, le bourgeonnement de sociétés de consultants alliant des compétences juridiques et techniques venant occuper un marché que de nombreux professionnels du droit cherchent eux aussi à conquérir[2]. Néanmoins, il convient sans doute de relativiser l'importance du changement opéré par le RGPD, qui est moins juridique que culturel. Le règlement européen est certes un instrument nouveau mais les grands principes du droit des données à caractère personnel datent de la loi de 1978 et sont réitérés dans le nouvel instrument européen[3]. S'il n'y a donc pas de véritable révolution, on observe en revanche un changement de paradigme. Il se manifeste par une prise de conscience plus aiguë, d'une part, des problématiques liées aux données à caractère personnel, qui s'explique en grande partie par des niveaux de sanction rehaussés et, d'autre part, de la nécessité d'un investissement financier et humain, à la hauteur des enjeux.

Les données imprègnent toutes les organisations, qu'il s'agisse de sociétés cotées, de petites et moyennes entreprises (PME), de collectivités territoriales, d'associations, et concernent de multiples acteurs, qu'ils soient salariés, sous-traitants ou clients, de sorte que la mise en œuvre du RGPD est susceptible de toucher tout un chacun. Or, bien que long et détaillé dans ses dispositions, le règlement européen ne prévoit aucun plan d'action clés en main. Ainsi, pour les organisations qui prendraient le train en marche et auraient jusqu'à présent fait peu de cas de la loi de 1978, le chantier de la mise en conformité pourrait s'assimiler aux douze travaux d'Hercule. Pour les autres, il convient de réduire l'écart entre ce qui a déjà été fait et

1 Règl. UE n° 2016/679 du Parlement européen et du Conseil, 27 avr. 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (texte présentant de l'intérêt pour l'EEE).

2 Outre les avocats, on observera que les huissiers proposent également d'assurer des fonctions de DPO externe, www.huissier-justice.fr.

3 En ce sens, V. l'interview d'I. Falque-Pierrotin, Dalloz IP/IT, 2018 4

les nouveautés du RGPD. Il importe donc de savoir piloter un plan de mise en conformité, qui soit adapté à l'entreprise ou l'organisation visée. L'avocat, doté de l'expertise nécessaire, qui est par sa profession tenu au secret et apte à délivrer des recommandations juridiques personnalisées, est très bien placé pour accompagner son client sur le chemin de la *compliance*.

Les programmes de mise en conformité pullulent aujourd'hui et sont parfois même très détaillés. Or, il paraît délicat de déterminer, dans l'absolu, un programme précis. La feuille de route que nous proposons présente les grandes étapes indispensables et décline, pour chacune d'entre elles, dans une perspective très pratique, les objectifs, les moyens et les outils utiles[4]. Quelle que soit la méthodologie retenue, il semble nécessaire de passer par cinq étapes : l'état des lieux, l'analyse de risques, le plan d'action, la mise en conformité et le suivi, qui se répartissent aisément en deux grandes phases : l'analyse et l'action.

L'ANALYSE

La première étape du pilotage de la mise en conformité doit être celle d'un diagnostic général de l'organisation concernée, qui consiste en un état des lieux assez factuel dans un premier temps, puis en une analyse plus critique, consistant en une cartographie des risques.

Dresser un état des lieux

L'objectif

L'état des lieux doit permettre d'identifier le niveau de conformité ou le niveau de maturité de l'organisation afin de mesurer la longueur du chemin à parcourir, ainsi que les éventuelles particularités dans les traitements de données afin d'identifier immédiatement les points de vigilance.

Les moyens

Plus qu'une cartographie des traitements, l'état des lieux doit permettre d'avoir une compréhension globale de l'organisation concernée et de fixer le périmètre de la mise en conformité (les entités juridiques concernées, le champ d'application territorial, notamment). Il convient d'identifier les personnes référentes en matière de données à caractère personnel au sein de l'organisation ainsi que les opérationnels qui traitent des données à caractère personnel, de manière à pouvoir les associer au processus de mise en conformité. L'activité principale de l'organisation permettra de déterminer les grandes catégories de données traitées. S'il s'agit d'une compagnie d'assurances, il est évident que les données de santé traitées devront faire l'objet de mesures de sécurité particulières.

En outre, il ne faut pas perdre de vue que les données ont une dimension interne, s'agissant des données des salariés, et externe, s'agissant des données de clients ainsi que celles des clients des clients, qu'il faudra également inclure dans le champ de l'analyse. Les flux de données vers d'éventuels sous-traitants et hors Union européenne font également partie du périmètre de l'analyse et il convient de les identifier.

Les supports des données doivent également être répertoriés (serveurs de l'entreprise, *cloud*, site Internet, questionnaires, formulaires, etc.) de manière à analyser les contrats sous-jacents et en particulier les clauses relatives à la protection des données.

Les outils et ressources

À ce stade de l'analyse, les outils utiles sont le registre, s'il existe, l'audit, ainsi qu'une cartographie des systèmes d'information, qui permettront de dresser une cartographie des traitements de données et une vigilance sur des points d'attention spécifiques tels que les données sensibles et les transferts hors Union européenne.

Le cœur du travail va résider dans l'analyse des risques posés par les traitements de données, qui devra déterminer leur sensibilité, mais aussi les carences et les points de non-conformité.

Les mesures organisationnelles qui peuvent être mises en place pourront consister en l'instauration de comités internes réunissant les compétences opérationnelles clés, notamment directions des services d'information (DSI), ressources humaines (RH), juridique, marketing/communication, accompagnées du correspondant informatique et libertés (CIL)/ *Data Protection Officer* (DPO). En l'absence de CIL/DPO, la question d'en nommer un doit se poser rapidement afin qu'il puisse, le cas échéant, être associé au processus de mise en conformité. Sa désignation est, en toute hypothèse, fortement recommandée

[4] Un pilotage idéal de la conformité ne peut être que le fruit d'une analyse personnalisée de l'organisation concernée. La présente contribution trace les grandes lignes d'un programme de conformité qui peuvent guider à la réalisation de ce dernier, sans prétention à l'exhaustivité. Pour d'autres exemples de lignes directrices, V. not. F. Natalski, « Feuille de route : les incontournables », JA 2018, n° 571, p. 22

compte tenu des enjeux financiers et de la sophistication du droit des données à caractère personnel qui requiert le regard d'un spécialiste.

Analyser les risques posés par les traitements de données

Les objectifs

Une fois l'état des lieux dressé, le cœur du travail va résider dans l'analyse des risques posés par les traitements de données, qui devra déterminer leur sensibilité, mais aussi les carences et les points de non-conformité. À cet égard, il convient de ne pas confondre le risque encouru par l'organisation qui ne respecterait pas une disposition du règlement et le risque que l'organisation fait peser sur les personnes concernées en raison du traitement de leurs données. Bien que les deux types de risques soient intimement liés, l'analyse des risques telle qu'elle est envisagée dans ce paragraphe vise plus précisément la seconde hypothèse[5]. Cette analyse des risques repose sur plusieurs dispositions du règlement européen et notamment sur le considérant 76 aux termes duquel « il convient de déterminer la probabilité et la gravité du risque pour les droits et libertés de la personne concernée en fonction de la nature, de la portée, du contexte et des finalités du traitement. Le risque devrait faire l'objet d'une évaluation objective permettant de déterminer si les opérations de traitement des données comportent un risque ou un risque élevé »[6].

La difficulté de l'élaboration d'un plan d'action réside dans la hiérarchisation des priorités qui sera vraisemblablement le résultat d'arbitrages autant juridiques que budgétaires.

L'article 24 du RGPD sur la responsabilité du responsable de traitement prévoit que ce dernier met en œuvre des mesures techniques et organisationnelles appropriées « compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques ».

Deux types d'analyses de risques se dessinent : une première analyse *prima facie* des risques qui doit permettre une cotation de tous les risques et une seconde, sur la base de la première, qui se focalise sur les traitements susceptibles d'engendrer des risques graves. Ces derniers doivent alors faire l'objet d'une analyse d'impact qui constitue une analyse de risques plus approfondie.

Les moyens

Il s'infère des dispositions du règlement que l'analyse du risque doit se faire à l'aune d'un certain nombre de paramètres : la nature, le contexte, la portée et la finalité du traitement[7]. Néanmoins, il ne peut s'agir des seuls critères. Une cartographie des risques comporte nécessairement d'autres paramètres tels que l'identification du risque, la source du risque, les mesures existantes pour contrer ou limiter ce risque ainsi que les mesures correctives qui pourraient être adoptées afin de circonscrire le risque de manière plus appropriée ou plus efficace.

À cela s'ajoute aussi une « évaluation objective du risque »[8], qui consiste en une cotation du risque. Celle-ci se fait traditionnellement selon deux critères : d'une part, la vraisemblance du risque et d'autre part, la gravité, évalués chacun sur une échelle de 1 à 4. Une présentation graphique du résultat obtenu sous forme de diagramme permet d'obtenir une image globale du risque au sein d'une organisation.

Les outils et ressources

De nombreux outils logiciels existent afin de modéliser le risque. Un tableau Excel peut également être utilisé afin de dresser cette cartographie des risques.

L'ACTION

Les constats et analyses ayant été effectués, le diagnostic ayant été posé, il s'agit à présent d'organiser les actions à mener par le biais d'un plan d'action, de mettre en musique les actions décidées et de poser les jalons d'une conformité durable.

Établir un plan d'action

Les objectifs

Sur la base de l'analyse des risques établie, il conviendra de déterminer les actions à mener afin de mettre l'organisation concernée en conformité, d'identifier les personnes en charge de ces actions et de fixer le délai pour y parvenir.

5 Sur cette distinction, V F. Mattatia et F Mordelet, « La mise en œuvre du RGPD au prisme du risque juridique », RLDI, n° 140 août 2017
6 V. égal. cons. 74 à 77
7 RGPD cons. 76
8 *Ibid*

Les moyens

La difficulté de l'élaboration d'un plan d'action réside dans la hiérarchisation des priorités qui sera vraisemblablement le résultat d'arbitrages autant juridiques que budgétaires. De toute évidence, les traitements de données présentant les niveaux de risques les plus élevés pour les droits et libertés des personnes concernées, au terme de la cartographie des risques, devront être analysés en premier et les mesures correctives prises le plus rapidement possible. Toutefois, cette approche se conjuguera probablement avec une prise en considération des points de non-conformité susceptibles de conduire l'organisation à se voir infliger les sanctions administratives les plus élevées ou de l'exposer à un risque pénal ou réputationnel inacceptable[9].

Pour mémoire, le RGPD prévoit deux niveaux de sanctions qui sont fonction des violations constatées[10]. Ces niveaux de sanctions peuvent ne pas coïncider avec le niveau de risque identifié dans le cadre de la cartographie des risques. Ainsi ne faut-il pas sous-estimer, par exemple, les principes de limitation des finalités, de minimisation des données et d'exactitude, qui figurent à l'article 5 du règlement et dont la violation fait encourir les plus hauts niveaux de sanction, alors même que le risque pour la personne concernée peut être difficile à appréhender au stade de la cartographie des risques.

Comme évoqué précédemment, la première analyse de risques réalisée doit aussi mettre en évidence l'existence de risques élevés pour les droits et libertés des personnes concernées, nécessitant une analyse d'impact. Celle-ci devra nécessairement se faire avec l'appui du DPO, s'il y en a un. À titre d'exemple, une collecte de données de clients à grande échelle qui aurait pour finalité de procéder à du profilage devrait faire l'objet d'une analyse d'impact[11]. Outre les risques résultant des traitements, il convient d'instaurer de nouvelles procédures spécifiquement prévues par le RGPD.

S'agissant des droits des personnes, le règlement ajoute un droit à la portabilité, un droit de limitation du traitement, consacre le droit à l'oubli et encadre dans un délai plus strict la réponse que doit apporter l'organisation visée dans le cadre d'une demande de droit d'accès[12]. Il faut alors s'assurer qu'une procédure interne existe ou la créer et s'assurer qu'elle est conforme au RGPD.

Le règlement européen introduit encore une nouveauté qui consiste en l'obligation de protéger les données dès la conception (*privacy by design*) et par défaut (*privacy by default*). La mise en œuvre de ces principes nécessite également l'instauration de procédures, notamment dans le cadre du développement de projets informatiques, afin de s'assurer que seules les données à caractère personnel utiles et nécessaires sont collectées, par exemple. Autre innovation, le règlement européen généralise l'obligation de notification des violations de données à l'autorité de contrôle et, le cas échéant, aux personnes concernées. Ici encore, il faut l'anticiper et prévoir les modalités techniques et organisationnelles de gestion de ces notifications.

Enfin, le règlement impose un encadrement contractuel très précis des relations entre le responsable de traitement et le sous-traitant. Il s'ensuit une obligation de révision des contrats passés avec les fournisseurs et prestataires, qui seraient des sous-traitants au sens du RGPD, afin de convenir d'avenants.

Outre le registre, deux autres documents paraissent essentiels afin de s'assurer de la conformité des traitements et respecter les obligations découlant du principe de responsabilisation : la politique de sécurité des systèmes d'information et la politique de protection des données, dont il appartiendra à l'organisation de se doter.

Les outils et ressources

La hiérarchisation des priorités doit nécessairement passer par une concertation entre différents acteurs, le responsable de traitement, le DPO s'il y en a un, le service juridique, le RSI/DSI, notamment.

Plusieurs organisations professionnelles ont mis au point des *checklists* très détaillées permettant de s'assurer que tous les aspects du RGPD sont couverts par le programme de mise en conformité[13].

Mettre en conformité

Les objectifs

Une fois le plan d'action établi, il faut le mettre en musique. Il s'agit donc de corriger les points de non-conformité, d'actualiser les mentions, d'instaurer des procédures, etc. Ce paragraphe est né-

9 V. F. Mattatia et F. Mordelet, préc.
10 RGPD, art. 83.4 et 83.5.
11 Le RGPD prévoit que l'autorité de contrôle peut établir et publier une liste des types d'opérations de traitement pour lesquels une telle analyse est requise (art. 35). La CNIL a annoncé l'actualisation de son guide sur l'analyse d'impact, qui devrait permettre d'identifier plus précisément les traitements de données concernés.
12 RGPD, art. 12.3.
13 V. not. « Données personnelles et systèmes d'information – Entreprises, les clés d'une application réussie du GDPR », AFAI, CIGREF, TECH'IN, nov. 2017.

cessairement peu détaillé car les actions à mettre en œuvre dépendront de chaque organisation et de son degré de maturité. À cet égard, l'avocat reste l'interlocuteur privilégié pour formuler des recommandations juridiques adaptées.

Les moyens

Le règlement européen met l'accent sur la responsabilisation des acteurs et au premier chef le responsable de traitement. Cela suppose de s'assurer de pouvoir démontrer *a posteriori* la conformité des pratiques et des procédures et, partant, de documenter les actions entreprises [14].

La mise en place opérationnelle est indéniablement l'étape la plus délicate puisqu'elle va se heurter à des considérations très pratiques. Dans ces conditions, il importe de comprendre que la mise en conformité n'est pas l'affaire d'une seule femme ou d'un seul homme mais le fruit d'une concertation entre différents acteurs. Il conviendra pour chaque action d'opérer une répartition des tâches et une coordination des efforts [15]. À titre d'exemple, la réalisation d'une analyse d'impact fera intervenir le responsable de traitement, le délégué à la protection des données, mais aussi le sous-traitant, le cas échéant, les personnes concernées, ainsi que la DSI [16].

Les outils et ressources

Le registre des traitements de données doit être mis à jour à l'aune des actions de conformité mises en œuvre. À cet égard, on signalera la multiplication des solutions logicielles qui permettent de constituer et d'actualiser aisément un registre. Outre le registre, deux autres documents paraissent essentiels afin de s'assurer de la conformité des traitements et respecter les obligations découlant du principe de responsabilisation : la politique de sécurité des systèmes d'information et la politique de protection des données, dont il appartiendra à l'organisation de se doter.

On signalera la création par la Commission nationale de l'informatique et des libertés (CNIL) d'un logiciel libre d'aide à la réalisation d'études d'impact qui permet de se familiariser avec la méthodologie requise pour une telle étude.

Assurer le suivi

Les objectifs

Une dernière étape du pilotage de la conformité est souvent occultée ou un peu négligée, il s'agit du suivi de la mise en conformité. De fait, la conformité est un processus continu. Lorsque les actions du programme de conformité ont toutes été réalisées, encore faut-il les actualiser et s'assurer que les recommandations sont suivies.

Cette obligation d'examen continu découle explicitement du règlement européen qui prévoit que les mesures techniques et organisationnelles qui permettent de s'assurer et de démontrer la conformité des traitements sont « réexaminées et actualisées si nécessaire » [17]. À titre d'exemple, l'analyse d'impact devra nécessairement être mise à jour en fonction des événements affectant le traitement de données concerné [18].

Les moyens

Afin de s'assurer de la conformité sur le long terme, il sera utile de procéder à des contrôles ainsi qu'à des audits, internes ou externes.

Les équipes en contact avec les données à caractère personnel devront également faire l'objet de formations ou de sensibilisations régulières de manière à perpétuer les bonnes pratiques.

Les outils et ressources

Le délégué à la protection des données joue un rôle crucial dans le suivi de la conformité. En vertu de ses fonctions, il est le gardien de la bonne application du règlement tout au long de l'exercice de sa mission. Dans le cadre de son obligation de sensibilisation, il pourra par exemple animer des sessions de formation, des ateliers, mettre à disposition des opérationnels des fiches pratiques. Les modalités de sensibilisation peuvent être variées [19].

Il est en principe associé à toutes les questions relatives à la protection des données au sein de son organisation et doit entretenir ses connaissances. Une veille juridique sera impérative afin de maîtriser les évolutions des textes, à commencer par la nouvelle mouture de la loi Informatique et Libertés ainsi que les interprétations prétoriennes qui en découleront. L'adhésion à une association de professionnels ou à des groupes de réflexion spécialisés en matière de protection des données à caractère personnel pourra être d'une aide précieuse [20]. En définitive, il semble important de garder à l'esprit le caractère continu du processus de conformité. D'une part, la mise en conformité ne se réalisera pas en un trait de temps, rien ne sert donc de courir après un résultat parfait à court terme. D'autre part, elle n'est pas un état de fait statique mais le fruit d'efforts constants, en d'autres termes, l'émulation générée par le RGPD devra s'inscrire dans la durée.

14 RGPD art. 5.2.
15 M. Bourgeois, F. Régnier-Pécastaing et O. Pélanchon, « RGPD : les bonnes résolutions 2018 ! », JCP E 2018, 1036.
16 Cette concertation collective est explicitement dictée par l'article 35 du RGPD.
17 RGPD, art. 24.1.
18 RGPD, art. 35.11 : « Si nécessaire, le responsable du traitement procède à un examen afin d'évaluer si le traitement est effectué conformément à l'analyse d'impact relative à la protection des données, au moins quand il se produit une modification du risque présenté par les opérations de traitement ».
19 V. not. G. Desgens-Pasanau, « Formation et sensibilisation des nouveaux acteurs : quelles solutions ? », JA 2018, n° 571, p. 27.
20 En ce sens, V. M.-L. Baron, « Données personnelles et collectivités », AJCT 2017, 27.