



Le RGPD, mise en conformité en moins de 100 jours ... c'est encore possible !

Sommaire

1. Le RGPD en quelques maux	2
2. Chantier n°1 – Cartographie juridique	3
3. Chantier n°2 – Registre du traitement	4
4. Chantier n°3 – Sous-traitance	5
5. Chantier n°4 – Information et transparence	6
6. Chantier n°5 – Protection by design et by default	7
7. Chantier n°6 – Sécurisation des données	8
8. Chantier n°7 – Transferts hors de l'Union Européenne	8
9. Chantier n°8 – Formation et sensibilisation	9
10. Chantier n°9 – La question du délégué à la protection des données (« DPO »)	10
11. Chantier n°10 – La question de l'analyse d'impact (PIA)	11
12. Conclusion	12

D'après le site archimag.com, à moins de 100 jours de l'entrée en vigueur du RGPD, près d'un tiers des entreprises françaises se disent préoccupées par leur capacité à être conforme au futur règlement européen sur la protection des données personnelles. A ce chiffre s'ajoutent les nombreux acteurs publics qui sont tenus de désigner un délégué à la protection des données à caractère personnel.

Pour préparer une mise en conformité plus sereine, voici quelques clefs pour aborder les principaux chantiers.

1. Le RGPD en quelques maux

Le règlement général sur la protection des données (ci-après appelé « RGPD¹ »), entré en vigueur le 24 mai 2016 et dont la mise en œuvre est fixée au 25 mai 2018, va profondément modifier le droit des données à caractère personnel tel que nous le connaissons aujourd'hui. Le RGPD, s'il allège certaines formalités (telles que les déclarations ou les autorisations), renforce considérablement le droit des personnes mais aussi les obligations des entreprises et des acteurs publics vis-à-vis de la protection des données, de même que les sanctions applicables.

L'incidence du RGPD est d'autant plus grande qu'elle repose sur le principe d'« accountability »

Au titre de ce nouveau principe, c'est désormais à l'entreprise ou à l'acteur public de démontrer à l'autorité de contrôle (la « CNIL ») qu'il ou elle est bien conforme aux obligations du RGPD.

Il s'agit donc d'un renversement complet de la charge de la preuve.

Le risque de ne pas respecter le RGPD est de quatre ordres :

- Risque 1 – Sanction financière qui se décline elle-même en deux points :
 - une sanction administrative, prononcée par l'autorité de contrôle, pouvant atteindre jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial ;
 - une réparation du préjudice, sachant que des actions de groupe pourront être menées sur ce terrain.
- Risque 2 – Risque en termes d'image notamment quand il s'agira des premières condamnations rendues après l'entrée en vigueur du RGPD ;
- Risque 3 – Risque de suspension ou de limitation des conditions d'utilisation d'un traitement qui sera considéré comme non conforme au RGPD.
- Risque 4 – Risque de condamnation pénal dans les cas les plus extrêmes.

Face à de tels risques, aucune entreprise ni aucun acteur public ne peut faire fi des nouvelles obligations fixées par le RGPD.

¹ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 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

Son impact sur les entreprises ou les entités publiques est important car il ne s'agit pas d'un « simple » texte de loi à mettre en œuvre.

Le RGPD représente un véritable projet d'entreprise qui implique toutes les directions et ce, bien au-delà de la seule direction juridique ou de la seule direction des systèmes d'information.

Sa mise en œuvre nécessite notamment une impulsion au plus haut niveau de l'entreprise, la désignation d'un « sponsor », la mobilisation d'une équipe projet et des moyens aussi bien techniques que financiers.

Aussi, en tant que projet, la mise en conformité au RGPD impose la structuration de nombreux chantiers, qu'ils soient, juridiques, organisationnels ou techniques.

L'impact est encore plus important pour les acteurs publics qui sont tenus de désigner un délégué à la protection des données (« DPD » ou « DPO » en anglais). Le DPO ayant notamment pour tâche de contrôler l'application du RGPD, leur conformité devra être exemplaire.

L'ensemble du RGPD, en ce compris ses 99 articles et ses 173 considérants, doit être respecté. Néanmoins, il est possible d'identifier plusieurs chantiers prioritaires :

- la cartographie juridique ;
- le registre du traitement ;
- la sous-traitance ;
- l'information et la transparence ;
- la protection “by design” et by “default” ;
- la sécurisation des traitements ;
- les transferts hors de l'Union européenne ;
- la formation et la sensibilisation ;

Par ailleurs deux questions se posent, l'une autour de la désignation ou non d'un DPO et l'autre autour de l'analyse d'impact.

2. Chantier n°1 – Cartographie juridique

2.1 Descriptif

La cartographie juridique est le socle de la démarche de mise en conformité au RGPD.

La mise en œuvre d'une cartographie juridique ne constitue pas une exigence posée par le règlement, mais un préalable indispensable pour :

- identifier l'ensemble des traitements connus, les personnes concernées et les données collectées ;
- lutter contre le « shadow IT », c'est-à-dire les traitements sauvages de données à caractère personnel.

Seule la réalisation de cette cartographie permet de définir une politique RGPD appropriée aux besoins de l'entreprise ou de l'acteur public.

2.2 Mise en œuvre

La cartographie juridique se distingue de la cartographie technique puisqu'il s'agit d'utiliser des outils permettant de « scanner » les systèmes d'information et d'en recenser les traitements, ou plus précisément l'existence de données à caractère personnel au sein des systèmes informatiques de l'établissement.

La cartographie juridique consiste à procéder à une analyse de la situation au regard du RGPD et de ses exigences.

Elle consiste notamment à identifier pour un traitement :

- les finalités ;
- les données concernées ;
- les personnes concernées ;
- les mesures de sécurité mises en œuvre ;
- les destinataires des données ;
- la durée de conservation...

Pour une entité privée ou publique déjà en possession d'une cartographie juridique de ses données, un réexamen à la lumière des exigences du RGPD sera essentiel.

Si une entreprise ou un acteur public a un doute sur le traitement ou l'existence de traitements cachés ("shadow IT"), ou même s'il y a simplement un souhait de mieux connaître ses données (données brutes/enrichies, données froides/chaudes, données sensibles/non-sensibles, données fraîches/périmées...), la réalisation d'une cartographie s'impose également.

La cartographie est généralement réalisée par l'intermédiaire de questionnaires d'audit spécifiques et peut être complétée d'une cartographie technique (il existe des prestataires spécialisés dans ce domaine).

3. Chantier n°2 – Registre du traitement

3.1 Descriptif

L'article 30 du RGPD impose la mise en œuvre d'un registre du traitement.

Cette obligation ne s'applique cependant pas à une entreprise ou à une personne publique comptant moins de 250 employés, sauf dans certains cas spécifiques (ex : lorsque le traitement présente un risque majeur pour les données à caractère personnel ou lorsqu'il s'agit d'un traitement de catégories de données dites « sensibles »).

Que l'entreprise ou l'acteur public soit astreint ou non à tenir un registre des traitements, cette opération s'avère essentielle au regard du RGPD, dans la mesure où elle participe au respect du principe « d'accountability ».

Par ailleurs, la tenue d'un tel registre permet d'organiser un véritable référentiel commun et un socle pour l'adoption de règles de gouvernance.

3.2 Mise en œuvre

Selon la taille de l'établissement et le nombre de traitements en cause, le registre peut nécessiter un travail avec la Direction des systèmes d'information.

Néanmoins, dans la majorité des cas, un simple tableur (sous Excel par exemple) suffit à élaborer le registre des traitements.

Dans les autres cas (choix d'une solution dédiée), il faudra veiller au 3 points suivants :

- Définition des prérequis juridiques pour sélectionner le prestataire adapté
- Analyse des offres et des solutions
- Rédaction d'un contrat approprié, notamment en cas d'offre en SaaS

4. Chantier n°3 – Sous-traitance

4.1 Descriptif

Le RGPD impose désormais au responsable de traitement de bien connaître ses sous-traitants et d'être en mesure de s'assurer qu'ils agissent de façon conforme aux exigences posées par le texte.

En témoigne son article 28 aux termes duquel :

- « Lorsqu'un traitement doit être effectué pour le compte d'un responsable du traitement, celui-ci fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée ».

La notion de sous-traitance au sens du RGPD est particulière puisqu'elle comprend toutes les situations dans lesquelles le traitement est réalisé par un prestataire extérieur.

Plusieurs exemples peuvent être appréhendés :

- des prestations de gestion de paie des salariés (ou délocalisation de tout autre service) ;
- des prestations d'hébergement ou de maintenance par des prestataires de services informatiques ;
- des prestations effectuées par les agences de marketing ou de communication dans la mesure où elles ont nécessairement accès à des données à caractère personnel.

Au cas particulier de la sous-traitance, le RGPD impose :

- l'existence d'un contrat entre le responsable de traitement et le sous-traitant ;

- un certain nombre de clauses au sein de ce même contrat ;
- des règles précises en termes de répartition de responsabilité ;
- des règles particulières sur le recours à la sous-traitance de la part des sous-traitants eux-mêmes.

4.2 Mise en œuvre

La prise en compte des nouvelles obligations en termes de sous-traitance nécessite préalablement :

- l'identification des sous-traitants qui est réalisée dans le cadre de la cartographie juridique ;
- l'identification des contrats avec lesdits sous-traitants et l'analyse de leur conformité au RGPD.

La « politique sous-traitant » impose :

- la rédaction d'une annexe contractuelle RGPD ;
- la mise en œuvre de procédures spécifiques d'audit des sous-traitants.

La première étape, urgente, consiste à interroger par courrier les sous-traitants identifiés pour vérifier leur niveau de conformité au RGPD.

5. Chantier n°4 – Information et transparence

5.1 Descriptif

Le RGPD renforce les droits des personnes concernées, parmi lesquels le droit à l'information, et met à la charge du responsable de traitement une obligation générale de transparence qui l'oblige à communiquer à la personne concernée toute information « d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples »².

Le respect de cette obligation peut notamment se matérialiser soit par la rédaction de politiques d'utilisation des données soit par la rédaction de documents qui recensent l'ensemble des informations devant être portées à la connaissance des personnes concernées. Ces documents doivent être distincts des chartes des systèmes d'information ou autres conditions générales.

Respecter cette obligation suppose que le responsable de traitement fournisse une information différenciée en fonction des différentes catégories de personnes concernées.

A ce titre, nous recommandons de rédiger :

- une politique relative aux données des salariés ou des agents pour les acteurs publics ;
- une politique relative aux données des clients et des prospects.

² RGPD, art.12

La loi Informatique et Liberté de 1978 imposait la mise en œuvre d'un certain nombre de mentions d'information obligatoires afin de recueillir le consentement de la personne concernée et de l'informer quant aux caractéristiques du traitement mis en œuvre et quant à ses droits.

Le RGPD est dans la même lignée puisqu'il s'agit d'une occasion de vérifier la conformité des entreprises et des personnes publiques aux exigences d'information des personnes concernées.

5.2 Mise en œuvre

Au titre de ce chantier il convient d'adopter :

- une politique de données salariées/agents qui fixe les droits et les obligations des salariés et répond à l'exigence légale;
- une politique des données clients / prospects qui fixe pour sa part les droits et obligations des clients et prospects qui constituent un document critique pour l'entreprise.

Les deux documents constituent en partie la « politique RGPD » mais ne peuvent pas être fondus dans un seul et même document.

6. Chantier n°5 – Protection by design et by default

6.1 Descriptif

L'article 25 du RGPD impose de protéger les données dès la conception et par défaut.

La protection dès la conception (« by design ») signifie que le responsable de traitement doit, dès la création d'un traitement de données, mettre en œuvre des mesures techniques et organisationnelles appropriées destinées à protéger et sécuriser celles-ci.

S'il est vrai que le RGPD n'apporte pas de définition du caractère « approprié » des mesures, il donne des exemples de celles-ci en citant notamment la « pseudonymisation » et la minimisation des données.

La protection des données par défaut (« protection by default ») impose, quant à elle, au responsable de traitement de s'assurer que, par défaut, ne sont traitées que les données à caractère personnel nécessaires, en référence aux finalités du traitement. Cela implique notamment que l'accès à ces données soit limité à un nombre déterminé de personnes.

6.2 Mise en œuvre

La mise en œuvre de ces principes nécessite l'adoption :

- de règles de gouvernance des données ;
- de spécifications juridiques de développement ;
- d'une méthodologie d'audit interne.

Par ailleurs, même si cela n'est pas imposé, la rédaction d'un rapport annuel d'activité sur le RGPD participe au respect des exigences du RGPD.

7. Chantier n°6 – Sécurisation des données

7.1 Descriptif

L'article 32 impose la mise en œuvre de mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.

Cette sécurisation est articulée autour de 4 grandes thématiques :

- la mise en œuvre de solutions de « pseudonymisation » ou de chiffrement de données ;
- la mise en œuvre de moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- la mise en œuvre de moyens permettant de rétablir la disponibilité des données et l'accès à celle-ci dans des délais appropriés en cas d'incident physique ou technique ;
- la mise en œuvre d'une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

7.2 Mise en œuvre

La mise en œuvre s'exerce en deux axes :

- un axe juridique et organisationnel ;
- un axe technique.

L'axe technique passe généralement par la réalisation d'audits de vulnérabilité et/ou de tests intrusifs et, le cas échéant, par le déploiement de solutions logiques et/ou physiques de sécurité.

L'axe juridique porte sur les outils suivants :

- une revue juridique de la PSSI (Politique de Sécurité des Systèmes d'information), du PCA (Plan de continuité de l'activité) et du PRA (Plan de reprise de l'activité) pour tenir compte spécifiquement du risque relatif au traitement des données à caractère personnel ;
- une sensibilisation des personnels à la sécurité des systèmes d'information ;
- une anticipation des situations de violation de données à caractère personnel qui implique d'informer la Cnil et, dans certains cas, d'informer les personnes concernées elles-mêmes.

8. Chantier n°7 – Transferts hors de l'Union Européenne

8.1 Descriptif

Afin d'assurer la protection des personnes concernées dans le monde entier, le RGPD réglemente les flux transfrontiers de données à caractère personnel.

Les transferts de données sont libres entre les pays membres de l'Union européenne ou d'un état membre vers un pays situé en dehors de l'Union européenne présentant un niveau de protection considéré comme « adéquat » par l'intermédiaire d'une décision d'adéquation de la Commission européenne.

Si, à l'inverse, le pays destinataire du transfert de données n'a bénéficié d'aucune décision d'adéquation de la part de la Commission européenne, le transfert est, par principe, interdit.

Néanmoins, le transfert peut être autorisé s'il est entouré de garanties appropriées, telles que :

- un instrument juridiquement contraignant et exécutoire entre organismes publics ;
- des règles d'entreprise contraignantes (« BCR ») ;
- des clauses contractuelles types ;
- un code de conduite ou un mécanisme de certification approuvé.

Cette thématique et ces obligations imposent au responsable de traitement de prêter une attention particulière aux contrats SaaS qu'il est susceptible d'avoir conclus dans la mesure où le lieu de stockage est souvent situé hors de l'Union européenne.

8.2 Mise en œuvre

Les situations sont complexes mais peuvent être classées en deux catégories :

- adoption de BCR au sein des groupes internationaux ;
- généralisation des clauses contractuelles types dans les autres cas.

9. Chantier n°8 – Formation et sensibilisation

9.1 Descriptif

Cet impératif ne ressort pas explicitement de la lettre du RGPD. Néanmoins, la formation est sous-jacente dans la mesure où le déploiement d'actions de formation et de sensibilisation permet de s'acquitter de ses obligations d'information et de transparence.

La formation permet également de s'inscrire dans une démarche « d'accountability » en accordant une position centrale à la protection des données à caractère personnel.

Si le RGPD n'évoque pas la nécessité d'une formation en interne, la Cnil elle-même, dans son Guide relatif à la sécurité des données à caractère personnel³, en fait sa première fiche pratique, intitulée « Sensibiliser les utilisateurs »⁴.

9.2 Mise en œuvre

La formation ou la sensibilisation des équipes internes, voire des sous-traitants, peut prendre différentes formes :

- réunion présentielle ;
- séquences vidéo ;
- FAQ ou Quizz ;
- tutoriels.

10. Chantier n°9 – La question du délégué à la protection des données (« DPO »)

La question du délégué à la protection des données (« DPO ») est importante.

Aux termes de l'article 37 du RGPD, la désignation d'un DPO est obligatoire lorsque :

- le traitement est effectué par une autorité publique ou un organisme public ;
- les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ;
- les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de données sensibles.

Dans les autres cas, la désignation d'un DPO est donc facultative.

Il convient toutefois de mener une vraie réflexion sur la désignation ou non d'un DPO même en dehors des 3 cas sus visés.

La désignation d'un DPO présente deux intérêts majeurs :

- l'existence d'un DPO permet de mettre en œuvre une vraie gouvernance en matière de données à caractère personnel car le DPO est mis en avant comme un sponsor, un interlocuteur spécifique dans le domaine.
- une telle désignation participe du respect du principe de « l'accountability » car l'existence d'un DPO peut orienter la position de la Cnil en cas de contrôle éventuel. En effet, cela démontre la proactivité de l'organisme et la préoccupation qu'elle nourrit au sujet des données à caractère personnel ;

³ [Guide de la sécurité des données personnelles, site internet de la Cnil](#)

⁴ [« Sécurité : sensibiliser les utilisateurs », site internet de la Cnil](#)

La désignation d'un DPO est un chantier à part entière qui nécessite notamment :

- l'identification du DPO ;
- la désignation formelle de ce DPO ;
- l'établissement des règles de gouvernance permettant d'assembler les pouvoirs et les obligations du DPO.

11. Chantier n°10 – La question de l'analyse d'impact (PIA – Privacy Impact Assessment)

L'analyse d'impact doit être réalisée lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

Le RGPD précise que cette analyse d'impact est impérative dans les 4 cas suivants :

- l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ;
- le traitement à grande échelle de catégories particulières de données visées à l'article 9, paragraphe 1, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 ;
- la surveillance systématique à grande échelle d'une zone accessible au public ;
- les traitements désignés comme tel par la Cnil.

Sur la forme, l'analyse d'impact contient au moins :

- une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement ;
- une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;
- une évaluation des risques pour les droits et libertés des personnes concernées conformément au paragraphe 1 ;
- les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.

Le RGPD précise enfin que le responsable du traitement doit consulter l'autorité de contrôle préalablement à la mise en œuvre du traitement lorsqu'une analyse d'impact révèle que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque.

Il s'agit alors là d'une sorte de demande d'autorisation qui ne dit pas son nom.

12. Conclusion

On ne peut décemment pas parler de « conclusion » quand on parle de RGPD, il est préférable de parler de ... prologue.

Ces différents chantiers sont des « essentiels » mais ne sont qu'un prologue à une mise en conformité à 360° qui nécessitera bien plus de temps que 100 jours et devra tenir compte de l'adoption de la loi dite LIL 3 et des publications de la Cnil..

Par ailleurs le RPG se veut être un texte « actif » comme en témoigne deux éléments qui le caractérisent :

- l'itération : La conformité au RGPD n'est pas instantanée. Il s'agit au contraire d'un projet d'entreprise permanent qu'il faut revoir à période régulière pour s'assurer que les mesures techniques et organisationnelles mise en œuvre sont toujours pertinentes;
- l'audit : Le RGPD impose des audits de tel ou tel sous-traitant ou process. Là encore les obligations posées en termes d'audit imposent une démarche d'amélioration continue du process de conformité.

Auteur



Eric Barbry
Associé
ebarbry@racine.eu