Focus #3 - Codes de conduite, labels et certifications

Avril 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.

Le RGPD[1] introduit la notion d'*accountability*[2]. L'accountability désigne l'obligation pour les entreprises de mettre en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer que les traitements des données à caractère personnel sont effectués conformément au règlement, et être en mesure de le démontrer.

Aussi, l'accountability implique la mise en place d'une véritable gouvernance des données, et notamment :

- **de déployer un processus permanent et dynamique de mise en conformité** de son entreprise à la réglementation « Informatique et libertés », notamment grâce à un ensemble de règles contraignantes, d'outils et de bonnes pratiques correspondantes ;

[1] http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679&from=FR
[2] Sur la notion d'accountability, voir la leçon 4 du « RGPD en 10 leçons ».

- **d'apporter la preuve que les mesures appropriées ont été prises** (cf. mécanisme permettant de démontrer l'efficacité et l'effectivité des mesures prises) : en pratique, les entreprises vont devoir faire et être en mesure de prouver, de tracer, ce qui a été fait ;

- **d'auditer les mesures prises dans le cadre d'un contrôle continu**, pour d'une part, vérifier l'efficacité desdites mesures et d'autre part, les actualiser le cas échéant pour assurer leur maintien en conformité au règlement au regard de l'évolution des traitements, de leurs finalités, des exigences réglementaires ou tout simplement du retour d'expérience.

Mais le Règlement ne se contente pas de créer de nouvelles notions et obligations puisqu'il prévoit de nouvelles méthodologies à destination des responsables de traitements et des sous-traitants pour démontrer la conformité de certains aspects de leurs traitements et le respect de certaines de leurs obligations respectives. Ces méthodologies peuvent notamment prendre la forme de « codes de bonne conduite », de « certifications » ou encore de « labels » (articles 40 à 43 du RGPD).

L'adhésion à de tels codes de conduite ou encore l'obtention de certifications ou de labels seront un atout pour les organismes mettant en œuvre des traitements de données à caractère personnel en vue de la démonstration éventuelle du respect de leurs obligations.

En effet, l'article 24 du RGPD précise que « *l'application d'un code de conduite approuvé comme le prévoit l'article 40 ou de mécanismes de certification approuvés comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des obligations incombant au responsable du traitement* ».

La mise en œuvre d'actions conformes à ces codes de bonne conduite, certifications ou labels pourra également être prise en compte par l'autorité de contrôle en cas de procédure contentieuse.

En effet, l'article 83 du RGPD précise qu'il convient, pour la détermination des sanctions pouvant éventuellement être prononcées, de tenir compte notamment de la nature, de la gravité et de la durée de la violation, du caractère intentionnel de la violation et des mesures prises pour atténuer le dommage subi, du degré de responsabilité ou de toute violation pertinente commise précédemment, de la manière dont l'autorité de contrôle a eu connaissance de la violation, du respect des mesures ordonnées à l'encontre du responsable du traitement ou du sous-traitant**,** mais encore de l'application d'un code de conduite ou d'un mécanisme de certification, et de toute autre circonstance aggravante ou atténuante.

Nota : Le recours à de tels mécanismes ne doit en tout état de cause pas être négligé car **il procurera en outre aux organismes concernés un avantage concurrentiel et compétitif à l'égard de l'ensemble de leur écosystème** (clients, fournisseurs, partenaires, prestataires,…), et ce d'autant que le RGPD encourage le déploiement de ces « instruments de la conformité ».

Les codes de conduite (**1**), labels et certifications (**2**) sont donc des outils précieux pour les responsables de traitements et sous-traitants dans le cadre de leur mise et de leur maintien en conformité opérationnelle aux dispositions issues du RGPD en matière de protection des données à caractère personnel.

1. Les codes de conduite

Les codes de conduite sont encadrés par les articles 40 et 41 du RGPD. Ils peuvent être élaborés par des « ***associations et autres organismes représentant des catégories*** *de responsables de traitement ou de sous-traitants* ».

Ces codes devront notamment avoir pour objectif de préciser les modalités d'applications du RGPD, **compte tenu de la spécificité des différents secteurs de traitement et des besoins spécifiques des micros, petites et moyennes entreprises**, plus particulièrement s'agissant des thématiques suivantes :

- le traitement loyal et transparent ;
- les intérêts légitimes poursuivis par les responsables du traitement dans des contextes spécifiques;
- la collecte des données à caractère personnel;
- la pseudonymisation des données à caractère personnel;
- les informations communiquées au public et aux personnes concernées;
- l'exercice des droits des personnes concernées;
- les informations communiquées aux enfants et la protection dont bénéficient les enfants et la manière d'obtenir le consentement des titulaires de la responsabilité parentale à l'égard de l'enfant;
- les mesures techniques et organisationnelles, ainsi que les procédures visées au RGPD devant être déployées pour le respect des principes d'accountability, de privacy by design et de privacy by default, ainsi que les mesures visant à assurer la sécurité du traitement ;
- la notification aux autorités de contrôle des violations de données à caractère personnel et la communication de ces violations aux personnes concernées;
- le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales; ou
- les procédures extrajudiciaires et autres procédures de règlement des litiges permettant de résoudre les litiges entre les responsables du traitement et les personnes concernées en ce qui concerne le traitement.

Les projets de codes de conduite devront être **présentés pour approbation** à l'autorité nationale de contrôle (ou à la Commission européenne après avis du comité européen de la protection des données si le code de conduite concerne des activités de traitement menées dans plusieurs Etats membres), qui vérifiera si le projet de code présente des garanties appropriées suffisantes en vue du respect du RGPD.

Une fois approuvés, ces codes de conduite seront **enregistrés et rendus publics** et pourront même, sur décision de la Commission, être considérés comme d'application générale au sein de l'Union.

Par ailleurs, outre leur application par les responsables de traitements ou les sous-traitants soumis au RGPD, les codes de conduite qui seront approuvés et d'application générale pourront aussi être appliqués par des responsables de traitements ou des sous-traitants qui ne sont pas soumis au RGPD, afin de fournir des garanties appropriées dans le cadre de transferts de données à caractère personnel vers un pays tiers ou une organisation internationale par exemple. Ces responsables de traitements ou sous-traitants devront alors à cette fin prendre l'engagement contraignant et doté de force obligatoire, au moyen d'instruments contractuels ou d'autres instruments juridiquement contraignants, d'appliquer ces garanties appropriées, y compris en ce qui concerne les droits des personnes concernées.

Enfin, sans préjudice des pouvoir de l'autorité de contrôle compétente, le contrôle du respect du code de conduite pourra être effectué par un organisme disposant d'un niveau d'expertise approprié au regard de l'objet du code et qui sera agréé à cette fin par l'autorité de contrôle compétente. Cet organisme agrée pourra prendre « *sous réserve des garanties appropriées, des mesures appropriées en cas de violation du code par un responsable du traitement ou un sous-traitant, et [pourra] notamment suspendre ou exclure le responsable du traitement ou le sous-traitant concerné de l'application du code. Il informe[ra] l'autorité de contrôle compétente de ces mesures et des raisons pour lesquelles elles ont été prises*. ».

2. Les certifications et labels

Les mécanismes de certification et de labels sont prévus aux articles 42 et 43 du RGPD et ont vocation en particulier à être des outils qui permettront de « *démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent le […] règlement* », **les besoins spécifiques des micros, petites et moyennes entreprises devant dans ce cadre être pris en considération**.

Ces mécanismes devront être **volontaires et accessibles via un processus transparent**.

Outre leur application par les responsables de traitements ou les sous-traitants soumis au RGPD, les mécanismes de certification ou les labels approuvés en matière de protection des données pourront être établis aux fins de démontrer que des responsables de traitements ou des sous-traitants qui ne sont pas soumis au RGPD fournissent des garanties appropriées dans le cadre de transferts de données à caractère personnel vers un pays tiers ou une organisation internationale par exemple. Ces responsables de traitements ou sous-traitants devront à cette fin prendre l'engagement contraignant et exécutoire, au moyen d'instruments contractuels ou d'autres instruments juridiquement contraignants, d'appliquer ces garanties appropriées, y compris en ce qui concerne les droits des personnes concernées.

Nota : une certification ou un label ne diminue pas la responsabilité du responsable du traitement ou du sous-traitant quant au respect du présent règlement et est sans préjudice des missions et des pouvoirs des autorités de contrôle.

Les certifications ou labels pourront être délivrés :

- **par un organisme de certification disposant d'un niveau d'expertise approprié en matière de protection des données ou par l'autorité de contrôle compétente** sur la base de critères approuvés par cette autorité de contrôle ou par le comité européen de la protection des données ;

- **après transmission à ces organismes**, par le responsable de traitements ou le sous-traitant qui soumet ses traitements à un tel mécanisme, de toutes les informations relatives au traitement et communication d'un accès à ses activités de traitement (opérations nécessaires pour mener la procédure de certification) ;

- **pour une durée maximale de trois années**, et pourront être renouvelés dans les mêmes conditions si les exigences continuent d'être satisfaites. Les organismes précités peuvent toutefois choisir de retirer la certification ou le label si les exigences s'y rapportant ne sont plus remplies.

De la même manière que pour les codes de conduite, l'organisme certifié devra se conformer aux exigences prévues dans la certification, sous peine de se voir retirer ladite certification.

*
* *

Les codes de bonne conduite, labels et certifications peuvent donc être considérés comme des moyens qui seront à disposition des responsables de traitements et sous-traitants pour leur permettre de démontrer la conformité de leurs traitements en matière de protection des données à caractère personnel, *a minima* pour certaines de leurs obligations à ce titre.

Le Règlement prévoit divers cas de mise en œuvre de ces nouvelles mesures (sécurité, transfert des données etc.).

Le tableau ci-après synthétise les aspects du Règlement susceptibles de faire l'objet d'une certification, d'un label ou d'un code de conduite, les articles du RGPD qui y font référence, ainsi que les outils existants ou à venir en la matière.

S'agissant des outils, il est précisé que sont listés dans le tableau ci-dessous les normes existantes et à venir, mais également de manière plus large les outils qui peuvent et pourront être utilisés par les responsables de traitements et sous-traitants dans le cadre de leur mise et de leur maintien en conformité aux obligations qui leur incombent en matière de protection des données à caractère personnel. Par ailleurs, ces outils sont rattachés « artificiellement » à une ou plusieurs thématiques dans le tableau ci-dessous en fonction du lien le plus pertinent mais peuvent bien entendu pour certains d'entre eux s'appliquer à plusieurs thématiques, notamment pour ce qui concerne les thématiques transverses.

Thématique	Disposition du RGPD	Commentaire	Outils existants et à venir
Responsabilité du responsable de traitements	**Article 24 : Responsabilité du responsable du traitement** « 1. 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, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement. Ces mesures sont réexaminées et actualisées si nécessaire. 2. Lorsque cela est proportionné au regard des activités de traitement, les mesures visées au paragraphe 1 comprennent la mise en œuvre de **politiques appropriées** en matière de protection des données par le responsable du traitement. **3. L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou de mécanismes de certification approuvés comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des obligations incombant au responsable du traitement. »**	Le responsable de traitements devra mettre en œuvre des mesures techniques et organisationnelles appropriées pour garantir la conformité de son traitement de données à caractère personnel. Selon les termes du RGPD, il pourra disposer d'outils visant à lui permettre de démontrer qu'il respecte les obligations lui incombant (*a minima* certaines d'entre elles). Ces outils pourront notamment prendre la forme de codes de conduite ou de mécanismes de certification.	Label Cnil « Procédure de gouvernance Informatique et libertés » Label Cnil « Procédure d'audit » Terminologie et principes : Privacy framework (ISO/IEC 29100) Communication de la CNIL : « Règlement européen : Les 6 étapes pour se préparer » **A venir :** Code of practice for personally identifiable information protection (ISO/IEC 29151) Certifications Bureau Veritas : « Privacy checked / privacy by design », « Gouvernance » et « RGPD »
Responsabilité du sous-traitant	**Considérant 81** « 81. Afin que les exigences du présent règlement soient respectées dans le cadre d'un traitement réalisé par un sous-traitant pour le compte du responsable du traitement, lorsque ce	Le sous-traitant voit sa responsabilité renforcée par le RGPD en matière de protection des données à caractère personnel.	Label Cnil « Procédure de gouvernance Informatique et libertés » Label Cnil « Procédure d'audit »

Thématique	Disposition du RGPD	Commentaire	Outils existants et à venir
	dernier confie des activités de traitement à un sous-traitant, le responsable du traitement ne devrait faire appel qu'à des sous-traitants présentant des garanties suffisantes, notamment en termes de connaissances spécialisées, de fiabilité et de ressources, pour la mise en œuvre de mesures techniques et organisationnelles qui satisferont aux exigences du présent règlement, y compris en matière de sécurité du traitement. **L'application par un sous-traitant d'un code de conduite approuvé ou d'un mécanisme de certification approuvé peut servir à démontrer le respect des obligations incombant au responsable du traitement.** La réalisation d'un traitement par un sous-traitant devrait être régie par un contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, liant le sous-traitant au responsable du traitement, définissant l'objet et la durée du traitement, la nature et les finalités du traitement, le type de données à caractère personnel et les catégories de personnes concernées, en tenant compte des tâches et responsabilités spécifiques du sous-traitant dans le cadre du traitement à effectuer et du risque pour les droits et libertés de la personne concernée. Le responsable du traitement et le sous-traitant peuvent choisir de recourir à un contrat particulier ou à des clauses contractuelles types, qui sont adoptées soit directement par la Commission soit par une autorité de contrôle conformément au mécanisme de contrôle de la cohérence, puis par la Commission. Après la réalisation du traitement pour le compte du responsable du traitement, le sous-traitant devrait, selon le choix du responsable du traitement, renvoyer ou supprimer les données à caractère personnel, à moins que le droit de l'Union ou le droit d'un État membre auquel le sous-traitant est soumis n'exige la conservation des données à caractère personnel. »	Selon les termes du RGPD, il pourra, tout comme le responsable de traitements, disposer d'outils visant à lui permettre de démontrer qu'il respecte les obligations lui incombant (*a minima* certaines d'entre elles). Ces outils pourront notamment prendre la forme de codes de conduite ou de mécanismes de certification.	Norme applicable au cloud uniquement : norme ISO 27018 Terminologie et principes : Privacy framework (ISO/IEC 29100) Méthodologie de la Cnil : « Règlement européen : les 6 étapes pour se préparer », 15-3-2017 **A venir :** Code of practice for personally identifiable information protection (ISO/IEC 29151) Certifications Bureau Veritas : « Privacy checked / privacy by design », « Gouvernance » et « RGPD »

Thématique	Disposition du RGPD	Commentaire	Outils existants et à venir
	Article 28 : Sous-traitant « 1. 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. (…) **5. L'application, par un sous-traitant, d'un code de conduite approuvé comme le prévoit l'article 40 ou d'un mécanisme de certification approuvé comme le prévoit l'article 42 peut servir d'élément pour démontrer l'existence des garanties suffisantes conformément aux paragraphes 1 et 4 du présent article.** **6. Sans préjudice d'un contrat particulier entre le responsable du traitement et le sous-traitant, le contrat ou l'autre acte juridique visé aux paragraphes 3 et 4 du présent article peut être fondé, en tout ou en partie, sur les clauses contractuelles types visées aux paragraphes 7 et 8 du présent article, y compris lorsqu'elles font partie d'une certification délivrée au responsable du traitement ou au sous-traitant en vertu des articles 42 et 43. »**		
Etude d'impact au regard de la sensibilité du traitement	**Considérants 76 et 77** « 76. 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.	Les traitements présentant une certaine sensibilité devront faire l'objet d'une étude d'impact préalablement à leur mise en œuvre. Pour mener à bien une telle étude, des codes de conduite ou mécanismes de certification entre autres pourront être	Maturité dans les processus : Privacy capability assessment model (ISO/IEC 29190) Guide de la Cnil « PIA-1, La méthode : comment mener une étude d'impact sur la vie privée », éd.2015

Thématique	Disposition du RGPD	Commentaire	Outils existants et à venir
	77. Des directives relatives à la mise en œuvre de mesures appropriées et à la démonstration par le responsable du traitement ou le sous-traitant du respect du présent règlement, notamment en ce qui concerne l'identification du risque lié au traitement, leur évaluation en termes d'origine, de nature, de probabilité et de gravité, et l'identification des meilleures pratiques visant à atténuer le risque, pourraient être fournies **notamment au moyen de codes de conduite approuvés, de certifications approuvées et de lignes directrices données par le comité ou d'indications données par un délégué à la protection des données**. Le comité peut également publier des lignes directrices relatives aux opérations de traitement considérées comme étant peu susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques et indiquer les mesures qui peuvent suffire dans de tels cas pour faire face à un tel risque. » **Article 35 - Analyse d'impact relative à la protection des données** « 1. 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 responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires. 2. Lorsqu'il effectue une analyse d'impact relative à la protection des données, le responsable du traitement demande conseil au délégué à la protection des données, si un tel délégué a été	établis en vue de proposer aux responsables de traitements et aux sous-traitants des lignes directrices s'agissant notamment de l'identification des risques liés aux traitements, de leur évaluation en termes d'origine, de nature, de probabilité et de gravité, et de l'identification des meilleures pratiques visant à atténuer ces risques.	Guide de la Cnil « PIA-2, L'outillage : modèles et bases de connaissances de l'étude d'impact sur la vie privée », éd.2015 Guide de la Cnil « PIA-3, Les bonnes pratiques : mesures pour traiter les risques sur les libertés et la vie privée », éd.2012 **A venir :** Privacy Impact Assessment (ISO/IEC 29134)

Thématique	Disposition du RGPD	Commentaire	Outils existants et à venir
	désigné. 3. L'analyse d'impact relative à la protection des données visée au paragraphe 1 est, en particulier, requise dans les cas suivants: a) 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; b) 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; ou c) la surveillance systématique à grande échelle d'une zone accessible au public. »		
Privacy by default et Privacy by design	**Article 25 : Protection des données dès la conception et protection des données par défaut** « 1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et 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, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux	Les responsables de traitements devront formaliser et mettre en place des processus en vue de garantir la protection des données dès la conception du traitement ainsi que par défaut. Un mécanisme de certification pourra servir au responsable de traitements d'élément visant à démontrer le déploiement de tels process et mesures.	Label Cnil « Procédure de gouvernance Informatique et libertés » Maturité dans les processus : Privacy capability assessment model (ISO/IEC 29190) Terminologie et principes : Privacy framework (ISO/IEC 29100) **A venir :** Code of practice for personally identifiable information protection

Thématique	Disposition du RGPD	Commentaire	Outils existants et à venir
	exigences du présent règlement et de protéger les droits de la personne concernée. 2. Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée. **3. Un mécanisme de certification approuvé en vertu de l'article 42 peut servir d'élément pour démontrer le respect des exigences énoncées aux paragraphes 1 et 2 du présent article. »**		(ISO/IEC 29151) Certifications Bureau Veritas : « Privacy checked / privacy by design », « Gouvernance » et « RGPD »
Sécurité des données	**Article 32 : Sécurité du traitement** « 1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et 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, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins: a) la pseudonymisation et le chiffrement des données à caractère personnel; b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des	Le responsable de traitements et le sous-traitant seront tenus de mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité des données adapté au risque existant. L'application d'un code de conduite ou d'un mécanisme de certification pourra servir aux responsables de traitements et aux sous-traitants d'élément visant à démontrer la bonne mise en œuvre de ces mesures.	Normes générales sur la sécurité : ISO 27001 et ISO 27002 Norme applicable au cloud uniquement : norme ISO 27018 Normes applicables aux techniques de cryptographie : -Requirements for partially anonymous, partially unlinkable authentication (ISO/IEC 29191) -Blind digital signatures (ISO/IEC 18370)

Thématique	Disposition du RGPD	Commentaire	Outils existants et à venir
	systèmes et des services de traitement; c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique; 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. 2. Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite. 3. **L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou d'un mécanisme de certification approuvé comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des exigences prévues au paragraphe 1 du présent article.** 4. Le responsable du traitement et le sous-traitant prennent des mesures afin de garantir que toute personne physique agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne les traite pas, excepté sur instruction du responsable du traitement, à moins d'y être obligée par le droit de l'Union ou le droit d'un État membre. »		Normes relatives à l'archivage des données : - NF Z42013 - ISO 14641-1 (système d'archivage électronique) Normes relatives à la sécurité de l'industrie des cartes de paiement : Payment Card Industry Data Security Standard ou PCI DSS Guides de l'ANSSI (voir notamment la note technique « Préoccupations relatives au respect de la vie privée et à la confidentialité des données sous Windows 10 », 31-1-2017) Label Cnil « Procédure de gouvernance Informatique et libertés » Guide de la Cnil : « La sécurité des données personnelles », éd.2010 Guide de la Cnil : « PIA-3, Les bonnes pratiques : mesures pour traiter les risques sur les libertés et la vie privée », éd.2012 Cnil, Délib. 2017-012 du 19-1-2017 portant adoption d'une

Thématique	Disposition du RGPD	Commentaire	Outils existants et à venir
			recommandation relative aux mots de passe **A venir :** Normes relatives aux techniques d'anonymisation : Privacy enhancing data de-identification techniques (ISO/IEC 20889)
Transfert de données	**Article 46 : Transferts moyennant des garanties appropriées** « 1. En l'absence de décision en vertu de l'article 45, paragraphe 3, le responsable du traitement ou le sous-traitant ne peut transférer des données à caractère personnel vers un pays tiers ou à une organisation internationale que s'il a prévu des garanties appropriées et à la condition que les personnes concernées disposent de droits opposables et de voies de droit effectives. 2. Les garanties appropriées visées au paragraphe 1 peuvent être fournies, sans que cela ne nécessite une autorisation particulière d'une autorité de contrôle, par: a) un instrument juridiquement contraignant et exécutoire entre les autorités ou organismes publics; b) des règles d'entreprise contraignantes conformément à l'article 47; c) des clauses types de protection des données adoptées par la Commission en conformité avec la procédure d'examen visée à l'article 93, paragraphe 2;	Les transferts de données à caractère personnel vers un pays tiers (hors Union Européenne) ne prévoyant pas de garanties appropriées devront être strictement encadrés. Les codes de conduite et certifications sont des garanties qui pourront être utilisées en vue de l'encadrement de tels flux, à l'instar des traditionnelles Binding corporate rules ou encore des clauses contractuelles types. Les articles 40 et 42 du RGPD prévoient d'ailleurs la possibilité pour des organismes non soumis au RGPD (qu'ils soient responsables de traitements ou sous-traitants) de se conformer à un code de bonne conduite ou à un mécanisme de certification afin de	Label Cnil « Procédure de gouvernance Informatique et libertés » Binding Corporate Rules (BCR) Clauses contractuelles types (CCT) Privacy Shield pour les entreprises US qui y ont adhéré.[3]

[3] Une vigilance accrue doit être portée quant à une possible remise en cause du Privacy Shield.

Thématique	Disposition du RGPD	Commentaire	Outils existants et à venir
	d) des clauses types de protection des données adoptées par une autorité de contrôle et approuvées par la Commission en conformité avec la procédure d'examen visée à l'article 93, paragraphe 2; e) **un code de conduite approuvé conformément à l'article 40, assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées**; ou f) **un mécanisme de certification approuvé conformément à l'article 42, assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées.** (…) »	garantir un niveau adéquat en termes de protection des données à caractère personnel.	

*
* *

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